Towards a Transparent and Systematic Approach to Conducting Risk Assessment under Article 35 of the GDPR

Von der Juristischen Fakultät

der Gottfried Wilhelm Leibniz Universität Hannover zur Erlangung des Grades

Doktor der Rechtswissenschaften

Dr. jur.

genehmigte Dissertation von

Iheanyi Samuel Nwankwo, LL.M.

2021

Referent: **Prof. Dr. Nikolaus Forgó**

Korreferentin: **Prof. Dr. Tina Krügel**

Tag der Promotion: **12 August 2021**

DEDICATION

This study is dedicated to my late parents, Mr. and Mrs. Patrick and Rosemary Nwankwo.

ABSTRACT

This dissertation focuses on the risk assessment carried out as part of a data protection impact assessment (DPIA) under Article 35 of the General Data Protection Regulation (GDPR), particularly, Article 35 (7)(c). Conventionally, risk assessment is a process of risk management that aims to identify the potential threats against an asset or object of value, analyse the likelihood and severity of the threats and potential harms if they materialise, and evaluate the risk level with the ultimate objective of implementing measures to mitigate the identified risks. The current data protection framework in the EU has integrated a risk-based approach, requiring that risk assessment be conducted in several situations, including in the course of a DPIA. When this risk management feature is transposed to the context of data protection, the question then is how this process should be appropriately carried out to meet the requirements of the data protection law and retain its risk management characteristics? There is no mandatory methodology under the GDPR for this exercise. Published guidelines on DPIA by the supervisory authorities have not clarified the scope of this core process. In most of these guidelines, for example, there are no clear and systematic criteria for identifying data protection threats, analysing and evaluating the likelihood and severity of the risk, as well as how to measure the risk level. This uncertainty undoubtedly affects the use and practical relevance of these guidance documents, as well as the resultant DPIAs that are based on them.

Bearing in mind that the GDPR does promote consistency and requires an objective assessment of risk, would the mostly subjective and unsystematic approach to risk assessment be sustainable henceforth? How could more procedural transparency be devised in this exercise, and what impact will it have? This dissertation argues in favour of a more uniform and systematic approach to data protection risk assessment and posits that it is feasible to achieve given that the GDPR contains provisions that can be used to design this risk assessment architecture systematically. Existing risk management tools can be leveraged to accomplish this objective. What is missing, however, is a careful adaptation of these tools to suit the data protection environment. The study further argues that good practices in DPIA should be incentivised as a way of encouraging well-designed and implemented risk assessment.

This study, therefore, proposes a method of mapping the ISO 31000:2018 processes with the relevant GDPR requirements for a DPIA and further suggests a methodology for operationalising risk assessment in a systematic way. This approach not only exposes the steps of conducting risk assessment during a DPIA, but also makes it easy to identify and focus on relevant criteria for completing each step. Theoretically, this translates a DPIA into a procedural 'tool of transparency' as advanced by De Hert and Gutwirth's theory of data protection.

In the end, several recommendations are made to relevant stakeholders on how to further achieve consistency in the application of risk assessment during a DPIA. The output of this study targets not only the data controllers and processors, who are eager to find the best method of complying with the DPIA obligation, but also the supervisory authorities, as it will be valuable in their review and audit functions. It also exposes parameters upon which these stakeholders can measure whether a risk assessment has been appropriately conducted. The broader privacy community will find the content of this study interesting in advancing their knowledge.

Keywords

Data Protection, Data Protection Impact Assessment, Risk Assessment

KURZFASSUNG

Diese Dissertation konzentriert sich auf die Risikobewertung, die im Rahmen der Datenschutz-Folgenabschätzung nach Art. 35 der Datenschutz-Grundverordnung (DSGVO), insbesondere Art. 35 Abs. 7 lit. c, durchgeführt wurde. Üblicherweise ist die Risikobewertung ein Prozess des Risikomanagements, der darauf abzielt, die potenziellen Gefahren für ein Gut oder einen Wertgegenstand zu identifizieren, die Wahrscheinlichkeit und den Schweregrad der Bedrohungen und potenziellen Schäden zu analysieren und das Risikoniveau zu bewerten mit dem Ziel, die identifizierten Risiken zu minimieren. Die DSGVO hat einen risikobasierten Ansatz integriert, der eine Risikobewertung in verschiedenen Situationen, auch im Rahmen einer Datenschutz-Folgenabschätzung, erforderlich macht. Wenn ein Risikomanagement im Datenschutz-Kontext durchgeführt wird, stellt sich die Frage, wie dieser Prozess auszugestalten ist, um den Anforderungen der DSGVO zu genügen. Es gibt dafür keine verbindliche Methodik. Veröffentlichte Richtlinien zur Datenschutz-Folgenabschätzung der Aufsichtsbehörden haben den Umfang dieses zentralen Prozesses nicht geklärt. In den meisten dieser Richtlinien gibt es zum Beispiel keine klaren und systematischen Kriterien für die Identifizierung von Datenschutzbedrohungen, für die Analyse und Bewertung der Wahrscheinlichkeit von Schäden und des Schweregrades des Risikos sowie für die Messung des Risikoniveaus. Diese Ungewissheit beeinträchtigt zweifellos den Nutzen und die praktische Relevanz dieser Leitfäden und damit auch die Qualität der darauf basierenden Datenschutz-Folgenabschätzungen.

Wenn man bedenkt, dass die DSGVO die Kohärenz fördert und eine objektive Risikobewertung erfordert, kann dann der meist subjektive und unsystematische Ansatz der Risikobewertung Nachhaltigkeit erzielen? Wie kann die verfahrenstechnische Transparenz verbessert werden und was wären die Auswirkungen? Diese Dissertation plädiert für einen einheitlicheren und systematischeren Ansatz zur Risikobewertung im Datenschutz und stellt fest, dass dieser machbar ist, da die DSGVO Bestimmungen enthält, die zur systematischen Gestaltung der Risikobewertung genutzt werden können. Dazu kann auf bereits existierende Instrumente für das Risikomanagement zurückgegriffen werden. Was jedoch fehlt, ist eine sorgfältige Anpassung dieser Instrumente an das Datenschutzumfeld. Diese Arbeit zeigt auf, wie dies erreicht werden kann. Es wird ferner argumentiert, dass gute Praktiken bei der Datenschutz-

Folgenabschätzung als Anreiz für eine gut konzipierte und umgesetzte Risikobewertung gefördert werden sollten.

Diese Studie schlägt daher eine Methode zur Abbildung der ISO 31000:2018-Prozesse mit den entsprechenden DSGVO-Anforderungen für eine Datenschutz-Folgenabschätzung und darüber hinaus eine Methode zur systematischen Operationalisierung der Risikobewertung vor. Dieser Ansatz legt nicht nur die Schritte der Durchführung der Risikobewertung während einer Datenschutz-Folgenabschätzung offen, sondern macht es auch leicht, die relevanten Kriterien für die Durchführung der einzelnen Schritte zu identifizieren und sich auf diese zu konzentrieren. Theoretisch wird eine Datenschutz-Folgenabschätzung damit zu einem verfahrenstechnischen "Werkzeug der Transparenz", wie es die Datenschutztheorie von De Hert und Gutwirth vorschlägt.

Abschließend werden mehrere Empfehlungen an die relevanten Interessengruppen gegeben, wie sie bei der Anwendung der Risikobewertung während einer Datenschutz-Folgenabschätzung Beständigkeit verwirklichen können. Die Ergebnisse dieser Studie sind zum einen für die Verantwortlichen und die Auftragsverarbeiter von Interesse, da jene bestrebt sind, die beste Methode zur Erfüllung der Verpflichtung zur Datenschutz-Folgenabschätzung zu finden. Zum anderen können auch die Aufsichtsbehörden bei Ausübung ihrer Auditaufgaben von dem vorgeschlagenen Konzept profitieren. Die Studie legt auch Parameter offen, an denen die genannten Interessengruppen messen können, ob eine angemessene Risikobewertung durchgeführt wurde. Auch für das breitere Umfeld der Datenschützer*innen wird der Inhalt dieser Studie interessant sein, um ihr Wissen zu erweitern.

Schlagwörter

Datenschutz, Datenschutz-Folgenabschätzung, Risikobewertung

TABLE OF CONTENTS

ABBREVIATIONS

Acronym	Meaning
AEPD	Agencia Española de Protección de Datos
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
BC	Before Christ
BSI	Bundesamt für Sicherheit in der Informationstechnik
CDPD	Computer, Privacy and Data Protection
CFREU	Charter of Fundamental Rights of the European Union
CIA	Confidentiality, Integrity, Availability
CIPL	Centre for Information Policy Leadership
CJEU	Court of Justice of the European Union
CNIL	Commission Nationale de l'Informatique et des Libertés
CNPD	Commission Nationale pour la Protection des Données
COBRA	CO-Benefits Risk Assessment
CoE	Council of Europe
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
DEFRA	Department for Environment Food and Rural Affairs
DHS	Department of Homeland Security
DPA	Data Protection Authority
DPC	Data Protection Commissioner
d.pia.lab	Brussel's Laboratory for Data Protection and Privacy Impact Assessments
DPD	Data Protection Directive
DPO	Data Protection Officer
DPIA	Data Protection Impact Assessment
DSK	Datenschutzkonferenz
DS-GVO	Datenschutz Grundverordnung
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
EC	European Commission
EDPB	European Data Protection Board
EU	European Union
EUM	Expected Utility Maximisation
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EFSA	European Food Safety Authority
EIA	Environmental Impact Assessment
ENISA	European Union Agency for Cybersecurity
FAIR	Factor Analysis of Information Risk
GBA	Gegevensbeschermingsautoriteit
GDPR	General Data Protection Regulation
HAZOP	Hazard and Operability

IAIA	International Association for Impact Assessment
ICCPR	International Covenant on Civil and Political Rights
ICO	Information Commissioner's Office
ICT	Information and Communication Technology
IDW	Institut der Wirtschaftsprüfer
IEC	International Electrotechnical Commission
IOSH	Institute of Occupational Safety and Health
ISO	International Organization for Standards
ISRM	Information Security Risk Management
IT	Information Technology
LINDDUN	Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance
LED	Law Enforcement Directive
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NRC	National Research Council
OECD	Organisation for Economic Co-operation and Development
OJ	Official Journal
ONF	Open Networking Foundation
OPC	Office of the Privacy Commissioner
PIA	Privacy Impact Assessment
PIAF	A Privacy Impact Assessment Framework for data protection and privacy rights
PCI DSS	Payment Card Industry Data Security Standards
PII	Personally Identifying Information
PRIAM	Privacy RIsk Analysis Methodology
RFID	Radio-frequency identification
SA	Suoervisory Authority
SDM	Standard Data Protection Model
SRA	Society for Risk Analysis
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
US	United States
UNEP	United Nations Environmental Program
WP29	Article 29 Working Party

TABLE OF CASES

TABLE OF STATUTES

International Treaties/Law

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981 (CoE Convention 108).
- International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR).
- Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (128th Session of the Committee of Ministers, Elsinore, Denmark, 17-18 May 2018) (Modernised Convention 108).
- Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR).

European Regional Treaties, Laws, Resolutions, Communications and Recommendations

- Charter of Fundamental Rights of the European Union 2000.
- Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radiofrequency identification (2009/387/EC).
- Commission, Commission Recommendation of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems (2014/724/EU).
- Commission, Commission Staff Working Paper Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) SEC (2012) 72 final.
- Commission, Communication from the Commission on Impact Assessment COM (2002) 276 final.
- Commission, Communication on safeguarding privacy in a connected world. A European Data Protection framework for the 21st Century' COM (2012) 9 final.
- Commission, Communication from the Commission on the Precautionary Principle COM (2000) 1 final.
- Council of Europe, Recommendation 509 Human Rights and Modern Scientific and Developments (1968).
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981.
- Council of Europe, Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private section (26 September 1973).
- Council of Europe, Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public section (20 September 1974).
- Council of Europe, Resolution 428 (1970) Declaration on mass communication media and Human Rights (23 January 1970).

- Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.
- European Convention on Human Rights (adopted 4 November 1950).
- European Parliament resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada (P7_TA(2010)0144).
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (as amended by Directive 2006/24/EC and 2009/136/EC).
- Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.
- Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on the assessment of the effects of certain public and private projects on the environment [2011] OJ L 26/1.
- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
- Directive (EC) 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive).
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
- Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.
- Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II).
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.
- Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law,

establishing the European Food Safety Authority and laying down procedures in matters of food safety.

- Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.
- Treaty of the Functioning of the European Union (Lisbon Treaty) 2007.

National Law

- French Civil Code (as amended in 1970).
- German Basic Law 1949.
- German Federal Data Protection Act
- German Census Act 1983
- Hesse Data Protection Act 1970.
- Kenyan Data Protection Act 2019
- Portuguese Constitution 1976.
- Spanish Constitution 1978.
- Swedish Data Act 1973.
- UK Human Rights Act 1998.
- UK Data Protection Act 1998.

LIST OF TABLES

LIST OF FIGURES

ACKNOWLEDGEMENT

It has been a long and exciting journey to complete this study. At some point, it seemed challenging, and in fact, thought of 'not being able to finish it' has cropped up severally. But, thank God this finally has come to an end. Indeed, I could not have achieved this without the support of my huge family, friends and colleagues. And I want to use this limited space to say a huge thank you to all of you.

Most importantly, I will remain forever grateful to my supervisor, Prof. Dr. Nikolaus Forgó, not only for agreeing to supervise this dissertation but also for giving me the opportunity to work at the Institute for Legal Informatics, Leibniz Universität Hannover as his research assistant. Needless to say, that it was this opportunity in the first place that metamorphosed into the idea of conducting this research. I say, thank you so much, Prof. Forgó for all the things I have learnt through and from you (most importantly, making me run, and since then, love marathon!). I am equally grateful to my official reviewer, Prof. Dr. Tina Krügel, who took out time despite her tight schedule to review my dissertation. Your remarks were indeed valuable. I also cherish the time we worked together at the IRI and your kindness at all times. Thank you so much.

My wife, Nkechi and children, Nora and Elliot, have been an excellent source of inspiration. They have also endured my busy schedules throughout the process of this study. I am grateful for ALL you have done. My siblings will be particularly thrilled that this has come to be a reality: Da Adanma, Da Ugbo, Da Gray, Da Mgbechi and Da Ezinna. You have no rivals in terms of being not only my sisters, but second as my multiple 'mothers' since we lost our mother. As if it was divinely ordained, I also got your husbands as wonderful in-laws, without whom, this day may not be a reality: Engr. CU Nwiwu, Late Mr. Alphonsus Amadi, Col. Joseph Ekoh, Pastor Samuel Chukwu. Thank you all immensely for your support. I equally thank my aunt, Lauretta for her love, prayers and good wishes towards me. I also want to thank my other in-laws (my wife's family) for their support. They are indeed 'a chosen generation'.

My friends and colleagues at IRI have helped me a lot in the course of this study, both in translation, guidance and above all, providing the best atmosphere to conduct this research. Prof. em. Dr. Dr. h.c. Wolgang Killian, Thorsten Heerman, Wolfgang Rottwinkel, Sarah Jensen, Ben Schutze, Kai Wendt, Friederike Knoke, Jonathan Stoklas,

Julia Pfeiffenbring, Iryna Lishchuk, Stefanie Hänold, Lukas Czeszak, Stephanie Heinrich, Gaby Paysen, Felix Montpellier,

I say thank you for all your support and love. I also want to immensely thank my very good friend and colleague Dr. Marc Stauch, for the support he gave me during this study. He went out of his way to encourage, review and direct me on how best to approach this complex subject of study. I am also indebted to Prof. Dr. Alex Makulilo, who despite his tight schedule, still found the time to review the draft of this dissertation. Thank you so much for all your valuable comments. To my childhood friend, Innocent Ufomba, I thank you very much for all your assistance in the course of this study, including granting me access to some of the IOSH materials that I used in this research. I also want to that my bosom friend and colleague, Mr. John Olufemi Ashamu, for translating most of the German literature and his warm company during this study, as well as Dr. Benson Olugbuo, for his encouragement and review of the early draft of this work. My friend, Barr. Maduka Ezeudo, who share much intellectual discussion with me in the course of this journey is much thanked.

In life, there are always those that come your way, sometimes, miraculously to help you achieve your dreams. The limited space here is not enough to narrate individual stories, but suffice it to say that without the following persons, this dream may not have come true: Engr. Chuks Nzei, Chief Regina Okafor, Dr. Eric Ntam and Mrs. Manuela Schimmels. I pray that you shall receive a hundred-fold reward for what you did to me. Thank you so much. To all my family and friends, even though the space here does not allow me to mention your names individually, I remain grateful for all your support.

OVERVIEW

This dissertation explores the intricate process of *ex-ante* risk assessment during a data protection impact assessment (DPIA) under Article 35 of the General Data Protection Regulation (GDPR).

Although the GDPR suggests the minimum content of a DPIA in Article 35 (7) to include: a systematic description of the envisaged processing operations and the purposes; an assessment of the necessity and proportionality of the processing operations; an assessment of the risks to the rights and freedoms of data subjects; and the measures envisaged to address the risks, what it means to carry out an "assessment of the risks to the rights and freedoms of the data subjects" under Article 35 (7)(c) is unclear. There is no corresponding methodology in the Regulation on implementing this process. Published guidelines on DPIA by various supervisory authorities have also not paid attention to this core aspect—the risk assessment process. The instructions relating to how to conduct it during a DPIA appear ill-defined, and under-theorised, at best polarised in these guidelines (in fact, most authorities simply advise data controllers to choose any method they deem fit). Regrettably, data controllers and processors have also followed divergent pathways in conceptualising what it means to assess data protection risk. This has resulted in DPIA's of varying quality, most of them lacking transparency and logic in their structure.

There is also a lack of clarity concerning the metrics (factors and parameters) to consider during a risk assessment within the context of Article 35. While some generic indicators are mentioned in the GDPR (nature, scope, context, and purpose), there are no conscious efforts to develop objective metrics harmoniously and with the required granularity to instruct risk assessment. What exists in practice is polarised and diverse. Multiple templates and guidelines lack the requisite parameters.

This dissertation seeks to close these gaps and suggests how the data protection risk assessment process could be made transparent and systematic by adapting the ISO3100 risk management framework and proposes some metrics that can introduce some objectivity into the risk assessment space. It consists of six chapters.

Chapter One provides the groundwork needed to understand the framework of *ex-ante* data protection risk assessment as required by the GDPR. It exposes specific issues around risk assessment in the area of EU data protection law, indicating the gap in this area that this study seeks to fill. It also outlines the research objectives and describes the research questions that the study aims to tackle. The study's conceptual framework is followed by the research methodology, significance of the study and the conclusion.

Chapter Two takes a historical look at the notion of risk, privacy, and data protection and broadens the study context to further capture the issues at state. The historical perspective to the notion of risk and its management is traced before particularising it to the domain of privacy and data protection. On its part, privacy's evolution from an ancient and demographic approach to modern societies is traced. This chapter equally traces the rise of data protection in Europe as a proactive risk governance instrument for informational privacy protection (or data protection). A theoretical examination of data protection theory as a 'tool of transparency' as propounded by De Hert and Gutwirth is carried out in this chapter. The notion of transparency is further explored to supply the missing link in De Hert and Gutwirth's theory and evaluate the importance of transparency as a data protection principle under Article 5 of the GDPR. The chapter also suggests an approach to apply procedural transparency in the framework of DPIA with respect to methodology and stakeholder consultation, and scoping of risk assessment.

Chapter Three focuses on the risk-based approach in data protection law, and gives a detailed analysis of Article 35 of the GDPR that provides for the conduct of DPIA. It traces the genesis of the appearance of the impact assessment tool in EU data protection law and the justification for introducing it. Next, individual articles of Article 35 are interpreted to evaluate how they are being implemented in practice. In the later part of this chapter, the impact of non-compliance with the requirements of Article 35 is addressed, followed by a distinction between a DPIA and other related tools.

A literature review of the approaches to conducting impact or risk assessment is conducted in Chapter Four. This includes current attempts at automating the impact assessment process. Further, the various DPIA guidelines issued by the EU supervisory authorities are reviewed to suggest how to design future DPIA guidelines.

Chapter Five presents a systematic approach to DPIA's risk assessment process and introduces examples from information security and environmental and food safety risk assessment to learn lessons for data protection law. For practical purposes, the ISO 31000:2018 risk assessment process is adopted as a tool for mapping the GDPR's requirements of DPIA systematically. An attempt is made here to operationalise the method proposed in this study with a use case, and suggesting factors that a data protection risk assessor should consider in each step of the risk assessment process during a DPIA. The concluding discussion in this chapter centres on the prospects and challenges of adopting the method proposed in this study.

Chapter Six concludes the study, presenting key findings of the research and their implications and a summary of the key contributions of the study. Specific recommendations are suggested to stakeholders on how to effectively implement DPIA's risk assessment requirements in this GDPR era. The chapter ends with some concluding remarks.

CHAPTER ONE

1. GENERAL INTRODUCTION

1.1 INTRODUCTION

This chapter sets the scene for the issues raised by the current state of DPIA's risk assessment framework as tackled in this study. It provides a background to the problem that culminates into the research questions that the study aims to answer. The study's objective, research questions, conceptual framework, methodology, significance, and limitations are all contained in this introductory chapter.

1.2 BACKGROUND

The rights to privacy and data protection are among the most developed fundamental rights in Europe today.[1] In the European Union (EU), both primary law[2] and several secondary laws[3] provide for or implement these rights. The

[1] On the regional level, the right to respect for private and family life has been provided for under the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) art 8. The European Court of Human Rights (ECtHR) has interpreted this right broadly to cover personal data protection. See *Case of Benedik v. Slovenia* App no 62357/14 (ECtHR, April 2018); see also Council of Europe, 'Guide on Article 8 of the European Convention on Human Rights – Right to respect for private and family life' (Last updated 31 August 2019) <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf> accessed 20 February 2020.

[2] See the Treaty of the Functioning of the European Union (Lisbon Treaty) art 16; the Charter of Fundamental Rights of the European Union (CFREU) arts 7 and 8.

[3] See among others, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1 (GDPR); Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89 (hereinafter LED); Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive) [2002] OJ L 201/37; Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L 295/39.

prominence and traction that legislative instruments that regulate these rights gain from their proposal stage to final adoption are a testament to their importance to the information society.[4] For example, the GDPR was negotiated over four years, during which several stakeholders organised various consultations, and about four thousand amendments were made to the original draft proposal.[5] A survey report by the DLA Piper indicates that EU data protection authorities had issued about €114 million fines within twenty months of its enforcement.[6] This figure shows a significant increase from an earlier number of about €56 million fines indicated by the European Data Protection Board (EDPB) within the first nine months from 25 May 2018.[7] The figure is undoubtedly likely to increase in the future because public awareness about the GDPR is very high (it once ranked as one of the most searched terms on the Google search engine).[8] All these indicate that privacy and data protection rights have acquired legal recognition equal to their societal importance, and reinforces Lord Nicholls statement that privacy 'lies at the heart of liberty in a modern state.'[9] As society progresses, it is conceivable that this interest will not diminish, especially as the economic value of personal data is becoming more apparent.

---

[4] One definition of information society refers to it as 'A society where the creation, distribution, use, integration, and manipulation of information is a significant economic, political, and cultural activity.' IGI Global, 'What is Information Society' <https://www.igi-global.com/dictionary/library-science-and-technology-in-a-changing-world/14504> accessed 20 February 2020.

[5] See Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' COM (2012) 011 final; PWC, 'General Data Protection Regulation' (*PWC*, 2017) <https://www.pwc.com.cy/en/publications/assets/general-data-protection-regulation-why-how-when-january-2017.pdf> accessed 2 September 2019.

[6] DLA Piper, 'DLA Piper GDPR Data Breach Survey 2020' (*DLA Piper,* 20 January 2020) <https://www.dlapiper.com/en/uk/insights/publications/2020/01/gdpr-data-breach-survey-2020/> accessed 20 February 2020.

[7] EDPB, 'First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities' (*EDPB,* 26 February 2019) <https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pd> accessed 4 July 2019.

[8] Tess Bonn, 'Europe's GDPR Outranks Beyonce on Google Search' (*CNBC*, 24 May 2018) <https://www.cnbc.com/2018/05/23/europes-gdpr-outranks-beyonce-on-google-search.html> accessed 4 July 2019.

[9] *Campbell v. MGN Limited* [2004] UKHL 22, para 12.

Despite this interest, there is still the need to accommodate societal needs for personal data processing. This requires balancing the rights and freedoms of the data subjects with those of the data controllers[10] and processors,[11] and the society at large in appropriate contexts. This balancing act, in essence, is the focus of data protection law. For example, while allowing data controllers to process personal data of others, the GDPR imposes some obligations on them and accords several rights to the data subjects.[12] One of these obligations is the requirement to carry out a DPIA under Article 35, which is a way of managing the risk faced by the data subjects due to this data processing (a risk-based approach). Many stakeholders have welcomed this risk-based approach, in general. However, the definitional and operational aspects (e.g., vocabulary, methodology and criteria for risk assessment), as well as the overall place of DPIA in the context of sanctions and liabilities, remain unclear.[13] These issues shall be elaborated on below, as they can affect the quality and effectiveness of DPIA conducted by data controllers and processors.

1.2.1 Contextualising the Issues

Several approaches to protecting informational privacy have been combined in the European data protection framework, including the principle-based, precautionary and risk-based approaches. The principle-based approach refers to using principles to represent general rules that express the fundamental obligations of data controllers.[14] These principles have evolved over the years (originating from the

[10] Data controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. See GDPR, art 4 (7).

[11] Data processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. See GDPR, art 4 (8).

[12] For data subjects' rights, see the GDPR, arts 12 to 23.

[13] See Istvan Borocz, 'Risk to the Right to the Protection of Personal Data: An Analysis through the Lenses of Hermagoras' (2016) 2:4 European Data Protection L Rev 467; Christopher Kuner et al., 'Risk Management in Data Protection' (2015) 5 (2) International Data Privacy Law 96; CIPL, 'A Risk-based Approach to Privacy: Improving Effectiveness in Practice' (19 January 2014) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf> accessed 12 June 2019.

[14] Australian Law Reform Commission, *Regulating Privacy* (ALRC Report 108, 2008) <http://www.alrc.gov.au/publications/4.%20Regulating%20Privacy/regulatory-theory> accessed 20

'fair information practice' from the US).[15] However, they have been criticised for often leaving 'room for interpretation'—that is, leaving it to data controllers 'to make appropriate decisions on how to implement these principles.'[16] This flexibility has severally led to broken 'promises'; the assumption that data controllers willingly implement these principles properly has not materialised in many instances.[17] This reality, no doubt, has prompted the need for a more proactive and practical framework to encourage compliance with these principles and create more room for accountability.

A precautionary approach (based on the precautionary principle) adds value to the principles by emphasizing the need to anticipate future harms and take preventative measures against those harm in the face of uncertainty of their occurrence.[18] This approach ties well in the context of data processing because information technologies used for such processing pose some risks to the data subjects, even though the precise nature of these risks may not be known with certainty at the initial stage. This uncertainty makes it even more important to anticipate their occurrence and think of a policy where data controllers are encouraged or obligated to take proactive measures to reduce the risks.[19]

July 2016. Note also that ISO 29100:2011 defines privacy principles as 'set of shared values governing the privacy protection of personally identifiable information (PII) when processed in information and communication technology systems.' ISO/IEC 29100:2011 Information technology -- Security Techniques -- Privacy Framework (ISO 2011).

[15] See the US Department of Health, Education and Welfare, 'Records, Computers and the Rights of Citizens' (DHEW Publication No. (OS)73-94, July1973) 50.

[16] CIPL, 'A Risk-based Approach' (n 13) 1.

[17] See for instance, the Facebook Cambridge Analytica saga. Natasha Lomas, 'Facebook Staff Raised Concerns About Cambridge Analytica in September 2015, Per Court Filing' (*Techcrunch,* 22 March 2019); BBC, 'Facebook Staff "Flagged Cambridge Analytica Fears Earlier Than Thought"' (*BBC News*, 22 March 2019) <https://www.bbc.com/news/technology-47666909> accessed 21 June 2019.

[18] See Ortwin Renn, Pia-Johanna Schweizer, Ulrich Müller-Herold and Andrew Stirling, *Precautionary Risk Appraisal and Management An Orientation for meeting the Precautionary Principle in the European Union* (Europäischer Hochschulverlag 2009) 14. The European Commission notes that the precautionary principle is employed when there are potentially dangerous effects deriving from a phenomenon, product or process and scientific evaluation do not allow the risk to be determined with sufficient certainty. Commission 'Communication from the Commission on the Precautionary Principle', COM (2000) 1 final, 3.

[19] See Helen Nissenbaum, *Privacy in Context: Technology, Privacy and the Integrity of Social Life* (Stanford University Press 2010).

Requirements such as prior checks under Article 20 of the Data Protection Directive (DPD) show this approach. Costa observes that '[i]dentifying and following-up risks are both actions coherent to the precautionary principle,'[20] which brings out the relationship between the precautionary approach and the risk-based approach.

Given the shortcoming in implementing the data protection principles, the risk-based approach evolved and is seen as an avenue to facilitate the application of these principles and other requirements;[21] a way of 'materialising the accountability principle' in a verifiable manner.[22] In general, it is an approach that signifies the use of risk as a yardstick for measuring the obligations of the data controllers and processors.[23] For example, the obligation of recording the processing activities does not apply to an organisation employing fewer than 250 persons 'unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects'.[24] This way of using the level of risk exposure of the data subjects to allocate responsibility to the data controller, some commentators have argued, reflects the designing of compliance in a more pragmatic and scalable manner.[25]

---

[20] Luiz Costa, 'Privacy and the Precautionary Principle' (2012) 28 CLSR 14, 21. See also David Wright et al, 'Precaution and Privacy Impact Assessment as Modes Towards Risk Governance' in R Schomberg (ed) *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (EU 2011) 88; Raphaël Gellert, 'Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative' (2015) 5 IDPL 1.

[21] CIPL, 'A Risk-based Approach' (n 13) 4.

[22] Katerin Demetzou, 'GDPR and the Concept of Risk: The Role of Risk, the Scope of Risk and the Technology Involved' in Eleni Kosta et al (eds) *Privacy and Identity Management Fairness, Accountability and Transparency in the Age of Big Data* (Springer 2019) 141. See also Claudia Quelle, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach' (2018) 9 European Journal of Risk Regulation 9; GDPR, art 24.

[23] See Milda Macenaite, 'The "Riskification" of European Data Protection Law through a two-fold Shift' (2017) 8 European Journal of Risk Regulation 506, 517-532.

[24] See GDPR, art 30 (5).

[25] See CIPL, 'A Risk-based Approach' (n 13); Demetzou, 'GDPR and the Concept of Risk' (n 22); Paul Schwartz, 'Risk and High Risk: Walking the GDPR Tightrope' (IAPP, 29 March 2016) <https://iapp.org/news/a/risk-and-high-risk-walking-the-gdpr-tightrope/https://iapp.org/news/a/risk-and-high-risk-walking-the-gdpr-tightrope/> accessed 25 July 2016; Article 29 Working Party, 'Statement on the Role of a Risk-based Approach in Data Protection Legal Frameworks' (WP 218, 30 May 2014); Gabriel Maldoff, 'The Risk-Based Approach in the GDPR: Interpretation and Implications' (IAPP, March 2016); Alessandro Spina, 'A Regulatory

The EDPS gives a practical example of this scalability with respect to the right of access. A risk assessment may indicate to a data controller not to 'invest in an automated self-service system for data subject assess request, but only provide a contact point and deal with requests manually, since a small number of such requests is expected given the nature of the processing.[26] Such an approach also allows for efficient allocation of scarce resources when managing risk, which is at the centre of this approach.

However, the unaddressed issue is how to design an appropriate model through which the risk management elements inherent in the risk-based approach can be seamlessly integrated with data protection law requirements. This issue is important because the notion of risk assessment has a scientific origin and may require some adaption before implementing it in a socio-legal context. In this respect, some suggestions have been made: the CIPL suggests that '[a]ttempts to manage privacy risks should be integrated as closely as possible alongside well-established risk management processes'.[27] However, the implementation of such a suggestion largely depends on certain conditions. Kuner et al. express doubt about the effectiveness of deploying conventional risk management techniques in the data protection field if the groundwork and preconditions for using such risk management tools have not been met. They highlight four areas that need to be addressed: lack of widely accepted principles surrounding the newly developing approach to data protection risk management; lack of understanding as to what harms or negative impact that this risk management is intended to identify and mitigate; incoherent expectations for the goals and uses of risk management; and lack of tools to implement this risk management framework.[28] Kuner et al.'s arguments are plausible given the already witnessed misuse of the established risk

Marriage de Figaro: Risk Regulation, Data Protection and Data Ethics (2017) 8 European Journal of Risk Regulation 88; Quelle, 'Enhancing Compliance under the General Data Protection Regulation' (n 22).

[26] EDPS, 'Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation' (February 2018) 16.

[27] CIPL (n 13) 5.

[28] Kuner et al., 'Risk Management in Data Protection' (n 13) 95-98.

management vocabularies in the data protection environment,[29] as well as the lack of consensus as to the constituent elements and principles of this risk management framework.

Since conducting a proactive risk assessment has become an integral part of EU data protection law, such an *ex-ante* risk assessment system ought to be done systematically to adequately identify the threats that innovative ICTs pose to the rights and freedoms of the data subjects, as well as to suggest measures to mitigate those threats. Moreover, the GDPR expects that 'risk should be evaluated on the basis of an objective assessment', meaning that such a process should not only be systematic but also transparent.[30] However, except for indicating a minimum content of a DPIA (at least to be shown in a report) in Article 35 (7), there is, unfortunately, no prescribed methodology for conducting this risk assessment under the GDPR. This has given rise to a fragmented situation where multiple approaches and methods exist for this exercise.

As a result of this uncertainty, which existed before the adoption of the GDPR, it is not surprising that data controllers have understood what it means to complete risk assessment differently. On the one hand, some have conceptualised impact or risk assessment as an exercise of a compliance check, or completion of a questionnaire to identify the purposes of data processing.[31] For example, noting that Privacy Impact Assessment (PIA) is used to assess 'the level of compliance against Nokia's core privacy requirement', Bräutigam indicates that Nokia relies on 'template or questionnaire' when completing its PIA. On the other hand, some other data controllers view impact assessment as a form of risk management exercise and tend to rely on established risk management tools and methodology in conducting it.[32] The outcome of this polarisation has been significant. In essence,

[29] See Section 1.2.2 below for further discussion on this issue.

[30] See GDPR, recital 76.

[31] See Tobias Bräutigam, 'PIA: Cornerstone of Privacy Compliance in Nokia' in David Wright and Paul De Hart (ed) *Privacy Impact Assessment* (Springer 2012) 261-267.

[32] The Vodafone's approach to PIA has a more risk management framework. See, Florian Thoma, 'How Siemens Assess Privacy Impacts' in David Wright and Paul De Hert (eds), Privacy Impact Assessment (Springer 2012) 291-299.

many impact assessments lack a logical and theoretical framework for risk assessment, a point highlighted by the WP29 in rejecting the initial DPIA framework for the RFID applications.[33]

Several attempts have been made to address these shortcomings from academia,[34] industry[35] and regulatory authorities, even before the GDPR era.[36] However, a lot still needs to be done. Unfortunately, guidelines from EU supervisory authorities seem to lack uniformity regarding how to achieve an objective risk assessment. There is also a significant difference in terms of the procedure and content of risk

[33] The WP29 lamented the absence of risk assessment process in its Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications [WP 175]. For a critique of the ICO PIA Code of Practice for similar point, see Marie Oetzel and Sarah Spiekermann 'A Systematic Methodology for Privacy Impact Assessments – A Design Science Approach' (2013) 23 EJIS1, 4.

[34] Recently, the Vrije Universiteit Brussel's Laboratory for Data Protection and Privacy Impact Assessments (d.pia.lab) has been active in this area. See <http://www.dpialab.org/> accessed 13 January 2020. The European Commission (EC) has also funded a project on PIA (PIAF Project), whose output is documented in several deliverables. See for example PIAF Deliverable D1: A Privacy Impact Assessment Framework for Data Protection and Privacy Rights (2011) <http://www.piafproject.eu/ref/PIAF_D1_21_Sept_2011.pdf> accessed 23 May 2019. See also David Wright and Paul De Hart (ed) *Privacy Impact Assessment* (Springer 2012); Roger Clarke, 'An Evaluation of Privacy Impact Assessment Guidance Documents' (2011) 1:2 International Data Privacy Law 111; Linden Consulting Inc, 'Privacy Impact Assessment: International Study of their Application and Effects' (October, 2007) <http://www.rogerclarke.com/DV/ICO_2007_Study.pdf> accessed 16 May 2019.

[35] For example, the Centre for Information Policy Leadership (CIPL) has published a series of guidance paper on privacy risk management. See CIPL, 'A Risk-based Approach' (n 13); CIPL, 'The Role of Risk Management in Data Protection' (2014), <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_2-the_role_of_risk_management_in_data_protection-c.pdf>; CIPL, 'Protecting Privacy in a World of Big Data – the Role of Risk Management', (discussion draft, February 2016), <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big _data_paper_2_the_role_of_risk_management_16_february_2016.pdf>; CIPL, 'Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR' (2016) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf> accessed 27 February 2019. Also, the International Organization for Standardization has published ISO/IEC 29134:2017 Guidelines for PIA, marking an effort to harmonise impact assessment at a global level.

[36] See Chapter Four for a full list of DPIA guidance documents from EU data protection authorities. Other non-EU regulatory guidance documents include OAIC, 'Privacy Impact Assessment Guide' (Revised May 2010) <http://www.icb.org.au/out/?dlid=38156>; OAIC, Guide to Undertaking Privacy Impact Assessment (2014) <https://www.oaic.gov.au/resources/agencies-and-organispations/guides/guide-to-undertaking-privacy-impact-assessments.pdf> accessed 9 July 2018; Sean Brooks et al, 'An Introduction to Privacy Engineering and Risk Management in Federal Systems', NISTIR 8062 (2017) <https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf> accessed 9 July 2018; Treasury Board, 'Directive on Privacy Impact Assessment' (2010) <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308&section=html> accessed 9 July 2018.

assessment they instruct—some are detailed in addressing most of the components of risk assessment. In contrast, others only address a few broad principles or advise risk assessors to choose any method they deem fit (see further discussion in Chapter Four).

Moreover, there are no uniform steps for carrying out the entire DPIA from these guidelines. Given this gap, it is not surprising to see non-uniform DPIA templates and reports emanating from their use.[37] A report of the Multi-stakeholder Expert Group on the first-year application of the GDPR highlights the differences between the supervisory authorities' methodologies on how to conduct a DPIA as one of the factors leading to uncertainty and inconsistency in the application of the GDPR.[38] Furthermore, a survey by the EDPS shows weak indicators concerning the length and quality of DPIAs conducted by EU institutions, with several recommendations pointing to the need for a reference risk assessment methodology.[39] Undoubtedly, such polarisation creates a loophole in realising the objectives behind the introduction of DPIA. However, this does not imply that it is impossible to achieve a common approach. What is needed is an authoritative clarification of how risk should be interpreted in the context of data protection and how the processes and tools of risk management could be leveraged to identify, analyse, and evaluate this risk systematically. The GDPR provides a starting point here because it gives examples of some relevant factors to consider when demonstrating compliance '[…] especially as regards the identification of the risk

[37] For example, see the articles on how PIA is conducted in Nokia, Siemens and Vodafone published in David Wright and Paul De Hart (ed) *Privacy Impact Assessment* (Springer 2012) indicating three different approaches.

[38] Multistakeholder Expert Group, 'Contribution from the Multistakeholder Expert Group to the Stock-Taking Exercise of June 2019 on One Year of GDPR Application' (Report, 13 June 2019) 13 <https://ec.europa.eu/commission/sites/beta-political/files/report_from_multistakeholder_expert_group_on_gdpr_application.pdf> accessed 17 September 2019.

[39] EDPS, 'EDPS Survey on Data Protection Impact Assessments under Article 39 of the Regulation (case 2020-0066)' <https://edps.europa.eu/sites/default/files/publication/20-07-06_edps_dpias_survey_en.pdf> accessed 12 September 2021.

related to the processing, their assessment in terms of origin, nature, likelihood and severity'.[40]

Another crucial issue that is yet to be addressed is the place of DPIA in the overall context of data protection law concerning its impact during sanction and liability assessment by the courts or supervisory authorities. This area is grey under the GDPR; it does not present an explicit place regarding the value or impact of a DPIA when assessing fines or compensation in the face of a breach that happens after it had been conducted. It seems though that under the GDPR, unlawful processing attracts strict liability towards the controller or processor, vis-à-vis the data subjects as per Article 82 (1), which provides:

> Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

Here, no element of fault is required, which means that no matter the appropriateness or otherwise of a DPIA, the controller or processor is strictly liable for any infringement of the GDPR that results in damage to the data subject. However, the controller or processor is only exempted from liability under Article 82 (3) 'if it proves that it is not in any way responsible for the event giving rise to the damage'. The ingredients of this defence are not defined, which leaves room for speculation as to whether an argument of no-fault is equivalent to 'not in any way responsible'. Nevertheless, a related provision in the DPD suggests that the defence of no-fault may not avail the defendant:

> […] whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in cases where he establishes fault on the part of the data subject or in case of force majeure.[41]

It is unclear why the elements of the data subject's fault and force majeure are omitted in the GDPR. Alsenoy, though, suggests that the liability regime under the

---

[40] GDPR, recital 77.

[41] DPD, recital 55. By contrast, Recital 146 of the GDPR, which is the equivalent of Recital 55 of the DPF, did not list such defence.

Regulation is similar to that of the DPD and remains strict, indicating that the infringing controller or processor 'cannot escape liability simply by demonstrating the absence of personal fault.'[42]

By contrast, though, when it comes to the issuance of administrative fines by the supervisory authorities, Article 83 (2) requires, among other things, that 'the intentional or negligent character of the infringement' be considered. Moreover, the WP29 has further clarified the issue of fines in its guidelines on applying administrative fines.[43] What is missing, though, is clear attribution of the impact of a DPIA in the considerations for fines. Which brings up the question of in what circumstances would the controller's or processor's performance of a DPIA (appropriately or otherwise) affect the sanction regime under the GDPR? For example, would conducting a DPIA well and acting on the insights it brings reduce the risk of a liability-inducing event and the prospect of supervisory authorities' fines – on top of (or separate from) liability to data subjects?

The answer to these questions may have a motivational effect for conducting a well-designed DPIA. If there are clear benefits for conducting a DPIA, it is conceivable that controllers and processors will invest time and effort in doing it well. While, the strict liability approach of the liability vis-à-vis the data subjects, may not offer many incentives since on a literal interpretation, the controller or processor is liable in any case of infringement, once a data subject suffers damage, it is, however, arguable that a different approach should prevail concerning supervisory authorities' fines. In such circumstances, a DPIA should form part of the consideration for assessing such fines. This opinion is suggestive from the language of Article 83 (2) (d), which provides that 'the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32' should be considered in issuing a fine. Although Article 35 is not explicitly mentioned here,

[42] Brenden Van Alsenoy, 'Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation' (2016) 7 J Intell Prop Info Tech & Elec Com Law 271, 282.

[43] WP29, 'Guidelines on the Application and Setting of Administrative Fines for the Purpose of the Regulation 2016/679' (adopted 3 October 2017) WP 253.

DPIA is an integral part of the data protection by design and the security obligations under the above two articles.

Furthermore, the WP29 guidelines suggest that the provision of Article 83 (2)(d) is not exhaustive to those two articles because the WP29 includes Article 24 as part of the considerations in its explanations relating to this article.[44] The WP29 comments further:

> Article 25 and Article 32 […] Rather than being an obligation of goal, these provisions introduce obligations of means, that is, the controller must make the necessary assessments and reach the appropriate conclusions. The question that the supervisory authority must then answer is to what extent the controller 'did what it could be expected to do' given the nature, the purposes or the size of the processing, seen in light of the obligations imposed on them by the Regulation.

Implicit in this statement is that other actions of the controller or processing, such as a well-done DPIA (which is expected), should be considered in assessing what is 'necessary' and 'appropriate' in the context of the data processing. This study argues that such a consideration during administrative fines will offer some incentive to do a DPIA appropriately. Since failure to do a proper DPIA may lead to a fine (as a violation of the requirements of the GDPR), a correctly done DPIA should attract a reward (at least when considering fines) to encourage proper conduct, particularly, where the affected controller or processor could show that it has taken adequate, foreseeable and necessary steps to assess the risks and implemented measures to mitigate them. Unfortunately, there is a dearth of judicial cases or supervisory authorities' opinions on this issue, and only a few authors have written on the subject.[45]

As shall be further elaborated in the subsequent sections and chapters, the nature of the problems associated with the introduction of DPIA as a tool for implementing the risk-based approach is manifold, including:

1. Definitional and vocabulary issues relating to core terms used around

[44] Ibid, 13.

[45] See Raphaël Gellert and Dariusz Kloza, 'Can Privacy Impact Assessment Mitigate Civil Liability? A Precautionary Approach' 2012 Jusletter IT; Alsenoy, 'Liability under EU Data Protection Law' (n 42).

DPIA. As shall be further elaborated in the next section, terms such as DPIA, data protection risk, threat and harm, lack precision in the context they are used.

2. The systematisation of the framework of DPIA so that there are precise and harmonised steps across the EU since the obligation to conduct a DPIA can have a cross-border effect. This can be seen from the variations in the various guidelines issued by various EU data protection authorities (see Chapter Four for a comparison of these guidelines).
3. The operationalisation of the processes of DPIA in terms of having clear indicators (factors and criteria) for completing each step in the whole DPIA exercise. For example, what factors should be considered when analysing the likelihood and severity of data protection risks (see Chapter Five for operationalisation of DPIA's risk assessment process).
4. The place of DPIA in the overall context of data protection liability and sanction regime, as already discussed above.

Regrettably, relatively little debate concerning these issues and their impact on the overall outcome and effectiveness of a DPIA has taken place. This study aims to contribute to this debate and provide a theoretical and practical framework for approaching data protection risk assessment in the future. This study argues that although the GDPR is flexible on implementing a DPIA, the quest for objectivity and transparency requires a systematic approach to assessing the data processing risks. As such, the normative purpose of Article 35 will be better served if this systematic approach is developed and backed up by clear guidelines on how risk should be identified, analysed and evaluated. This way, data protection as a 'tool of transparency'[46] will bring about an ex-ante control of the data controllers and processors by the data subjects and supervisory authorities and lead to a consistent and systematic risk assessment framework that is verifiable and reproducible.

This position draws inspiration from the theory of data protection as propounded by De Hert and Gutwirth, which posits that data protection is a legal means of control that 'tend to guarantee the transparency and accountability of the powerful'—in this case, data controllers and processors.[47] This study aims to

[46] See Paul De Hert and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of The Individual and Transparency of Power' in Erik Claes, Anthony Duff and Serge Gutwirth (eds), *Privacy and the Criminal Law* (Intersentia 2006).

[47] Ibid, 66-68.

explore this theory and suggests ways of applying it through the lens of the doctrine of foreseeability. Drawing further inspiration from ISO 31000:2018 standard,[48] the study intends to map the requirements of DPIA with this standard to structure a uniform and systematic DPIA methodology, particularly the risk assessment process.

Having identified the broader problem that this study seeks to address in the preceding discussion, the following section shall elaborate more on the specifics by looking at the lack of precise definition of the core concepts of DPIA, data protection risk and its dependencies, such as threat and harm.

1.2.2 The Problem of Definition and Vocabulary

Kuner et al. have identified the development of a professional practice of risk management, which would assist in developing a common vocabulary for data protection risk management, among others, as one of the issues to be addressed for a smooth implementation of risk management in data protection circle.[49] This is important given that most authors who write about data protection or privacy risk appear to ignore any rule in using the terms associated with risk management. They indiscriminately and interchangeably use terms such as privacy risks, privacy threats and privacy harms, treating them erroneously as synonyms in most cases. As such, the vocabulary, components and techniques used to define, identify and measure privacy/data protection risk are ambiguous and imprecise, as the following discussion indicates. This has the potential of affecting the effectiveness of a DPIA.

1.2.2.1 Defining Data Protection Impact Assessment

The term Data Protection Impact Assessment is not defined in the GDPR.[50] This may have partly contributed to some confusion about what it means in practical terms and its relationship and distinction with other tools of similar nature such

[48] ISO 31000:2018 Risk Management — Guidelines.

[49] Kuner et al., 'Risk Management in Data Protection' (n 13) 96-97. See also CIPL (n 13).

[50] The term DPIA appeared 24 times in the GDPR, see GDPR, recitals 84,89,90,91,92,94,95; arts. 35, 36, 39, 57 and 64.

as compliance checks, privacy audits, etc.[51] One earlier academic work by De Hert seems to equate the term with compliance check:

> To keep terminology and argumentation simple, I equate data protection impact assessment with simply checking the legal requirements spelled out in the European data protection framework, in particular, those contained in regulations created by the EU, especially the Data Protection Directive (95/46/EC), the e-Privacy Directive (2002/58/EC), as amended by Directive 2006/24/EC and 2009/136/EC, the Data Retention Directive (2006/24/EC) the Council Framework Decision 2008/977/JHA (dealing with data protection with regard to criminal matters, i.e., former third pillar issues) and Regulation 45/2001 (laying down data protection rules for the institutions and bodies).[52]

This simplification, though, misses the point that, while compliance check is implied in a DPIA, a DPIA certainly goes beyond that as a risk management tool by requiring data controllers to anticipate, identify threats, and institute mitigation plan against those threats.[53] A DPIA will offer limited value if it merely checks compliance with specific laws since some data processing projects may be legally compliant without meeting the expectations of data subjects or considering future risks posed by a current operation. This is arguably why stakeholders such as data subjects or their representatives must be consulted in appropriate cases when conducting a DPIA. It is not surprising that De Hert did not repeat this line of definition in his subsequent works.[54] Other academics have also provided alternative views. Alnemr et al. define the term more interestingly:

> A Data Protection Impact Assessment (DPIA) method aims to identify the main risks of a project with respect to the rights of data subjects concerning their personal data. It is a systematic process to elicit threats to the privacy of individuals, identify the procedures and practices in place to mitigate

[51] See further discussion on the distinctions between DPIA and similar tools in Chapter Three.

[52] Paul De Hart, 'A human rights perspective on privacy and data protection impact assessment' in D Wright and P De Hert (eds.) *Privacy Impact Assessment* (Springer Heidelberg 2012) 34-35.

[53] See PIAF Deliverable D1 (21 September 2011) 189.

[54] In another article with Papakonstantinou, they wrote: 'A Data Protection Impact Assessment (DPIA) may be defined as a systematic process for evaluating the potential effects on privacy and data protection of a project, initiative, proposed system or scheme and finding ways to mitigate or avoid any adverse effects.' Paul De Hert and Vagelis Papakonstantinou, 'The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals' (2012) 28 Computer Law and Security Review 130, 140.

> these threats, and document how the risks were addressed in order to minimise harm to data subjects.[55]

Although it is not clear why Alnemr et al. limit the assessment to 'main risks' instead of all risks that could be potentially identified, their definition gives credence to the assertion that DPIA is a risk management tool. The WP29 guidelines also re-echo this view in its description of DPIA as 'a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them'.[56] Here, in addition to its risk management feature, the WP29 tries to sum up the content of Article 35 (7) of the GDPR into a single definition. Notably, the European Commission has also referred to DPIA as 'a process whereby a conscious and systematic effort is made to assess privacy risks to individuals in the collection, use and disclosure of their personal data.' DPIAs, it continues, 'help identify privacy risks, foresee problems and bring forward solutions.'[57] Subsequently, in the Smart Meter recommendation, the Commission calls it 'a systematic process for evaluating the potential impact of risks where processing operations are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes to be carried out by the controller or processor, or the processor acting on the controller's behalf".[58]

Although, when considered side-by-side, terminological differences can be seen in the definitions above, they all see DPIA in a positive light as a proactive tool for

---

[55] Rahab Alnemr et al., 'A Data Protection Impact Assessment Methodology for Cloud' in Bettina Berendt et al., (eds) *Privacy Technologies and Policy Third Annual Privacy Forum, APF 2015 Luxembourg, Luxembourg, October 7–8, 2015 Revised Selected Papers (*Springer 2016) 60.

[56] WP29, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679' (Adopted on 4 October 2017) WP 248rev.01, 4.

[57] Commission, 'Commission Staff Working Paper Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' SEC (2012) 72 final, i.

[58] Commission, 'Commission Recommendation of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems' (2014/724/EU).

managing risk: for discovering, assessing and treating the risks that personal data may face while undergoing processing. However, the above approaches to defining DPIA fail to ground the concept within its root words, that is, 'data protection' and 'impact assessment' capable of independent definition. As an alternative to the current approach, this study shall attempt a more nuanced explanation by dissecting the term 'data protection impact assessment' into two—'data protection' and 'impact assessment', and bring our understanding of both together to arrive at a holistic definition that uncovers the essence and nature of the concept.

I. Data Protection

The concept of data protection has been extensively discussed in the literature, often bugged with authors trying to show the difference between the terms 'data protection' and 'privacy'.[59] In a nutshell, privacy is a multi-dimensional concept of which data protection is a dimension that focuses on protecting the informational aspect of privacy. Suffice it to say that the key difference between the term privacy and data protection is the scope. Data protection is the common parlance in Europe to denote this informational privacy, and its principles have been codified in various data protection laws such as the GDPR.

Other terms, such as data privacy, informational self-determination, and information privacy, have been interchangeably used with data protection.[60] It is not intended in this section to discuss the differences in the definition of these terms at this stage, but to simply understand the essence of data protection and its connection with impact assessment.

As Blume eloquently puts it, 'data protection is the price that the data controller must pay in order to be able to process personal data.'[61] This price stems from

[59] See Peter Blume, 'Data Protection and Privacy – Basic Concepts in a Changing World' in Peter Wahlgren (ed), *Information and Communication Technology Legal Issues* (2010) 54 Scandinavian studies in law, 152; Maria Tzanou, *The Fundamental Right to Data Protection* (Hart Publishing 2017) 21-24; HIIG, 'Warum Privacy ≠ Datenschutz ist (und wie sie sich überschneiden)' (4 May 2016) <https://www.hiig.de/warum-privacy-%E2%89%A0-datenschutz-ist-und-wie-sie-sich-ueberschneiden/> accessed 12 November 2019.

[60] See Chapter Two for a fuller discussion on the rise of data protection law in Europe.

[61] Blume, 'Data Protection and Privacy' (n 59)162.

the idea that processing personal data poses a threat to the data subject, and whoever undertakes such an operation should take reasonable care to prevent harm to the subjects. The process of uncovering this threat that could harm the data subjects and suggesting ways of mitigating them is the essence and focus of 'impact assessment'—an aspect of risk management that concentrates on understanding what could happen if a threat materialises. Below we shall examine the concept of impact assessment in detail.

II. Impact Assessment

The International Association for Impact Assessment (IAIA) defines the term impact assessment as: 'the process of identifying the future consequences of current or proposed action. The "impact" is the difference between what would happen with the action and what would happen without it.'[62] This definition is attractive and straightforward; it captures the essence of impact assessments. The concept of impact assessment gained prominence in environmental protection, where Environmental Impact Assessment (EIA) is said to be the oldest use of the concept.[63] Here, it is used as a tool for analysing the possible consequences of an environmental-related initiative to society and supporting decision-making in mitigating those concerns. Thus, EIA is defined as 'the process of identifying, predicting, evaluating and mitigating the biophysical, social, and other relevant effects of development proposals prior to major decisions being taken and commitments made.'[64] Article 3 of the EU Directive on environmental impact assessment, for example, provides the scope of an EIA under the Directive:

> The environmental impact assessment shall identify, describe and assess in an appropriate manner, […] the direct and indirect effects of a project on the following factors: (a) human beings, fauna and flora; (b) soil, water, air,

[62] IAIA, 'What is Impact Assessment' (*IAIA,* October 2009) <http://www.iaia.org/uploads/pdf/What_is_IA_web.pdf> accessed 29 July 2019. The terms 'impact' and 'effect' are frequently used synonymously.

[63] Ibid, 1.

[64] Ibid. Although there is no universal consensus on this definition, this definition appears to capture the essence of the concept.

climate and the landscape; (c) material assets and the cultural heritage; (d) the interaction between the factors referred to in points (a), (b) and (c).[65]

This provision indicates the essence of an EIA, as well as the parameters for the assessment. Notably, the impact assessment tool was soon broadened to cover other areas: the European Commission introduced it in 2003 as a tool for estimating *ex-ante*, the impact of its policy and regulatory proposals in economic, social and environmental terms.[66] Since this introduction, an impact assessment report now accompanies all legislative proposals by the Commission.[67]

In light of these legislative initiatives, authors have tried to provide a theoretical analysis of impact assessment application in risk scenarios. Hillson and Hulett, for example, believe that it is relatively simple to assess the impact of risk since this merely requires defining the situation after the risk has occurred, and then estimating the possible effect on each objective.[68] This approach sees impact assessment as an exercise in structured imagination encapsulated in the question: 'If this were to happen, what would the effect be?'[69] From this perspective, one element of impact assessment stands out, its anticipatory quality. It hinges on anticipation of the future effect of an event if it happens. There is, however, an inherent element of uncertainty in an impact assessment since there is a possibility that the impact may not happen as predicted.

[65] Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on the assessment of the effects of certain public and private projects on the environment [2011] OJ L 26/1.

[66] European Parliament, 'How Does Ex-ante Impact Assessment Work in the EU?' (February 2015) <http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/528809/EPRS_BRI(2015)528809_EN.pdf> accessed 30 July 2019.

[67] The European Parliament in its resolution on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada notes that PIA shall precede any new legislative instrument. See European Parliament, 'European Parliament resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada' (P7_TA(2010)0144).

[68] David Hillson and David Hulett, 'Assessing Risk Probability: Alternative Approaches' (PMI Global Congress Proceedings – Prague, 2004) 1.

[69] Ibid.

Nevertheless, Kloza et al. have identified certain generic best practices for impact assessments following a comparative analysis of its use in multiple areas, suggesting that there is 'no "silver bullet" method for carrying out impact assessment'.[70] The tools used for impact assessment, though, include a systematic structure, making it easy for others to review such an assessment in the light of the context it is made.

III. Data Protection Plus Impact Assessment

From the discussion above, it could be seen that the process of assessing the effects of a proposed data processing operation is the central domain of a DPIA. This assessment extends from how the data is collected to how it is archived or destroyed. Suppose we adopt the definition of impact assessment by the IASA to the data protection field. In that case, a DPIA could then be said to refer to *the systematic process of identifying, predicting, evaluating and mitigating the impact of a proposed personal data processing on the data subject before the commencement of the processing*.[71] This approach exposes the essence of the tool. It solves the problem of confusing a definition of a DPIA with the provisions of the law requiring its performance (as seen in the WP29 Guidelines) or compliance check as De Hert tends to suggest. It is apparent that, in practice, a DPIA can still be carried out on an ongoing processing operation (including a review of an initial DPIA in the course of the processing). Nevertheless, it has to be stressed that the core idea behind carrying out an impact assessment before the commencement of most activities is to forestall risks that could have been discovered and mitigated before it is too late.

Suffice it to say that the main focus of an impact assessment is the systematic manner in which risks are uncovered and mitigated, irrespective of the timing of the assessment (precise timing could be a matter dealt with by a regulation mandating such assessment). In the case of the GDPR, for example, impact assessment can happen vis-à-vis the lifespan of the data processing operation: both

[70] Dariusz Kloza et al., 'Data Protection Impact Assessment in the European Union: Complementing the New Legal Framework Towards a more Robust Protection of Individual' d.pia.lab Policy Brief No.1/2017, 2.

[71] This is an adaptation of the EIA definition by the IASA. IASA (n 62).

before the risk events happen, that is, before the commencement of the data processing, as well as after a breach has occurred in order to notify the authorities and the data subjects in appropriate cases (see arts. 33 and 34). The former is seen from the provisions relating to DPIA under (art 35), data protection by design (art 25), and security of the data (art 32).

The latter case is implicit in the condition that the data controller shall notify the supervisory authority of a breach 'unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons' (art 33 (1)). Arguably, there is no way to determine this except if an impact assessment of the breach has been carried out. Furthermore, in the case of notifying this breach, the notification shall, among other things, 'describe the likely consequences of the personal data breach' (art 33 (3) (c)). This provision, again, supports the position that an impact assessment is required to determine these likely consequences. Article 34(1) also conveys an implicit condition that a risk assessment is needed to know 'when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons' so that the data controller shall notify the data subjects. The WP29 has noted in its guidelines on data breach notification that 'an additional assessment' shall be required in case of a data breach, which shall take into account the actual circumstances.[72] It further explains that this risk assessment has a different focus from that of a DPIA since a DPIA is hypothetical, while in the case of a breach, the focus is about the real impact to the data subject based on the circumstances of the actual data breach.[73]

This timeline is illustrated in Figure 1 below.

[72] WP29, 'Guidelines on Personal Data Breach Notification under Regulation 2016/679' (adopted 6 February 2018) WP 250rev.01, 12.

[73] Ibid, 23.

Figure 1: Illustration of when to carry out a risk assessment under the GDPR

Having stated the above, it is also pertinent to consider other definitions of terms associated with DPIA such as data protection risk, harm and threat to see how the imprecise manner they are defined contribute to the problem around DPIA.

1.2.2.2 Defining Informational Privacy/Data Protection risks

Various sources have attempted to define risk in the context of informational privacy without any consensus as to what it means. For example, the ISO/IEC 29100:2011, defines privacy risk as 'the effect of uncertainty on privacy'.[74] Such a definition does not assist much in untangling the complexity of the subject matter, as it merely equates risk with the element of uncertainty. The Spanish AEPD, for its part, sees data protection risk as a risk stemming from the exposure to threats associated with data processing.[75] It categorises these threats as illegitimate access to data, unauthorised modification of data and deletion of data resulting in unavailability when needed, an approach familiar to information security risk management. Indeed, such an approach raises the issue of whether any processing that does not pose these threats is not 'risky'. On the surface, this definition does not account for those instances where legitimate processing, such as profiling, could pose a risk to data subjects without any data security breach.

The CNIL prefers a descriptive definition of the term privacy risk as:

> [A] hypothetical scenario that describes:
> - how risk sources (e.g. an employee bribed by a competitor)

[74] ISO/IEC 29100:2011—Information technology—Security techniques—Privacy framework <https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en> accessed 22 December 2019.

[75] AEPD, Guia Práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD (March 2018) 3-4 (hereafter 'Practical Guide on Risk Analysis'). (Translation by the author).

- could exploit the vulnerabilities in personal data supporting assets (e.g. the file management system that allows the manipulation of data)
- in a context of threats (e.g. misuse by sending emails)
- and allow feared events to occur (e.g. illegitimate access to personal data)
- on personal data (e.g. customer file)
- thus generating impacts on the privacy of data subjects (e.g. unwanted solicitations, feelings of invasion of privacy, etc.).[76]

This description adopts a more information security vocabulary (e.g. supporting assets), although it seeks to highlight risk and its components as much as possible, which is a potentially helpful move. However, it ends up sacrificing brevity; its 'hypothetical' nature makes it challenging to appreciate privacy risk precisely. Borocz also criticises it because 'it implies that only unwanted events have [an] impact on the privacy of the data subject.' [77]

For its part, the CIPL has sought to avoid this pitfall by proposing a probabilistic definition of privacy risk:

> […] privacy risk equals the probability that a data processing activity will result in an impact, threat to or loss of (in varying degrees of severity) a valued outcome (e.g. rights and freedoms). An unacceptable privacy risk, therefore, would be a threat to, or loss of, a valued outcome that cannot be mitigated through the implementation of effective controls and/or that is unreasonable in relation to the intended benefits.[78]

This definition precisely describes the core elements of risk in the context of data processing. Such an approach of defining personal data processing risk in terms of likelihood and severity is common; it appears in several parts of the GDPR and other sources.[79] For example, the NIST Draft Internal Report on privacy risk

[76] CNIL, 'Privacy Impact Assessment (PIA) Methodology' (CNIL February 2018 edition) 6.

[77] Borocz, 'Risk to the Right to the Protection of Personal Data' (n 13) 469.

[78] CIPL 'Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR' (n 35) 14.

[79] See for example, AEPD, 'Practical Guide on Risk Analysis' (n 75); ICO, 'Guide to the General Data Protection Regulation - Data Protection Impact Assessment' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>; Sean Brooks and Ellen Nadeau (eds), 'Privacy Risk Management for Federal Information Systems' (NISTIR 8062 (Draft), 2015) <http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf> accessed 18 March 2019. Note that the German DSK defines risk in the context of GDPR as 'the existence of

management even contained a mathematical formula for privacy risk, using the properties of likelihood and impact (see Figure 2).[80]

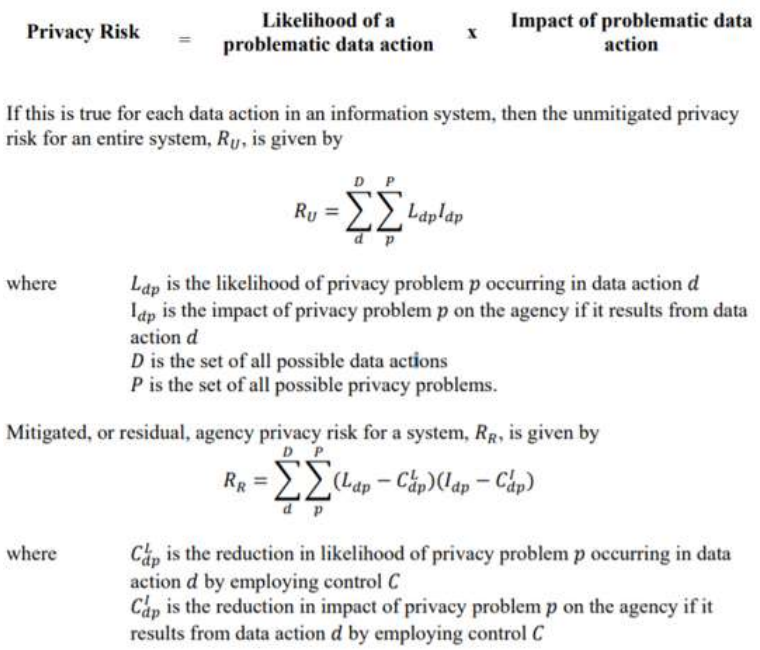


Figure 2: NIST's mathematical definition of risk

When compared, some similarities and differences could be seen from these definitions, including the terminology used. While they all define one aspect of privacy risk—informational privacy risk, they term it broadly as 'privacy risk'. However, there is an agreement that the risk they describe emanates from the processing of personal data, as indicated in the last three definitions. The AEPD and the CNIL definitions are explicit in their focus on the data subject as the entity that bears the impact of the manifestation of the threats and, therefore, is the object of protection. However, unlike the CIPL definitions, the CNIL and AEPD do not incorporate the element of likelihood or probability, even though these are considered elsewhere in their respective guidance documents. On the part of the

---

the possibility of occurrence of an event which itself constitutes damage (including unjustified impairment of rights and freedoms of natural persons) or which may lead to further damage to one or more natural persons. It has two dimensions: first, the severity of the damage and, secondly, the likelihood that the event and consequential damage will occur.' DSK, 'Kurzpapier Nr. 18 Risiko für die Rechte und Freiheiten natürlicher Personen' (26 April 2018) 1 <https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf> accessed 18 March 2019. (Translated from German by the author).

[80] Sean Brooks and Ellen Nadeau (eds), ibid, 31. Note that is report has been superseded by a 2017 version Sean Brooks et al, 'An Introduction to Privacy Engineering and Risk Management in Federal Systems' (NIST 2017).

NIST, representing privacy risk in a mathematical equation is a bold move. However, when conducting an impact assessment, there might be difficulty transposing complex mathematical values to a socio-legal construct (of rights and freedoms). The value in such equations is perhaps, on programming a software tool for PIA, as it may be easy for software engineers to translate equations into models.[81] Other definitions even expose further fragmentation,[82] and it is beyond the scope of this study to attempt a reconciliation of them all.

What is though, not clear from these definitions is what risk a DPIA is meant to address. Is it the risk emanating from planned data processing, a data breach, or both? This gap is significant, as noted by the CIPL and Kuner et al. earlier cited. Most data controllers and processors assume they should focus on data breach risk, but this is not correct since a DPIA is meant to manage all risks, both from planned and unplanned events. This position could be seen in the statement of the WP29 that: 'DPIA considers both the risks of the data processing being carried out as planned, and the risks in case of a breach'.[83] This study agrees with this approach and favours the conceptualisation of data protection risk as covering both scenarios. Such an approach allows a further opportunity to profoundly articulate the various situations that the data protection processing could present threats and multiple measures to mitigate these threats.

Another thing that needs to be untangled from these definitions of privacy risk is the meaning of the risk dependencies (threats, harms, etc.) when put in context. This shall be the focus of the following section.

[81] Many PIA software tools are currently available such as CNIL, PIA Software https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment>; AvePoint PIA, <https://www.avepoint.com/privacy-impact-assessment/> accessed 18 March 2019. See also Section 4.2.2 and Annex 3.

[82] See Kathleen Greenaway et al. 'Privacy as a Risk Management Challenge for Corporate Practice' <https://www.ryerson.ca/content/dam/tedrogersschool/privacy/privacy_as_a_risk_management_challenge.pdf> accessed 18 December 2019; David Wright and Charles Raab, 'Privacy Principles, Risks and Harms' (2014) 28 (3) IRLCT 277.

[83] WP29, 'Guidelines on Personal Data Breach Notification' (n 72) 23.

1.2.2.3 Informational Privacy/Data Protection Threats

There is no agreement as to what informational privacy or data protection threats are. However, a conventional definition of the term threat refers to 'anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm'.[84] A threat could refer to several things in risk vocabulary, for example, a tornado, flood, a hacker, etc.; the key consideration is that threats apply the force (water, wind, exploit code, etc.) against an asset that can cause harm.[85]

The term threat has appeared severally in privacy discussions, although with a different focus. Warren and Brandeis, for example, argued that by overstepping their journalistic boundaries in reporting private matters, the modern press poses a threat to privacy, which could result in injury to the subject's feelings.[86] Here, the unwanted incident that could harm a person is the overzealous press intrusion in reporting private affairs. Prosser identifies four interferences that threaten privacy right (as found in US tort cases): intrusion upon a person's seclusion or solitude; public disclosure of embarrassing private facts about a person; publicity which places a person in a false light in the public eye; and appropriation, for another's advantage, of a person's name.[87] Solove, for his part, also broadly groups activities that threaten privacy into four kinds: information collection, information processing, information dissemination, and invasion.[88]

[84] Jack Jones, 'An Introduction to Factor Analysis of Information Risk (FAIR)' (2005) Risk Management Insight, 13.

[85] Ibid.

[86] Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) IV Harvard Law Review 193, 196.

[87] William Prosser 'Privacy' (1960) 48: 3 CLR 383.

[88] Daniel Solove, 'A Taxonomy of Privacy' (2006) 154:3 University of Pennsylvania Law Review 447.

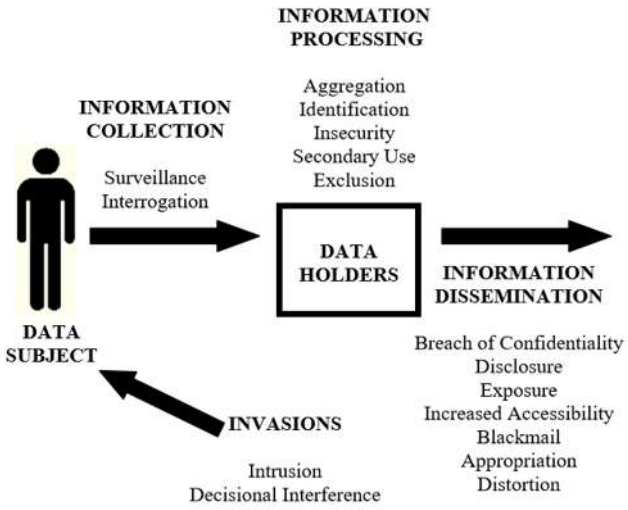


Figure 3: Daniel Solove's examples of privacy threatening activities which could lead to harms

Solove shows in the diagram above that each group consists of related subgroups of activities that threaten privacy (with the potential to harm the data subjects in diverse ways). For example, under the broad threat of information collection are two other sub-threats: surveillance which could lead to the harm of self-censorship and inhibition; and interrogation, which could lead to the harm of compulsion, divulgence of private information and forced betrayal.[89]

As is evident from these examples from the US privacy law, fragmented use of the term 'threat' abounds. Similar indiscriminate usage is also witnessed in the European jurisdiction, where, in the context of data protection, it is commonly assumed that the mere processing of personal data poses a threat to informational privacy: a threat of interference with the rights of the affected subjects.[90] Although this stand is debatable, there is no agreement on the definition or characterisation of what amounts to a data protection threat. However, it is understood that how data is processed may present different kinds of threats at a lower level. For example, collecting excessive personal data, further processing data for purposes unknown before the collection, transmitting unencrypted personal data over a public network, storing data for an indefinite time, etc., are typical examples of

[89] Ibid, 491-504.

[90] See CIPL, 'A Risk-based Approach to Privacy' (n 13) 5; the Census case BVerfGE 65, 1.

processing that threaten personal data protection because of the vulnerabilities associated with such processing that could be exploited to harm the data subjects.

However, Taylor frames data protection threats into two activities: insecure use of data and imprecise use of data.[91] He explains these threats thus:

> 1. Insecure use of data. This causes harm through unauthorised or illegal use whether that be through loss or theft of data or use by data controllers outside of areas for which they have legal authority. Harm here would include identity theft and fraud or sharing with third parties without permission and could result in financial loss, nuisance marketing or discrimination.
>
> 2. Imprecise use of data. This is use of data within legally authorised purposes, but in a manner that none-the-less harms the data subject through the poor quality of the application e.g. personalisation algorithms that produce advertising of no interest to the data subject; medical algorithms that have a high error rate in diagnosis; financial algorithms that make inaccurate risk assessment; or security algorithms that have low precision in identifying threats. These problems can also result in financial loss, nuisance marketing or discrimination.[92]

Taylor's statement above suggests that illegal data processing poses a threat to the data subjects as well as specific lawful processing if executed through a poor technique. He, however, fails to mention other legally sanctioned processes, which though using 'high-quality' techniques (e.g. artificial intelligence), may yet, in their application, harm the data subjects, such as some profiling that leads to the discrimination of the data subject. It is also doubtful whether this categorisation considers threats from activities before the 'use of data', such as the collection processes.

Some data protection authorities have also commented on data protection threats. For example, the CNIL defines threat as '[p]rocedure comprising one or more individual actions on data supporting assets.'[93] On its part, the Spanish AEPD sees

[91] Roger Taylor, 'No Privacy without Transparency' in Ronald Leenes et al (eds), *Data Protection and Privacy: The Age of Intelligent Machines* (Hart Publishing 2017) 68-71.

[92] Ibid, 68.

[93] CNIL (n 76) 10. It further notes that the action could be 'intentionally or otherwise', performed by the risk sources and 'may cause a feared event.' In the CNIL PIA Knowledge Bases, three feared events were identified with many illustrations of each: illegitimate access to personal data;

a threat as 'any risk factor with potential to cause damage or harm to data subjects whose personal data are processed'.[94]

The terminological disunity in describing what amount to a data protection threat is apparent from the examples above. Again, it is unclear what threats a DPIA should assess. Are they those from the planned use of data or those of unplanned events such as a data breach? Should they emanate from humans or non-humans? How could these threats be categorised, and what factors should be considered when identifying them, their likelihood of materialising and their severity? There is no consensus on these issues. However, if we transpose the conventional wisdom about threats (where a threat is regraded as something/someone that exploits a vulnerability to harm an asset) to the context of data protection, a threat should cover both the planned and the unplanned activities that can potentially cause an unwanted incident, which can harm the data subjects. The element of 'potentiality' here, arguably, gives room for using the foreseeability test to circumscribe a threat (see further Section 2.5.2). The sources of these threats should also include both humans and non-humans. Although there is also no agreement regarding the categorisation of data protection threats, the literature suggests that they could be categorised using the data lifecycle: collection, use/processing, storage, transfer, destruction.[95]

In general, attempts to develop a generic list of data protection threats have not yielded any consensus. For example, the Spanish AEPD has a 'risk typology' in its guide on risk assessment.[96] However, this typology is not widely referred to

unwanted modification of personal data and disappearance of personal data. CNIL, 'Privacy Impact Assessment (PIA) Knowledge Bases' (February 2018) 6-10, <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf> accessed 12 December 2019.

[94] AEPD, 'Practical Guide on Risk Analysis' (n 75) 3-4. (Translation by the author).

[95] See Cindy Ng, 'A Guide on the Data Lifecycle: Identifying Where Your Data is Vulnerable' (21 August 2018) <https://www.varonis.com/blog/a-guide-on-the-data-lifecycle-identifying-where-your-data-is-vulnerable/>; See also AEPD (n 75) Annex II.

[96] AEPD, 'Practical Guide on Risk Analysis' (n 75) 31. Although the list is short, it indicates that such a generic list could be achieved if resources are pooled by stakeholders to painstaking compile a lexicon of data protection threats, harms, vulnerabilities, etc.

elsewhere in Europe. Notably, the GDPR gives some examples of what amounts to threats in the context of data processing.[97] The GDPR also indicates using the nature, scope, context and purpose of processing to assess risk. In Chapter Five, these indicators or metrics shall be analysed further to achieve a level granularity required to instruct a risk assessment.[98]

In summary, there is no consensus on how to define threats in informational privacy or data protection and the components of such threats. Learning lessons from other areas where threats form a core of risk assessment framework can assist in untangling this issue and hoping that the community will develop a common vocabulary in the future.

1.2.2.4 Privacy/Data Protection Harm

In conventional parlance, harm is seen as damage or injury to an asset due to the threat source exploiting a vulnerability. However, it is not always easy in many cases to substantiate what harm is caused when informational privacy or data protection rights are violated. Van der Sloot's somewhat sarcastic question goes to this point: 'what harm follows from entering a home or eavesdropping on a telephone conversation as such when neither objects are stolen nor private information disclosed to third parties?' [99] In reality, many people may be unaware that their informational privacy or data protection right has been violated, especially in a complex information processing system. This may be due to the manner of data collection or the automated nature of the processing. Take the example of placing cookies on people's devices without adequately informing them or obtaining their consent; these cookies may be there for years. Nevertheless, the data subjects may not notice any harm (but perhaps wonder why certain adverts are targeted at them).

---

[97] See for example, GDPR, Recital 91—difficulty to exercise data subjects' rights; prevention from using a service or contract; surveillance; Recital 75—unauthorised reversal of pseudonymisation, processing that reveals special categories of data, among other provisions.

[98] The Spanish AEPD and the Finnish supervisory authorities have also attempted to provide some characteristics for analysing nature, scope, context and purpose of data processing. See Chapter Four.

[99] Bart van der Sloot, 'Where is the Harm in a Privacy Violation? Calculating the Damages Afforded in Privacy Cases by the European Court of Human Rights' (2017) 8 JIPITEC 322.

As noted in the Rand Technical Report:

> Identifying damage or the resulting harm when privacy protections are removed or breached is a complex task. There may be direct and indirect forms of damage and they may have consequences upon the individual in a variety of ways, ranging from monetary to social, mental and physical. *It is also difficult to identify types of harm in advance.* Finally, loss of privacy may also affect society at large, by undermining trust and confidence in those using personal data.[100]

This statement indicates the difficulty of defining harm precisely, although there is a tacit and broad understanding that it refers to a negative consequence from a privacy violation.[101]

As could be deduced from the discussion above, the imprecise nature of harm poses a challenge in identifying, categorising and defining it in advance in the context of data protection. Some authors, though, have attempted to define it from various angles. The CIPL, for example, defines informational privacy harm as signifying 'any damage, injury or negative impact—whether tangible or intangible, economic, non-economic or reputational—to an individual that may flow from the processing of personal data. It extends to any denial of fundamental rights and freedoms.'[102] While this definition captures the nature of loss that may flow from a violation of data protection, it does not reveal the element of uncertainty in the assessing harm *ex-ante* during a DPIA. Harm could manifest in unimaginable ways; as such, it is very challenging to assess it *ex-ante* since this may differ significantly when an actual breach happens.

Even assessing harm *ex-post* is also not free from challenges. A look at how courts determine harm may reveal this challenge and how society appreciates privacy harm. The courts are usually reluctant to accept any harm claim that is not tangible (involving some dimension of palpable physical injury or financial loss) and vested

---

[100] Neil Robinson, Hans Graux, Maarten Botterman and Lorenzo Valeri, 'Review of the European Data Protection Directive' (Rand 2009) 2 <http://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR710.pdf> accessed 3 September 2019. See also ICO, 'Conducting Privacy Impact Assessments Code of Practice' (Version 1.0, 2014) 7 (italics mine).

[101] See M. Ryan Calo, 'The Boundaries of Privacy Harm' (2011) Indiana Law Journal 1132.

[102] CIPL (n 13) 2.

(must have already occurred).[103] Recent cases that emerged after the adoption of the GDPR (though from different legal jurisdictions) tend to prove this point. These rulings have taken some national specificities, sometimes opposing each other. In a case in which a plaintiff alleges harm of pain and suffering as a result of an email he received from the defendant (in breach of the GDPR), the District Court Diez (Germany) dismissed the claim for compensation on the premise that a mere infringement of the GDPR without causing any damage does not directly lead to compensation.[104] A similar decision was reached by the Dresden Court of Appeals (Oberlandesgericht Dresden – Court of Appeals) in a claim where the plaintiff alleges that he suffered harm due to the deletion of his post and suspension of his social media user account for three days by the defendant.[105] The court refused to award damages because the alleged action does not constitute a serious breach of the right to privacy, which would justify monetary compensation under Article 82 (1) GDPR. In order words, the alleged harm is not tangible. These decisions, in a way, go to support Solove and Citron's assertion that 'harm drives the way courts think data-breach cases'.[106]

However, there is a recent contrasting decision of the English Court of Appeal in *Lloyd v Google LLC.* The court ruled that a claimant can recover damages for infringement of their data protection rights under Section 13 of the UK's Data Protection Act, without proving pecuniary loss or distress.[107] In this case, Google acquired and used the browser generated information from iPhone's Safari browser users without their consent between August 2011 and February 2012. As

[103] Daniel Solove, 'Privacy and Data Security Violations: What's the Harm? <https://teachprivacy.com/privacy-data-security-violations-whats-harm/> accessed 26 August 2019; Daniel Solove and Danielle Citron, 'Risk and Anxiety A Theory of Data-Breach Harms' (2017) 96 Texas Law Review 737, 749.

[104] AG Dietz, Schlussurteil vom 07.11.2018 - 8 C 130/18, para 10.

[105] Oberlandesgericht Dresden Beschl. v. 11.06.2019, Az.: 4 U 760/19. See also Sven Schonhofen, Friederike Detmering and Alexander Hardinghaus, 'German court ruling: no claims for damages under Article 82 GDPR for minor GDPR violations' (Lexicology, 21 August 2019) ,

[106] Daniel Solove and Danielle Citron, 'Risk and Anxiety A Theory of Data-Breach Harms' (2017) 96 Texas Law Review 737, 749.

[107] [2019] EWCA Civ 1599.

the claimant alleges, this violation resulted in the affected subjects suffering damage due to the loss of control over their data. The Court of Appeal agreed with this argument. It ruled 'that a claimant can recover damages for loss of control of their data under section 13 of DPA, without proving pecuniary loss or distress'.[108] The appellate court noted that control over personal data is an asset that has value, 'so that loss of that control must also have a value'.[109] Although this case originated before the GDPR, the appellate court cited relevant portions of the GDPR to buttress the impact of a loss of control in damage assessment going forward.

An Austrian Regional Court of Feldkirch has also ruled that the mere feeling of being disturbed by the unlawful processing of political party affinity data by itself already constitutes immaterial harm that entitles a claimant to damages.[110] These cited cases may look contradictory; however, it is essential to note that they are from different legal systems, and not final (as the time of writing), as they are pending appeal to the higher courts. It will be interesting if these cases get to the CJEU to see how they will be resolved, especially on the issue of harm.

While these cases reveal the uncertainty concerning *ex-post* data breach harm, the situation is even more challenging in *ex-ante* situations, where harm is expected to play a role in risk assessment. The lack of a transparent methodology of identifying and categorising harm makes it challenging to determine the role and scope of identifying harm in *ex-ante* risk assessments. This determination is crucial, and it seems that the bar is very high judging by the comment of the WP29 that the risk-based approach 'should take into consideration every potential as well as actual adverse effect, assessed on a very wide scale […]'.[111] This appears to be too broad an exercise and spans from relying on common knowledge to expert knowledge to determine harm. A more recent statement from the ICO that 'harm does not

[108] Ibid, para 88.

[109] Ibid, para 47.

[110] Christopher Schmidt, 'Austria: EUR 800.– in GDPR Compensation for Unlawful Processing of Political Affiliation Data (Hint: It's not Schrems ... yet!)' <https://www.linkedin.com/pulse/austria-eur-800-gdpr-compensation-unlawful-processing-christopher/> accessed 11 November 2019.

[111] WP29, 'Statement on the Role of a Risk-based Approach in Data Protection Legal Frameworks', (2014) 14/EN, WP218, 4.

have to be inevitable to qualify as a risk or a high risk',[112] support the view that the authorities will pay attention to the extent of foreseeability of harm when reviewing a DPIA. This thinking may have prompted the ICO's remarks when imposing fine on Sony Entertainment following a data breach in 2013. The ICO noted that in the circumstances surrounding the breach, the data controller knew or ought to have known or anticipate a risk that the contravention would occur unless reasonable steps were taken to prevent it.[113] This implies a high degree of foreseeability when assessing harm.

Yet, there are no precise guidelines on how to define *ex-ante* harm. Thus, how wide a DPIA should speculate about threats and harms are still a grey area of data protection law. Moreover, how to categorise harm[114] and what features the data protection authorities would consider in a breach–harm constellation is still undefined.[115] Nevertheless, some provisions of the GDPR, including Recital 75,

[112] ICO, 'How do we a DPIA?' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/> accessed 12 December 2019.

[113] ICO, 'Data Protection Act 1998 Monetary Penalty Notice Dated 14 January 2013', 6. This breach involved the infiltration of the various online networks of the Sony group following several Distributed Denial of Service (DDoS) attacks that resulted in the attackers accessing the personal data of its customers such as customer names, email addresses, user account password, etc. While it was acknowledged that Sony made some effort to protect customer password, the ICO argued that the measure was not up to date, given the technical development at that time, and therefore not adequate to address the vulnerability of the system. The ICO identified that the nature of the breach is likely to cause 'substantial damage or substantial distress to the data subjects' involved in the breach. Substantial distress here arose, according to the ICO, as a result of the knowledge of the data subjects that their 'data has been or may have been accessed by third parties and could have been further disclosed […] exposing them to possible fraud.'

[114] There is no agreement on how to categorise harm. Arguably, the list of harms cannot be closed, as privacy violation could result in several forms of harms, many of which could even take several years to manifest. Calo, for example, argues that a clear majority of privacy harms fall into just two categories—subjective and objective harms. M. Ryan Calo (n101). Solove adopts a different approach; he categorises US law of data harm from two broad perspectives: the privacy harm and data breach harm. Solove (n 103). The CIPL on its part identifies three types of harm to individuals whose privacy rights are violated: tangible damage (e.g., bodily harm), intangible distress (e.g., reputational harm) and societal harm (e.g., loss of social trust). CIPL (13). The ICO's guide to the GDPR simply gave 'some examples of the harm caused by the loss or abuse of personal data' without categorising them. ICO, 'How to do a DPIA' (n112). See also ICO, 'Security' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/> accessed 12 December 2019.

[115] In the Sony breach, the ICO considered the following feature in determining the amount of the monetary penalty: Nature of the contravention; Effect of the contravention; Behavioural issues; Impact on the data controller. ICO, 'Data Protection Act 1998 Monetary Penalty Notice' (n 113)

comes to aid to an extent. This recital refers to harm in terms of physical, material or non-material damage (although what is non-material could be as broad as any human imagination could go).[116]

In conclusion, the whole discussion in this part illustrates the definitional challenges involving risk management in data protection. The question of what risk, threat and harm a DPIA is meant to assess is not yet clearly defined. Likewise, other risk dependencies such as data protection vulnerabilities and assets are not uniformly defined.[117] Much work still needs to be done in this regard, as well as to harmonise the vocabulary and methods of assessing these risks, threats, vulnerabilities and harms. This arguably is a prerequisite towards building a knowledge base in this area. Kuner et al.'s remarks that '[i]t is vital that risk management around data protection, while remaining flexible, not continues in the largely ad hoc, colloquial terms in which it has evolved today'[118] is a suitable suggestion towards achieving the desired goals.

1.2.3 Systematisation of Data Protection Risk Assessment

Although 'systematisation' is not a data protection principle, the GDPR promotes systematic and consistent application of its rules. This is evident from the provision of Article 10 of the GDPR, which requires a harmonised and equivalent level of data protection, despite national scope. It is also reflected in the consistency mechanism adopted by the supervisory authorities in issuing the blacklist and whitelist under Article 35 (4) and (5). All these features indicate the value of a systematic approach in implementing the rules of the Regulation.

The Law Dictionary defines a systematic approach as an 'approach that is methodical, repeatable and able to be learned by a step-by-step procedure'.[119]

7.

[116] The WP29 also notes the phenomenon of societal harm. WP29 (n 111).

[117] See conventional usage of these terms in risk management in Chapter Two.

[118] Kuner et al., 'Risk Management in Data Protection' (n 13) 96.

[119] The Law Dictionary 'What is Systematic Approach' <https://thelawdictionary.org/systematic-approach/> accessed 7 July 2019.

Elsewhere, it is regarded as 'a process used to determine the viability of a project or procedure based on the experiential application of clearly defined and repeatable steps and an evaluation of the outcomes.' [120] In essence, a systematic approach aims to 'identify the most efficient means to generate consistent, optimum results'.[121] The above definitions indicate that a systematic approach contributes to the consistency of a process, especially when such a process is susceptible to future repetition and evaluation. Therefore, adopting a systematic approach to conducting a risk assessment during a DPIA is essential to addressing the aforementioned contextual issues. In addition, several advantages could accrue from such an approach.

1. A systematic approach will assist in establishing a clear and logical structure for completing the task envisaged under Article 35 (7)(c) and Recital 76. This translates to achieving consistency, transparency, verifiability and repeatability of the risk assessment process.

2. A systematic approach will make risk explicit and easy to manage (in terms of operationalisation). Furthermore, it will assist in developing clear metrics (factors and criteria) for completing each step in the whole DPIA exercise and the actions to be performed in each process.

3. It will help to develop precise and harmonised procedure across the EU since the obligation to conduct a DPIA can have a cross-border effect.

4. It will also assist in developing precise vocabulary relating to core terms used around DPIA, such as risk, threat, vulnerabilities, harm, etc.

Several respondents recommendations in the EDPS survey point towards the need for a systematic approach to DPIA.[122] This solidifies the motivation of this study and its central argument that data protection risk assessment would benefit from clearly defined sequence and methods to align with the consistency objective of the GDPR.

[120] InvestorWords, 'Systematic Approach' <http://www.investorwords.com/19342/systematic_approach.html#ixzz5oEC7p62q> accessed 7 July 2019.

[121] Ibid.

[122] EDPS, 'EDPS Survey on Data Protection Impact Assessments under Article 39 of the Regulation' (n 39).

1.3 OBJECTIVES OF THE STUDY

This study aims to present a comprehensive introduction to data protection risk assessment in the context of a DPIA and identify key indicators that should be considered when systematically performing such an assessment. The outcome is to enhance the transparency tool associated with data protection law. More specific objectives are:

(a). To define and discuss how risk assessment can be conceptualised in the context of DPIA and how the dimensions may be evaluated and scoped using specific indicators.

(b). To propose and present a methodology for DPIA risk assessment process and illustrate how it may be carried out in practice with a use-case.

1.4 RESEARCH QUESTIONS AND HYPOTHESIS

The introduction of DPIA as a risk management tool under the GDPR has been positively received in many quarters. There is a prospect that it may change the attitude of assessing and managing data protection risks. To minimise risks, carrying out a DPIA does not only create an obligation but also offers an incentive to data controllers to spend scarce resources in a prioritised manner when treating the risks. This approach may potentially increase the overall level of data protection and security for high propriety areas and decrease social and financial costs arising from data protection violations and fines associated with such breaches.

The pertinent question is how this risk assessment should be modelled to be most effective, consistent and transparent. For example, since the risk assessment envisaged under Article 35 is *ex-ante,* what will be the scope of this risk identification, analysis and evaluation? Similarly, if the severity and likelihood of risk must be measured accurately, what yardstick for this measurement will create consistency, effectiveness, transparency and predictability in the DPIA framework? Against this backdrop, this dissertation seeks to answer the following questions:

i. What does risk assessment entail for the purpose of conducting an *ex-ante* DPIA?
ii. What key attributes or parameters should be considered when conducting a risk assessment during a DPIA?

These questions are to explore the **hypothesis** that a systematic approach to conducting a data protection risk assessment will enhance legal certainty and transparency and positively impact the overall outcome of a DPIA.

1.5 CONCEPTUAL FRAMEWORK

Assuming that a data controller must decide whether a proposed data processing operation poses a high risk or not, what is the right thing to do? What factors should be considered in this exercise, and should the approach be objectively or subjectively focused? These questions first raise a decisional problem, because any conclusion about the risk level may have consequences in terms of the mitigation plans, further consultation with the supervisory authority, and compliance in general. They also raise a methodological problem, because as popularly stated, 'to measure is to know', and an assessment will only be as good as the metrics employed.[123] Bräutigam suggests this point in his remarks that '[a]n assessment is only as good as the metrics employed. So, if the "privacy requirements" are unclear, the results will be less useful'.[124]

Assuming also that a data protection authority (DPA) has to review this DPIA, how should this authority judge whether the assessment is appropriate or not? If questions regarding methodology, transparency, scope, and factors considered in completing the assessment arise, what key indicators should the authority rely on in answering those questions? Ideally, the DPA ought to provide the reason for its judgement (at least for the sake of transparency). This reasoning ought to be as objective as possible to serve as precedent in the future, given that such opinion is authoritative.

Therefore, the conceptual framework of this study is built from the perspectives of a data controller and a supervisory authority. It is meant to answer the above questions, which bear both how data controllers measure the risks associated with their data processing operations and how the authorities should review it. This is important since, as noted earlier, evidence suggests that data controllers currently

[123] Bräutigam (n 31) 269.

[124] Ibid.

approach risk assessment differently. Many adopt a significantly subjective framework in this exercise. This breeds inconsistency, lack of repeatability and verifiability (a fact observed from available reports and templates on the subject). Discrepancies have also been found in the supervisory authorities' DPIA guidance documents concerning the methodology for the entire DPIA process and the risk assessment step in particular.

To fill these gaps, this study, therefore, conceptualises risk assessment as a systematic exercise that facilitates data controllers in identifying, analysing and evaluating the risk associated with their data processing operation. It further proposes an adaptation of a standard framework (ISO 31000:2018) to design this systematic process (which correspondingly divides risk assessment into three: risk identification, risk analysis and risk evaluation).[125] The GDPR's non-exhaustive metrics for assessing risk, such as the nature, scope, context and purpose of processing, shall be relied upon to populate this framework and suggest parameters for completing each risk assessment process using a multiple attribute approach. This approach allows the use of both subjective and objective elements during a risk assessment. Furthermore, the doctrine of foreseeability[126] shall be explored to scope the range of foresight required in the risk assessment exercise. The application of this doctrine shall play a role in guiding data controllers and processors to identify and mitigate those risks which are reasonably foreseeable (through consultations, scientific evidence, historical data, industrial practice, expert knowledge, etc.). Finally, this approach gives meaning to the requirement of the GDPR that risk should be objectively assessed, which means that the risk assessor is expected to consider risks that a reasonable man would have foreseen, given the context of the proposed data processing.

This conceptual framework is diagrammatically shown in Figure 2 below.

[125] ISO 31000:2018 Risk Management — Guidelines.

[126] Meiring de Villiers, 'Foreseeability Decoded' (2015) 16:1 Minnesota Journal of Law, Science & Technology, 355. The doctrine of foreseeability is popularly considered in negligence cases, presupposing that "the degree to which a defendant could foresee the consequences of a wrongful act is a factor in assigning blameworthiness and moral responsibility for any harmful consequences".

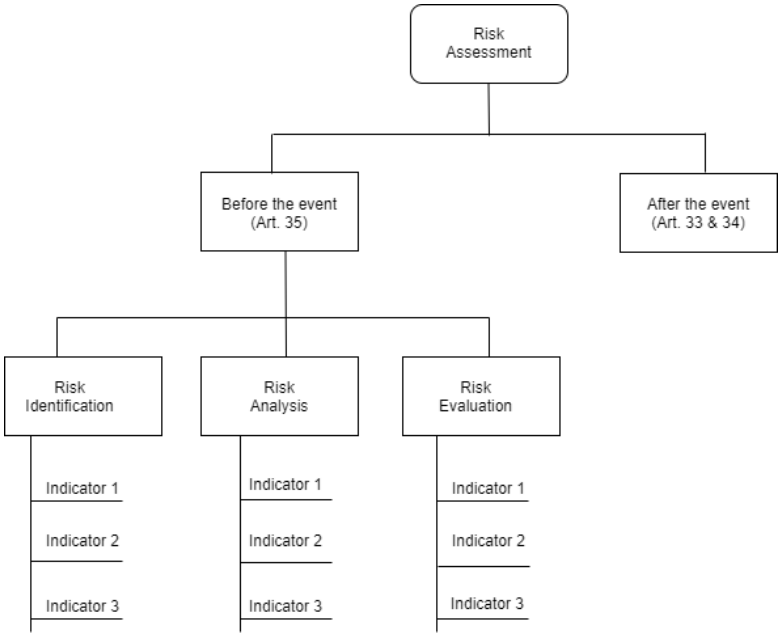


Figure 4: A conceptual framework for GDPR's Article 35 risk assessment

From the diagram above, each risk aassessment process is focused on particular aspects, and several parameters or attributes are considered (represented as indicators) to show transparency in the process. For example, in identifying the risks, the relevant indicators (developed from nature, scope, context and purpose of data processing as indicated by the GDPR) can be used to identify the threats, vulnerabilities and harms associated with the processing. The aim here is to ensure that relevant aspects that would affect the assessment outcome have been addressed for maximum impact.

While the data controller must assess the risk posed by their data processing operations, there is a tacit role of the supervisory authorities in ensuring the consistent application of the GDPR, which requires them to issue guidance on how to carry out a DPIA. As such, guidelines from the DPA ought to explain the risk assessment processes and relevant indicators to assist and make it clear to the data controller what to consider. It is also suggested that even when the supervisory authority decides to penalise a data controller or processor, the fact that an appropriate DPIA was conducted should be considered positively in setting the sanction value or level. It then follows that conducting a rational DPIA is more valuable. When these indicators are exposed beforehand, a rational data controller would prefer to carry out the risk assessment based on indicators that would

produce the most valid assessment, given the substantial consequences of not complying with this obligation.[127]

In the end, with the help of normative guidelines issued by the supervisory authority, which provide the steps and indicators for conducting a risk assessment, among the other processes of the DPIA, a level of transparency will be achieved. Furthermore, this approach will support the data subjects and the DPAs in exercising control because they have contributed to shaping the risk assessment in appropriate cases. They will also be able to evaluate and review the metrics used by data controllers to proactively assess and implement measures to mitigate risks posed by their operations.[128]

1.6 METHODOLOGY

This dissertation adopts a qualitative, descriptive doctrinal research method. Doctrinal research is a method of '[r]esearch which provides a systematic exposition of the rules governing a particular legal category, analyses the relationship between rules, explains areas of difficulty and, perhaps, predicts future developments.'[129] The doctrinal method is usually a two-part process: it involves first locating the sources of the law and then interpreting and analysing the text.[130] In the first step, this study determines the law creating the obligation to conduct a risk assessment before a feared risk event occurs in the course of personal data processing. In the second step, the provisions of the relevant laws are interpreted and analysed with the assistance of other primary and secondary sources on the subject.

[127] The assumption here is that the data controller is a rational decision-maker who would choose actions with the highest expected utility based on the principle of expected utility maximisation (EUM) when facing a situation of uncertainty. See Martin Peterson, *An Introduction to Decision Theory*, (Cambridge University Press 2009) 8; Katie Steele, and Orri Stefánsson, 'Decision Theory' in Edward Zalta (ed.), *The Stanford Encyclopedia of Philosophy* (Winter 2016 Edition) <https://plato.stanford.edu/archives/win2016/entries/decision-theory/> accessed 16 July 2019.

[128] See also CNIL, PIA Methodology (n 76) 2.

[129] Nigel Duncan, Terry Hutchinson, 'Defining and Describing What We Do: Doctrinal Legal Research' (2102) 17 (1) Deakin Law Review 83, 101.

[130] Ibid.

Primary data relied upon for this study include international treaties, EU primary and secondary law, national legislation, and judicial decisions. In addition, secondary materials were obtained from textbooks, journal articles, blogs, presentations, white papers, guidelines, opinions, media reports, EU reports, privacy policies, and other relevant publications on the topic under study.[131] For conducting the literature review and interpreting the above sources, a set of models were developed as a guide for sourcing and categorising the relevant literature. Three categories of publications were identified. The first consists primarily of publications that looked at privacy or data protection risks. The second are those that examined the impact assessment of such risks using a risk management tool such as PIA or DPIA. The third group represents guidelines from the authorities and institutions on carrying out a PIA/DPIA.[132]

1.7 SIGNIFICANCE AND JUSTIFICATION OF THE STUDY

Understanding how to systematically identify, analyse and evaluate risks associated with the processing of personal data risks *ex-ante* is vital for effective implementation of the risk-based approach emphasised in the GDPR. Currently, there is no agreement on the methodology for executing this risk assessment within the EU privacy community, and existing DPIA guidelines and templates have articulated divergent components and processes. Moreover, emerging open-source and commercially available tools for automating PIA/DPIA processes contain 'black boxes'. It is difficult to understand the algorithm these tools are built on and the theoretical framework behind their assessment techniques.

From both theoretical and practical view, a more systematic and consistent approach to conducting a DPIA in general and risk assessment, in particular is important because of the technical character of the obligation, compliance purpose

[131] Several research tools were relied upon for sourcing the materials used for this study including: Google search engine; Google Scholars, Leibniz Universität library and online resources, Taylor & Francis Online database, Oxford Journal of International Privacy Law, HeinOnline, the official websites of EU DPAs and Article 29 Working Party (now EDPB), Blog posts from the Hunton and Williams' Privacy and Information Security Law Blog, the d.pia.law policy briefs, activeMind.legal website, the PIA Watch.

[132] The following keywords were used for searching materials: Privacy Impact Assessment; Data Protection Impact Assessment; Privacy Risks, Data Protection Risks; Privacy Risk Assessment Methodology; Data Protection Risk Assessment Methodology.

and practical usefulness in day-to-day data protection and management. Given these shortcomings aforementioned and the reality that the GDPR requires risk to be assessed objectively, there is a need to overcome the polarization and uncertainty caused by the current state of affairs. Therefore, research is necessary to create a more systematic and consistent approach to conducting a DPIA in general and risk assessment, which represent the core aspect of the whole exercise. Exploring the possibility of developing such a uniform, consistent and concrete strategy for risk assessment, based upon a theoretical foundation, will be the contribution of this dissertation. It is hoped that such a systematic method will be of value to the privacy community at large. Thus, data controllers and processors who are obligated to carry out a DPIA will potentially benefit from this research. Furthermore, it will address their desire for practical advice for conducting impacts assessments. The study will also be helpful to supervisory authorities in their future work on DPIA, particularly when reviewing a DPIA, following consultation under Article 36 GDPR, and in their aim to ensure consistent implementation of the GDPR.

1.8 LIMITATIONS OF THE STUDY

Although this study presents a detailed view of the process of data protection risk assessment, it is also important to point out some of the limitations encountered during the conduct of the research. First, the language of this study is English; however, there is numerous rich literature on European data protection law concerning the subject matter in other languages. The examples of guidelines in Table 2 (Chapter Four) attest to this point. Second, some documents have been read in translated versions, which does not necessarily involve official translations or certified translators. Thus, there is a possibility of some errors or loss of meaning in translation. Furthermore, it is also possible that some statements on DPIA from the national authorities which do not qualify as 'guidelines' may not have been captured in the search results due to the language and technical barriers.

Another limitation witnessed in this study is the relative absence of European case law in DPIA or data protection risk management. Given that DPIA is relatively new in the European data protection law, this situation is to be expected. However, such legal pronouncement would have afforded an insight into how the courts

value *ex-ante* risk assessment. Finally, the proposed methodology of this study could be said to be a proof of concept yet to be validated by competent authorities. This lack of validation may make some data controllers hesitant in adopting it. However, a further study is suggested to incorporate a validation stage where the output of this study will be presented to relevant stakeholders, including supervisory authorities, for their comments. Despite these limitations, the study made use as far as possible of available materials and extrapolations where necessary.

1.9 CONCLUSION

The lack of precise methodology for conducting a DPIA that considered the conventional risk management tools and how they should apply in the area of data protection has a direct negative effect on how risk assessment is carried out during a DPIA. This has resulted in a lack of systematic manner of conceptualising and conducting a risk assessment. In several cases, the parameters for risk identification and assessing the likelihood and severity of risk that culminate to the risk level are unclear. This problem is compounded by the lack of standard terminology in defining the data protection risk, harm, threat and associated terms. Solving these issues will go a long way in enhancing the effectiveness of DPIA and its value as a tool for managing the risk associated with personal data processing.

In a broader context, the place of DPIA in the whole equation of data protection sanction and liability regime is not clearly defined. While on the one hand, the strict liability feature of the liability regime vis-à-vis the data subjects, data controllers and processors makes it less attractive to consider DPIA once an infringement of the GDPR results to harm to the data subject, it is unclear, on the other hand, whether a well-defined and conducted DPIA will affect the fines issued by the supervisory authorities in the case of a data breach. This study has suggested that it should positively affect such penalties from the supervisory authorities to incentivise conducting a well-designed DPIA. However, we await future decisions and further developments in this area, as no such cases have cropped up since the adoption of the GDPR.

Having contextualised these issues in this introductory chapter, the next chapter shall provide a bigger picture to the focus of this study by taking a historical look

at the developments around the notions of risk, privacy, and data protection to establish the study's theoretical framework.

CHAPTER TWO

2. HISTORICAL DEVELOPMENTS AND THEORETICAL FRAMEWORK

'Ultimately, the wish to have privacy must be in our hearts, not only in our laws.'

Ruth Gavison

2.1 INTRODUCTION

The previous chapter provided a background to the study that culminated in the research questions to be addressed. It set the scene for understanding the problems around DPIA under EU data protection law. This chapter shall present a bigger picture of the context of this study, providing the historical developments around the notions of risk, privacy and data protection. It shall trace how European data protection law came up as a measure against the risks to informational privacy due to technological developments from the 1960s. This presentation is pertinent to appreciate the need for a systematic and transparent approach in conducting DPIA. It goes to the heart of the theory of data protection propounded by De Hert and Gutwirth. The theoretical framework presented in this chapter aims to buttress how transparency and consistency can be achieved in the DPIA framework.

2.2 THE NOTION OF RISK AND ITS MANAGEMENT

The notion of risk and its management have a history as old as society and civilisation.[133] Luhmann writes that the etymology of the word is unknown;[134] however, there are several accounts of how different communities conceptualise and mitigate risk. For example, one source writes that around 3200 BC, a particular Babylonian group called Asipu was usually consulted in risky, uncertain,

[133] Peter Bernstein, *Against the Gods: The Remarkable Story of Risk* (John Wiley and Sons Inc 1996).

[134] Niklas Luhmann, *Risk: A Sociological Theory* (De Gruyter 1993) 9.

or difficult situations. As a result, they could analyse a problem and propose actions for people.[135] A variety of prescriptions about risk have been noted in historical documents such as the Code of Hammurabi around 1700 BC.[136] However, Frey, Mccormick and Rosa suggest that the early foundations of the classical idea of risk are traceable to classical Greece.[137] Urbanisation and industrialisation, and technological advancements such as nuclear technology (which became widely available after the Second World War), Beck argue, mostly shaped the modern understanding of the concept of risk.[138] Luhmann[139] and Douglas[140] have also echoed this sociological construct of risk.

These accounts are diverse, and there is no consensus regarding the definition of the term 'risk' from them. Risk is also often confused or interchanged with other words such as 'danger'.[141] The difficulty in defining risk precisely has been lamented by authors, as may be seen in the following remarks by Kaplan:

> Many of you here remember that when our Society for Risk Analysis was brand new, one of the first things it did was to establish a committee to define the word "risk". This committee labored for 4 years and then gave up, saying in its final report, that maybe it's better not to define risk. Let each author define it in his own way, only please each should explain clearly what that way is.[142]

---

[135] R. Scott Frey, Sabrina Mccormick and Eugene Rosa, 'The Sociology of Risk' in Clifton Bryant and Dennis Peck (ed) *21st Century Sociology: A Reference Handbook*. (SAGE Publications 2006) 81.

[136] Ibid.

[137] Ibid.

[138] Ulrich Beck, *Risk Society: Towards a New Modernity* (Sage Publications 1986); see also Anthony Giddens, 'Risk and Responsibility' (1990) 62 (1) The Modern Law Review.

[139] Luhmann (n 134).

[140] Mary Douglas, *Purity and danger: An analysis of the concepts of pollution and taboo* (Routledge 1966).

[141] For a distinction between risk and danger, see Maximilian von Grafenstein, The Principle of Purpose Limitation in Data Protection Laws: The Risk-based Approach, Principles, and Private Standards as Elements forRegulating Innovation (Nomos Verlagsgesellschaft mbH. 2018) 82-90; Werner Heun, 'Risk Management by Government and the Constitution' in Gunnar Duttge, Sang Won Lee (Eds.), The Law in the Information and Risk Society (Universitätsverlag Göttingen 2011) 15-29.

[142] Stan Kaplan, 'The Words of Risk Analysis' (1997) 17(4) *Risk Analysis* 407.

Given such difficulty, it is of little surprise that the Society for Risk Analysis (SRA) gave multiple definitions of risk.[143] Many other sources have equally approached risk's definition substantially differently. The concept of risk has also been studied and explained through several disciplinary perspectives, such as sociology, economics, mathematics, physical and health sciences, law, among others. Each field, though, tends to define risk to suit its purposes. Equally remarkable is that significant accidents and disasters, such as the Three Mile Island nuclear accident in the United States in 1979 and the Chernobyl nuclear disaster in the former Soviet Union in 1986, has galvanised risk research involving a multi-disciplinary approach. Today, advances in ICTs seem to have reawakened the societal interest in risk, especially those resulting from developments and applications of information technologies.[144]

As already alluded to, risk perception differs, and inconsistency is rife in the vocabulary used to express its notions. One suggestion for understanding the notion, both technical and non-technical, is to contextualise risk.[145] Alberts, for example, sees context as one of the core elements of risk and writes: '[w]ithout setting an appropriate context, you cannot definitively determine which actions, conditions, and consequences to include in risk analysis and management activities.'[146] This suggestion is pertinent here, and attempts shall be made to define risk from a conventional to a more specific legal context and identify risk dependencies.

[143] Committee on Foundations of Risk Analysis, 'Society for Risk Analysis Glossary' (Approved June 22, 2015) 5.

[144] For example, there has been debate whether mobile phone present the risk of cancer emanating from radiation and how such risk could be avoided. See, National Cancer Institute, 'Cell Phones and the Cancer Risk' <https://www.cancer.gov/about-cancer/causes-prevention/risk/radiation/cell-phones-fact-sheet> accessed 11 July 2019.

[145] See Christopher Alberts, 'Common Elements of Risk' (Technical Note CMU/SEI-2006-TN-014) <https://resources.sei.cmu.edu/asset_files/TechnicalNote/2006_004_001_14687.pdf> accessed 12 July 2019; Mark Talabis, Jason Martin and Evan Wheeler (eds), *Information Security Risk Assessment Toolkit* (Elsevier, 2013) 3.

[146] Alberts, ibid, 6.

2.2.1 Defining Risk

In its day-to-day usage, risk often refers to a situation 'in which it is possible but not certain that some undesirable event will occur.'[147] However, in some contexts, 'risk' is associated with a positive outcome.[148] Thus, specific components and central attributes that are given to those components by authors are used to classify risk over the years. For example, Sayers et al. define risk with two prominent components in mind:

> Risk is a combination of the chance of a particular event, with the impact that the event would cause if it occurred. Risk, therefore, has two components – the chance (or probability) of an event occurring and the impact (or consequence) associated with that event. The consequence of an event may be either desirable or undesirable.[149]

This definition attributes a central role to the components of probability and consequence, an approach to defining risk that appears to be popular nowadays. This two-component definition is often represented in a mathematical equation as R(E) = p(E) x (D),[150] or Risk = Probability × Consequence.[151] Other definitions with more components exist: The Business Dictionary, for example, defines risk as '[a] probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through pre-emptive action'.[152] Here, four risk elements are prominent:

---

[147] Ove Hansson, 'Risk', in Edward Zalta (ed.), The Stanford Encyclopedia of Philosophy (Fall 2018 Edition) <https://plato.stanford.edu/archives/fall2018/entries/risk/> accessed 11 July 2019.

[148] See Jack Jones, 'What about "Positive Risk"? – Part' (30 November 2019) <https://www.fairinstitute.org/blog/what-about-positive-risk-part-1> accessed 28 August 2019; David Dunkelberger, 'Enterprise Risk Management [Part III]: 5 Examples of Positive Risk (17 July 2018) <https://www.ispartnersllc.com/blog/erm-5-examples-of-positive-risk/> accessed 28 August 2019.

[149] Sayers et al, Risk, Performance and Uncertainty in Flood and Coastal Defence – A Review (R&D Technical Report FD2302/TR1, 2003) xvi.

[150] Where p(E) represents the probability of a dangerous event, while (D) represents the amount of the expected damage. See Alfons Bora, 'Risk, risk society, risk behavior, and social problems' in G. Ritzer (Ed.), *The Blackwell Encyclopedia of Sociology* (Vol. 8, Blackwell Publishing, 2007).

[151] Sayers (n 145); see also Jones, 'An Introduction to Factor Analysis' (n 84) 8.

[152] Business Dictionary 'Risk' <http://www.businessdictionary.com/definition/risk.html> access 12 July 2019.

probability, the threat of harm, vulnerability, and mitigation. A glossary of qualitative definitions of risk according to the SRA exposes even more components.[153]

From a conceptual perspective, the notion of risk has a futuristic nature; most times, a risk assessment is carried out for making informed decisions about a future occurrence. This point could be bolstered by Kaplan and Garrick's conception of risk as a 'set of triplets idea' hinged on answers to three fundamental questions: (1) What could go wrong? (2) What is the likelihood of that happening? (3) What are the consequences?[154] Such characterisation is relevant for risk assessment, although there is usually a limitation of 'epistemic credibility' in answering these questions since 'some risk issues refer to possible dangers that we know very little about'.[155] Researchers have though attempted to develop several risk management tools to remedy this knowledge gap and suggest models for identifying, assessing and mitigating risks before they happen (although post-event risk assessment is also conducted in many cases).

A structured approach to answering the questions above is within the domain of risk assessment. As Rausand notes, to answer the first question of what could go wrong, a risk assessor must first identify the possible hazardous or threat events that may cause harm to the assets that are to be protected (data, humans, equipment, etc.).[156] Regarding the second question of likelihood, a qualitative or quantitative approach or both could be used to consider each of the events identified from the first question. Causal analysis is performed here to identify the underlying causes of the hazards or threats events. Finally, identifying the potential harm or adverse impacts on the assets is required to answer the third question

[153] Committee on Foundations of Risk Analysis, 'SRA Glossary' (22 June 2015) 3 <http://www.sra.org/sites/default/files/pdf/SRA-glossary-approved22june2015-x.pdf> accessed 14 July 2019.

[154] Stanley Kaplan and B. John Garrick, 'On the Quantitative Definition of Risk' (1981) 1:1 Risk Analysis.

[155] Sven Hansson, 'A Panorama of the Philosophy of Risk' in Sabine Roeser et al (eds.), *Handbook of Risk Theory* (Springer 2012) 34

[156] Marvin Rausand, *Risk Assessment Theory, Methods, and Applications* (John Wiley and Sons 2011) 5.

about the weight of consequences. Mitigation or prevention mechanisms and their ability to function when the threat events occur is essential to consider at this stage too.[157] Various risk management models and tools have been developed around this cluster to define the relationship between the identified threat events in question 1, and the analytical processes used to answer questions 2 and 3.[158]

It is important to note that in some circumstances, risk has a specific contextual definition. In some contexts, it can assume definite meaning and be assessed in conjunction with clearly identified hazards, such as the levels of chemical toxicity.[159] As a juridical term, Heun defines risk 'as a product of the extent of the expected [legal] damage and the probability of its occurrence.'[160] While this definition is coated with the two-component attribution seen earlier, Heun further relied on the degree of probability to distinguish between 'danger' and 'risk'.[161] However, a more specific and contemporary understanding of 'legal risk' is in terms of an entity's exposure to a legal dispute, which could result in sanctions. Spacey defines a legal risk in this context as 'the potential for losses due to regulatory or legal action'.[162] He further identifies several types of legal risk, such as regulatory risk, compliance risk, contractual risk, among others. Compliance risk, for example,

[157] Ibid.

[158] Ibid; see also UK National Cyber Security Centre, 'Guidance Summary of Risk Methods and Frameworks' (23 September 2016) <https://webarchive.nationalarchives.gov.uk/20170307014628/>; NCSC, 'Risk Management Guidance' <https://www.ncsc.gov.uk/guidance/summary-risk-methods-and-frameworks>; ENISA, 'Risk Management / Risk Assessment Standards' <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards>; ENISA, 'Inventory of Risk Management / Risk Assessment Tools' <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools> all websites accessed 22 December 2019.

[159] For example, carbon monoxide level of above 70 ppm is considered risk to human health. See United States Consumer Product Safety Commission, 'Carbon-Monoxide-Questions-and-Answers' <https://www.cpsc.gov/Safety-Education/Safety-Education-Centers/Carbon-Monoxide-Information-Center/Carbon-Monoxide-Questions-and-Answers> accessed 14 May 2019.

[160] Werner Heun, 'Risk Management by Government and the Constitution' in Gunnar Duttge and Sang Won Lee (Eds.), *The Law in the Information and Risk Society* (Universitätsverlag Göttingen 2011) 17.

[161] He explains that the probability is higher in situations of imminent danger. Ibid.

[162] John Spacey, 'What is Legal Risk' (Simplicable, 24 August 2015) <https://simplicable.com/new/legal-risk> 16 November 2019.

refers to the 'potential for fines and penalties to an organisation that fails to comply with laws and regulations.'[163] The GDPR, for instance, has imposed several obligations on data controllers and processors and provides that any data subject who suffers damage as a result of a violation of this regulation can recover compensation from such parties.[164] Also, the supervisory authorities can impose fines on data controllers and processors for breaching these obligations, all of which present compliance risks to data controllers or processors.[165] It could also be tagged an operational risk, which includes regulatory risk.[166] In a nutshell, the instrument of legal sanctions is one of the ways of addressing the risks associated with data processing; it is a way of ensuring compliance with data protection rules.

Having looked at the meaning of risk, it is essential to note that risk is contextual and depends on interaction with certain elements such as assets, vulnerabilities, threats, etc. In the following section, some of these risk dependencies shall be introduced briefly to enhance our understanding of risk.

2.2.2 Risk Dependencies

As indicated earlier, risk assessment is contextual. Risk depends on certain elements to materialise, such as an asset, vulnerabilities, threats, and controls. Let us briefly define these concepts.

2.2.2.1 Assets

In risk management, asset refers to anything that is considered of value, which needs to be protected for specific objectives. The US National Institute of Standards and Technology (NIST) defines it as "an item of value to

[163] Ibid.

[164] See GDPR, art 82.

[165] See GDPR, art 83.

[166] Article 13 (33) of Directive 2009/138/EC (the Solvency II Directive) defines operational risk as 'the risk of loss arising from inadequate or failed internal processes, personnel or systems, or from external events.' This includes regulatory risk of which the Enterprise Risk Management Academy (ERMA) ranked privacy and data security risk as the 2nd top regulatory and litigation risk in 2018. ERMA, 'Top 4 Regulatory and Litigation Risks in 2018' (*ERMA,* 2018) <https://erm-academy.org/sites/default/files/Top%204%20Regulatory%20and%20Litigation%20Risks%20in%202018.png> accessed 20 February 2019.

stakeholders."[167] An asset comes in diverse forms; it may be tangible in physical appearances, such as computers, hardware, software, physical infrastructure, etc. or intangible such as information, databases, data, operational or critical data, reputation, intellectual property etc. Under the GDPR, asset primarily relates to the personal data as defined in Article 4. The value and criticality of an asset is a major factor in determining the level of protection it requires.

2.2.2.2 Vulnerabilities

Vulnerability refers to weaknesses that could be exploited and could result in exposure or damage to the asset. In general, it is defined as "intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence." [168] In the context of information systems and management, vulnerabilities are seen as "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source." [169] Such weaknesses include unencrypted data, weak passwords, outdated operating systems, bugs in software, human error, ineffective controls, etc.

2.2.2.3 Threats

Threat refers to something, someone or circumstance with the potential to exploit a vulnerability with respect to an asset.[170] Such an exploit can harm the assets. Examples here include hackers, cybercriminals, natural disasters, competitors, etc. Over the years, threat actors in information security risk management have expanded to include: persons, organisations, government. Similarly, their motivations now span from publicity to financial gain. These actors also possess various capabilities and tools to exploit vulnerabilities from any part of the globe. In the light of this, threats to personal data are enormous since information

---

[167] Ron Ross, et. al, 'Developing Cyber Rsilient Systems: A Systems Security Engineering Approach', NIST Special Publication 800-160 Volume 2 (NIST 2019) 1 <https://doi.org/10.6028/NIST.SP.800-160v2> accessed 20 September 2021.

[168] ISO Guide 73: 2009, 8.

[169] NIST Computer Security Resource Centre Glossary <https://csrc.nist.gov/glossary/term/vulnerability> accessed 20 September 2021.

[170] Ibid, < https://csrc.nist.gov/glossary/term/threat> accessed 20 September 2021.

systems used to process such data are increasingly susceptible to multifarious threats and attacks from several adversaries including through the supply chain.

2.2.2.4 Controls

Controls refer to measures that are applied to modify risk.[171] Controls mostly target vulnerabilities and threats to eliminate, modify or reduce them. As a measure of risk modification, controls include policies, procedures, guidelines, practices, or organisational measures of varying nature such as administrative, technical, management, or legal nature.[172] These controls span from those aiming at detecting the risk to preventing it, as well as corrective and recovery controls.

In summary, several definitions assume risk as a product of a threat exploiting a vulnerability to impact an asset, despite controls. In modern times, control not only target dissuading or preventing risks but also recovery assuming risk eventually occurs. Thus, risk and its management are not static; they involve a continuous monitoring process so that these dependencies are always in check. In the following sections, the regulatory approach to privacy risk management shall be focused on to understand how legal systems have tried to mitigate risk to the right to informational privacy.

2.3 REGULATORY APPROACH TO PRIVACY RISK MANAGEMENT

Legislative instruments have often provided a normative basis for regulating risks of various kinds, from road accidents to cybersecurity. This is visible in certain areas of public law, such as environmental protection law, public health law, critical infrastructure protection law, etc. Several approaches to regulating risk have emerged from these instruments, ranging from the obligation on the risk creator to obtain insurance, to undertaking a proactive *ex-ante* risk assessment of the proposed project.[173] For instance, in environmental law, the use of Environmental

[171] ISO Guide 73: 2009, 10.

[172] NIST Computer Security Resource Centre Glossary <https://csrc.nist.gov/glossary/term/control> accessed 20 September 2021.

[173] See Jonathan Nash, 'Law and Risk', in James Wright (ed), *International Encyclopedia of the social and Behavioral Sciences* (2nd Ed, Vol. 13 2015).

Impact Assessment has crystallised as a regulatory requirement for projects that affect the environment, such as oil drilling, nuclear plant construction, fracking, etc.[174] The responsible entity is required, as a precautionary measure, to undertake a risk assessment and put in place measures to address the identified risks before engaging in such projects. This way, arguably, the law serves as a risk management instrument; it provides the framework for mitigating societal risk exposure.

Over time, this regulatory approach to risk has been extended to the area of information technology (IT).[175] Terms such as 'technology risk assessment' and 'technology impact assessment' capture this extension. Here, information technology developers are required to assess the risk of their products to society. One crucial aspect of IT risk is the privacy of individuals who use IT products and/or whose data are processed with IT systems. As will be shown later, this technological risk perception prompted various data protection laws in Europe and elsewhere. This point has been rightly noted by Raab and Bennett when they write that: '[...] the concept of risk pervades data protection regulations and rhetoric and serves as a rationale for the design of protective devices, be they rules, codes of practice, standards, or privacy-enhancing technologies.'[176] Perri 6's observation that the concept of privacy has severally been advanced as a claim for protection against a series of risks equally ties in with this assertion.[177]

As we shall see in the following sections, this idea of risk management galvanised the development of informational privacy right or data protection (as popularly known in Europe). Before going into details regarding the rise of data protection law in Europe, the next section shall look at the historical landscape of the concept of privacy, being an umbrella term with a multi-dimensional feature within which the subject matter of this study is located.

---

[174] See Tseming Yang, 'The Emergence of the Environmental Impact Assessment Duty as a Global Legal Norm and General Principle of Law' (2019) 70 Hasting Law Journal 525.

[175] Rinie van Est, Bart Walhout and Frans Brom, 'Risk and Technology Assessment' in Sabine Roeser et al (eds), *Handbook of Risk Theory* (Springer 2012) 1069-89.

[176] Charles Raab and Colin Bennett, 'The Distribution of Privacy Risks: Who Needs Protection?' (1998) 14 The Information Society 263.

[177] Perri 6, *The future of privacy Volume 1 Private life and public policy* (Demos 1998) 34.

2.3.1 The Notion of Privacy: A Historical Background

As we use the term today, privacy assumes more than one interpretation, mainly, as each individual or group may hold different expectations of what constitutes privacy or its invasion.[178] However, several authors have tried to define the concept and demarcate its dimensions without consensus on this front. While it is uncontested that the notion of privacy is deeply rooted in history, it remains challenging to pinpoint any universally accepted single source of its historical origin. Literature, instead, suggests numerous entry points through which the idea of what we regard today as privacy could be traced. Citing the biblical story of Adam and Eve, for instance, Konvitz brings a religious dimension to the discussion. 'Thus', he writes, 'mythically, we have been taught that our very knowledge of good and evil—our moral nature, our nature as men—is somehow, by divine ordinance, linked with a sense and a realm of privacy.'[179] This 'divine origin' ties in nicely with the argument of some philosophers who believe that human beings have an instinctual desire for privacy. As such, the notion of privacy should be understood as a natural right that every man should enjoy in line with natural law.[180] As Cobb J pointed out in *Pavesich v New England Life Insurance Co*, '[t]he right of privacy has its foundation in the instincts of nature […] A right of privacy in matters purely private is therefore derived from natural law.'[181]

---

[178] Adam Moore, 'Defining Privacy' (2008) 39:3 Journal of Social Philosouphy 411. See also Iheanyi Nwankwo, 'Information Privacy in Nigeria' in Alex Makulilo (ed), *African Data Privacy Laws* (Springer 2016) 47.

[179] Milton Konvitz, 'Privacy and the Law: A Philosophical Prelude' (1996) 31 LCP 272.

[180] See Glenn Negley, 'Philosophical Views on the Value of Privacy' (1966) 31 LCP 319, 325. In a broad sense, this falls under the natural law theory. Proponents of this theory assert that the moral standards that govern human behaviour are, in some sense, objectively derived from the nature of human beings and the nature of the world. They also assert that the authority of legal standards necessarily derives, at least in part, from considerations of the moral merit of those standards. See Kenneth Himma, 'Natural Law' (IEP) <http://www.iep.utm.edu/natlaw/>; Jstor, 'Natural Law' (Jstor) <https://www.jstor.org/topic/natural-law/?refreqid=excelsior%3A9a2f84b2ca3603c2e62e1d04b0873b8a>; Thomas Aquinas, *Summa Theologica* (ST I-II, Q.94, A.II, 1947) <http://www.sacred-texts.com/chr/aquinas/summa/>; Joseph Magee, 'St. Thomas Aquinas on the Natural Law' (*Acquinasonline,* last updated 5 February 2015) <http://www.aquinasonline.com/Topics/natlaw.html>; Thomas Aquinas 'Of Human Law' (ST I-II, Q.95, A.II, 1947) <http://www.sacred-texts.com/chr/aquinas/summa/sum233.htm>; William Blackstone, 'Commentaries on the Laws of England (1765-1769)' <http://lonang.com/library/reference/blackstone-commentaries-law-england/bla-002/> all webstites accessed 23 January 2019; Lon Fuller, *The Morality of Law* (Yale University Press 1964).

[181] *Pavesich v New England Life Insurance Co* (Ga. 1905) 50 S.E. 68.

There are, though, several other ancient demographic traces of privacy's origins. In a study of the socio-cultural perspective of privacy, Moore cites examples of the Greek, the Hebrew, and the Chinese societies to show how several traditional societies viewed privacy at different times.[182] Such an approach offers a more nuanced way of understanding how ancient and modern notions of privacy evolved. However, despite this demographic approach, literature regarding privacy's evolution usually contains a narrative on the influence of the demarcation between the public and the private spheres of life. Authors have relied on this narrative to explain 'that there is a sphere of space that has not been dedicated to public use or control'.[183] As Mill puts it, 'there is a part of the life of every person […], within which the individuality of that person ought to reign uncontrolled either by any other individual or by the public collectively.'[184] Konvitz reinforces this idea in the following remarks, '[t]o mark off the limits of the public and the private realms is an activity that began with man himself and is one that will never end; for it is an activity that touches the very nature of man'.[185]

Notably, not all societies have developed this notion of the public-private sphere on an equal level. The ancient Greek society, as Moore indicates, had a more visible boundary of what is public and private, and had developed some notions around it relating to how individuals are protected in their private sphere.[186] Aristotle's distinction between the *'polis'* (public) and the *'oikos'* (private) attests to this assumption, where citizens' public governance collectively reflects the public sphere. In contrast, the private sphere covers the household governance within the domestic and family life.[187] By contrast, in the ancient Hebrew society, for

<http://faculty.uml.edu/sgallagher/pavesich_v.htm> accessed 12 January 2019.

[182] Barrington Moore, *Privacy Studies in Social and Cultural History* (M.E Sharpe Inc 1984).

[183] Konvitz, (n 179) 279-280.

[184] John Stuart Mill, *Principles of Political Economy*, Book V, Chapter XI 2, <http://www.econlib.org/library/Mill/mlP73.html> accessed 23 June 2016.

[185] Konvitz, (n 179) 274.

[186] Moore, *Privacy Studies in Social and Cultural History* (n 182).

[187] Aristotle, *Politics: A Treaties on Government* (English version by the Project Gutenberg) <http://www.gutenberg.org/files/6762/6762-h/6762-h.htm> accessed 20 June 2016. This

instance, a person's daily life was circumscribed by religious tenets in which the 'eye' of God left little or no room for autonomous individual existence.[188] In some cases, even where the demarcation could be cited, it did not always generate ideas of 'individual' protection (e.g., in ancient China).[189]

It is equally notable that it is sometimes difficult to distinguish between the public and the private spheres clearly. This point is highlighted in Gleeson CJ's remark that:

> There is no bright-line which can be drawn between what is private and what is not. Use of the term 'public' is often a convenient method of contrast, but there is a large area in between what is necessarily public and what is necessarily private.[190]

Thus, it is no surprise that many societies have distinct approaches to privacy.[191] In most African traditional societies, for example, where social cohesion and communal living take priority over individuality, agitation for western-style individual privacy was primarily unknown.[192] Marcus also notes that Muslim societies in the Middle East enjoy a reputation for attitudes and conducts especially protective of private life, such as strict dress code, high walls and enclosed courtyards of houses, elaborate restrictions on relations between the sexes and some other private spheres immune from public observation and unlicensed contact.[193] Nevertheless, evidence suggests that people in these communities

---

arrangement has a democratic implication in the governance structure: the polis does not intervene in the family life of citizens except in limited circumstances such as where children fail to support their parents; or in limited capacity in adultery cases; or where the King takes charge of orphans, pregnant widows and families about to become extinct. See Moore, Ibid, 135.

[188] Religion was above all things in the ancient Hebrew and humans could not hide anything from Yahweh (God) who is omniscient, omnipotent, and omnipresent. What was important for them was a distinction between holiness and defilement rather than public and private realms. Moore, ibid, 168-205.

[189] Moore, ibid, 35.

[190] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* [2001] HCA 63, para 42.

[191] See Joseph Cannataci (ed), *The Individual and Privacy* (Vol. 1, Ashgate Publishing 2015).

[192] Alex Makulilo (ed), *African Data Privacy Laws* (Springer 2016).

[193] Abraham Marcus, 'Privacy in Eighteenth-century Aleppo: The Limits of Cultural Ideals' in Joseph

readily make their personal and family information public.[194] Although it has survived centuries of discussion, the public-private sphere narrative does not account for all societal attitudes on privacy issues. Differences abound, suggestive that the time and space dimension is vital in any enquiry about privacy's roots.[195] Nevertheless, the private-public dichotomy, at least, offers a conceptual image to explain the notion of privacy rights and still appears relevant today.

Admittedly, in our present age, mass surveillance by public and private organisations has been facilitated by innovations in ICTs, particularly the Internet. Here it is apparent that those innovations have radically changed how individuals generate and share personal information on global reach (e.g. social networks). This marks a watershed era in the evolution of the concept of privacy. However, these innovations also permit governments, corporations and private persons to snoop on information within these social networks. In fact, in this digital sphere, the demarcation of private-public spheres seems ever more blurred. That this era has brought about a different culture and attitude to privacy is obvious. Many people, who share personal details online, appreciate the elements of risk associated with such dissemination; yet, most people in this 'information society' appear undeterred by this fact. They seem to share as much information online as possible, despite knowing that it is challenging to keep it private in such an online environment.[196] For the more enlightened ones, privacy here is shaped by one's

Cannataci (ed), *The Individual and Privacy* (Vol 1 Ashgate Publishing 2015).

[194] Ibid.

[195] As alluded to earlier, there are other historical entry points from where authors have investigated privacy. Perri 6, for example, outlines three themes: the rising demand for privacy because of the development of a culture of individualism; the rise of urbanism which eliminates the proximity and mutual involvement of people in agrarian societies; and the development of techniques for the collection, storage, selection, matching, analysis, disclosure and publication of information. He, however, admits that none of these themes is entirely compelling. Fallible as these themes may be though, many authors have narrated instances to suggest the evolution of privacy through them. Perri 6, *The Future of Privacy* (n 177). Furthermore, the transformation that occurred in the sixteenth Century Europe, recalls Dowding, meant that privacy was becoming an issue of personal individualism, noting that the architectural evolution of the upper-class houses allowed for more seclusion in England. Martin Dowding, *Privacy Defending an Illusion* (Scarecrow Press 2011).

[196] Simon Chandler, 'We're giving away more personal data than ever, despite growing risks' (*Venture Beat*, 24 February 2019) <https://venturebeat.com/2019/02/24/were-giving-away-more-personal-data-than-ever-despite-growing-risks/> accessed 28 June 2019. See also Daniel Solove, 'The Myth of the Privacy Paradox' (2020) GW Legal Studies Research Paper No. 2020-10.

ability to configure their privacy settings, hoping that those within their social circle would reciprocate such configuration.[197] This approach, though illusory, presents the notion of privacy with a new meaning among the so-called 'netizens'.[198]

Nevertheless, the transition from the ancient to modern notion of privacy has its ups and downs. On a positive note, a more open society has been facilitated due to the ability of individuals and corporate entities to process private and personal data to create values and possibilities that were hitherto exclusive for a few individuals. On the other hand, however, there is a consequence: the once-revered intimate and private sphere can no longer be maintained and controlled by individuals as they may wish. This tension has been a subject of both legal and academic contention over the years. Notably, as to how to conceptualise privacy right to maintain, on the one hand, the level of control required by the individual within his/her private domain, and on the other hand, not stifling innovative and public uses of data. The following section shall focus on how information technological advancements gave rise to data protection as a standalone right in Europe.

2.3.2 Rise of Data Protection Law in Europe

Significant attention was brought to legal protection of privacy in the US tort law following Warren and Brandeis warning of the threat to privacy by technology and call for a distinct legal recognition and protection of privacy.[199] The idea that privacy relates to a 'right to be let alone' (a phrase adopted from Judge Thomas Cooley) has been canvassed in their seminal article in 1890. They attempt to expose the threat to the individual's personality by technological developments of that time, particularly by the press. The authors explain privacy as protecting the 'inviolate personality' of an individual. This value allows humans to have peace of

[197] See Julian Hauser, 'The Evolution of the Concept of Privacy' (EDRi, 25 March 2015) <https://edri.org/evolution-concept-privacy/> accessed 23 June 2016.

[198] The Oxford Dictionary defines a Netizen as 'A user of the Internet, especially a habitual or keen one.' <https://en.oxforddictionaries.com/definition/netizen> accessed 24 February 2017.

[199] Warren, 'The Right to Privacy' (n 86).

mind and prevent publicity about them that they wish not to be made public. They wrote:

> Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-top'. [200]

In the presence of such threats, they argue that the legal system ought to recognise a free-standing right of inviolate personality because, strictly speaking, tort law does not focus on the intangible injuries resulting from privacy violations.[201] At times, they further argue, the injury that occurs when information about an individual's private life is made available to others goes to the very core of that individual's personality—'his estimate of himself.' This violation inflicts 'mental pain and distress, far greater than could be inflicted by mere bodily injury'. This threat of serious harm warrants a free-standing right to safeguard privacy in their view. The impact of Warren and Brandeis's work is felt till the present, although the limits of their conception of privacy are apparent today, considering that it is not in all cases that letting someone alone is the crux of privacy controversies. Sometimes, it is in respecting the legitimate expectations of the data subjects, even when they have allowed access to their private domain. Nevertheless, this theory has survived years of serious discussion and has been applied in several scenarios to advance the right to privacy. Moreover, it galvanised the movement towards informational privacy in other jurisdictions.

Other privacy conceptions have appeared over the years. [202] Nevertheless, this study shall not focus on analysing these various privacy conceptions. However, the

---

[200] Ibid, 195.

[201] Ibid, 196.

[202] See Daniel Solove, 'Conceptualizing Privacy' (2002) 90 California Law Review 1088; Kirsty Hughes 'A Behavioural Understanding of Privacy and its Implications for Privacy Law' (2012) 75:5 The Modern Law Review 806, 808-809; Ruth Gavison, 'Privacy and the Limits of Law' (1980) 89:3 The Yale Law Journal 421; Richard Posner, 'Privacy, Secrecy, and Reputation' (1978) 28 BUFF L REV 1, 11; see also Richard Posner, *The Economics of Justice* (Harvard University Press 1981); Charles Fried, 'Privacy' (1968) 77 Yale L.J. 475; Alan Westin, 'Privacy and Freedom' (1968) 25 Wash. & Lee L. Rev. 166; Anita Allen, 'Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm (2000) Faculty Scholarship Paper 790.; Paul Schwartz, 'Internet Privacy and the State', (2000) 32 CONN. L. REv. 815; Solon Barocas and Karen Levy 'Privacy Dependencies' (2019) Washington Law Review, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3447384> accessed 12 December 2019; Nathan Eagle 'Who owns the data you generate online?' (World

development of the protection of privacy in the context of traditional human rights is worthy of mention. The emergence of the right to privacy in international law after World War II seems unique and unprecedented, especially, considering that no national developments have been prominent at that time. The typical situation is for human rights to metamorphose from national recognition to the international stage, but this happened the other way.[203] Perhaps the war may have prompted this development.[204] Primary international human rights instruments after the war, such as the Universal Declaration of Human Rights (UDHR),[205] the European Convention on Human Rights (ECHR),[206] as well as the International Covenant on Civil and Political Rights (ICCPR),[207] contain a right to privacy.

Nevertheless, this human rights approach had some challenges. It faced the reality that it could not cope with more intrusive information technologies used for personal data processing and storage (in both private and public sectors). This is partly because the human rights mechanism of protecting privacy could only be

Economic Forum, 11 October 2014) <https://www.weforum.org/agenda/2014/10/digital-footprint-data-mining-internet/> accessed 25 June 2019; James Craven, 'Personhood: the Right to be Let Alone' (1976) Duke Law Journal 699; Jed Rubenfeld, 'The Right to Privacy' (1989) 102 Harv.L.Rev 737; Natalie Banta, 'Death and Privacy in the Digital Age' (2016) 94 N.C. L. Rev. 927; Edina Harbinja, 'Post-mortem Privacy 2.0: Theory, Law, and technology' (2017) 31 International Review of Law, Computers & Technology 26; Britta van Beers, 'The Changing Nature of Law's Natural Person: The Impact of Emerging Technologies on the Legal Concept of the Perosn' (2017) 18:3 German Law Journal; Julie Inness, *Privacy, Intimacy and Isolation* (Oxford University Press 1992); Robert Gerstein, 'Intimacy and Privacy' (1978) 89:1 Ethics 76; Kirsty Hughes 'A Behavioural Understanding of Privacy and its Implications for Privacy Law' (2012) 75:5 The Modern Law Review 806; Roger Clarke, 'What's Privacy' (Version of 7 August 2006) <http://www.rogerclarke.com/DV/Privacy.html>; Roger Clarke, 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms' (Version dated 24 July 2016) <http://www.rogerclarke.com/DV/Intro.html> accessed 12 January 2018; Bert-Jaap Koops et al, 'A typology of Privacy' (2017) 38 University of Pennsylvania Journal of International Law 483.

[203] Oliver Diggelmann and Maria Cleis, 'How the Right to Privacy Became a Human Right' (2014) 14:3 Human Rights Law Review 441. They write that no state constitution, however, contained a general guarantee of the right to privacy at the time the right appeared in primary international human rights instruments.

[204] Ibid.

[205] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR), art 12.

[206] European Convention on Human Rights (adopted 4 November 1950) (ECHR), art 8.

[207] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR), art 17.

used against the state, when, in fact, private entities were increasingly computerising their systems.[208] Besides, human rights remedies are reactionary, while the threats from computerisation require a more proactive framework if the risks were to be meaningfully mitigated. As Hondius pointed out, 'many legal provisions existing in the pre-computer era' were not enough to meet the challenge to individual rights, posed by automated data systems.[209] This called for some legal reforms[210]—a more regulatory approach that will control both public and private actors.[211]

European data protection law evolved as an instrument to fill this gap: mitigating the risk posed by the computerisation of information processing systems, first in public administration from the late 1960s,[212] and later by private entities. However, several factors raised concerns among commentators: first, the speed with which various governments started experimenting with computers for citizens' data processing and databank creation had the potential of eroding data subjects' control over this process. Also, the possibility of unlimited processing and the automated nature of computerised data processing aggravated these fears.[213] Furthermore, the limitations of the human rights mechanism, as identified above, is significant.[214]

---

[208] Frits Hondius, *Emerging Data Protection in Europe* (North-Holland publishing 1975)1- 8.

[209] Frits Hondius, 'A Decade of International Data Protection' (1983) 30 (2) Netherlands International Law Review 103, 107.

[210] Ibid, 125.

[211] It is notable that the Committee of experts in the CoE recommended that new legislation is needed to tackle the problems posed by modern science and technology to human rights. See Report by the Committee of Experts on Human Rights, Council of Europe (DH/EXP (70) 15).

[212] See Frits Hondius, *Emerging Data Protection in Europe* (n 208); Collin Bennett, *Regulating Privacy Data Protection and Public Policy in Europe and the United States* (Cornell University Press 1992). A similar development was seen in the US, even though a 'patchwork' and sectoral approach was adopted there. See Martin Weiss and Kristin Archick, 'U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield' (Congressional Research services, 2016) 3-4; Margaret O'Mara, 'The End of Privacy Began in the 1960s' *New York Times* (New York, 5 December 2018) <https://www.nytimes.com/2018/12/05/opinion/google-facebook-privacy.html> accessed 19 January 2019.

[213] Hondius, Ibid.

[214] See Committee on Legal Affairs, Report on human rights and modern scientific and technological

Specific examples of the gaps in the legal systems could be cited from both the common law and civil law jurisdictions. For example, in the UK common law system, there is no overarching tort of privacy, as the court acknowledged in *Kaye v Robertson.*[215] This gap meant that cause of action for alleged invasion of informational privacy had to be brought under the tort of breach of confidence (a misnomer in many instances), of which the remedy is only equitable.[216] Moreover, such privacy claims must also fulfil certain conditions listed in *Coco v A N Clark (Engineers) Ltd* to succeed for breach of confidence:

1. the information must have the necessary quality of confidence;
2. the information must have been imparted in circumstances importing an obligation of confidence; and
3. there must be an actual or threatened unauthorised use or disclosure of the information to the detriment of the confider.[217]

Fulfilling these conditions proved difficult in some cases, despite an apparent or potential threat of privacy violation.[218] This created a degree of uncertainty within the common law system, as succinctly summed up by Butler:

> The mere fact that something is private does not make it confidential. Difficulties may also result from any residual elements of confidentiality when applied to the privacy context. If the claimant were still required to show an obligation of confidence, then a privacy claim could be rejected on the ground of the defendant's reasonable ignorance. Confidentiality should

developments (Doc. 2326, 1968); Council of Europe, Recommendation 509 Human Rights and Modern Scientific and Developments (1968).

[215] (1991) 19 IPR 147. Note however that this is not the case in all common law jurisdictions. In the United States, for example, there is common law tort of invasion of privacy, as well as a constitutional right to privacy. Prosser wrote that the American common law tort of invasion of privacy consists of four distinct wrongs: (i) the intrusion upon the plaintiff's physical solitude or seclusion; (ii) publicity which violates the ordinary decencies; (iii) putting the plaintiff in a false, but not necessarily defamatory position in the public eye; and (iv) the appropriation of some element of the plaintiff's personality for a commercial use. William Prosser 'Privacy' (n 87). See also *Griswold v. Connecticut*, (1965) 381 US 479.

[216] Markesinis et al, 'Concerns and Ideas about the Developing English Law of Privacy (and How Knowledge of Foreign Law Might be of Help)' (2004) 52:1 The American Journal of Comparative Law 133.

[217] [1969] RPC 41.

[218] See for example *A v B and C* [2002] EWCA Civ 337, where the English Court of Appeal seemed unwilling to grant the level of confidentiality required to sustain a claim of invasion of privacy, perhaps, due to the moral content of the case.

> not protect publication of any images of a person in a public place, since such information would not have the necessary quality of confidence. Moreover, once information has reached the public domain, no action for confidentiality should remain regardless of how private the information may be. Finally, the action for breach of confidence goes nowhere in correcting the deficiency in the common law identified in Kaye concerning unreasonable intrusions.[219]

This imprecise and reactionary nature of common law privacy protection was problematic, given that the damage suffered by the subjects may be irreversible in some instances. However, it is fair to point out that the UK's privacy law has been transformed over the years following the UK's signing of the ECHR and the adoption of the Human Rights Act 1998. For example, the court has extended the interpretation of breach of confidence, as seen in *Campbell v Mirror Group Newspapers Ltd,*[220] where an action was allowed in the absence of an existing relationship of confidence. Furthermore, in *Vidal-Hall v Google Inc.*,[221] the court advanced a new tort of misuse of private information. Nevertheless, as Stauch rightly suggests, tort law in general 'is less suited to address more surreptitious risks that arise from collection storage and analysis of information (without disclosing it), as well as the capture and collection of data in a less complete state.'[222] Given the advancements in technology that permit invisible intrusion into privacy, surveillance, extrapolated processing of personal data through artificial intelligence, among others, of which the traditional tort law did not contemplate, the need for a regulatory augmentation of the tort law seems obvious.

Cracks were also be seen within civil law jurisdictions regarding informational privacy protection. For example, the French Civil Code, which introduced a

[219] Des Butler, 'A Tort of Invasion of Privacy in Australia?' [2005] MelbULawRw 11; (2005) 29(2) Melbourne University Law Review 339, <http://www.austlii.edu.au/au/journals/MelbULawRw/2005/11.html#fn63> accessed 19 January 2021.

[220] [2004] UKHL 22; [2004] 2 AC 457.

[221] [2015] EWCA Civ 311. See also Paula Giliker, 'A Common Law Tort of Privacy? The Challenges of Developing a Human Rights Tort' (2015) 27 SAcLJ, 761.

[222] Marc Stauch, 'Data Protection Law' in Paula Giliker (ed), *Research Handbook on EU Tort Law* (Edward Elgar Publishing 2017) 186.

general provision on privacy right in 1970, left the term undefined.[223] Patchwork amendments to some provisions of the civil codes lacked clarity.[224] Also, the national constitutional framework was not focused explicitly on the right to informational privacy at this time.[225] These gaps in the legal systems prompted various recommendations from both the Council of Europe (CoE) and some national committees to suggest new approaches, including introducing new legislation to check the privacy threats.[226] The CoE, for example, in Resolution 509 (1968), emphasised that: '[…] the law in the majority of the member States does not provide adequate protection against such threats to the right of privacy'.[227]

This remark was pertinent for informational privacy as no rules were providing affirmative requirements on how personal data should be appropriately processed and managed in the civil law jurisdictions. Therefore, there was a need for a more regulatory and proactive approach to require those wishing to use these ICTs to process personal data to justify such processing and establish a specific procedure for them to follow to ensure that personal data is always safeguarded.[228] In reaction, the CoE seemed to favour a principle-based approach as could be seen in its Resolution 428 (1970) that declared:

> Where regional, national or international computer-data banks are instituted the individual must not become completely exposed and transparent by the accumulation of information referring even to his private life. Data banks

[223] Hondius, *Emerging Data Protection* (n 208) 34. See also the French Civil Code, art 9 <https://www.fd.ulisboa.pt/wp-content/uploads/2014/12/Codigo-Civil-Frances-French-Civil-Code-english-version.pdf> accessed 24 September 2021.

[224] Ibid.

[225] Note that it was not until 1976 when an amendment to the Portuguese Constitution introduced the right to privacy (the Portuguese Constitution 1976, art 35), followed by Spain in 1978 (the Spanish Constitution 1978, sec 18). See also Diggelmann, 'How the Right to Privacy Became a Human Right' (n 203) 3. See also Sian Rudgard, 'Origins and Historical Context of Data Protection Law', in Eduardo Ustaran (ed), *European Data Protection Law and Practice* (IAPP 2018) 18.

[226] Hondius *Emerging Data Protection* (n 208) 17-53.

[227] CoE, Resolution 509 (1968) on Human Rights and Modern Scientific and Technological Developments, para 4.

[228] See Stauch, 'Data Protection Law' (n 222) 184-194.

> should be restricted to the necessary minimum of information required for the purposes of taxation, pension schemes, social security schemes and similar matters.[229]

Implicit in this declaration are some of the fair information principles—data minimisation and purpose limitation. These principles represent general rules that express the fundamental obligations and limitations on how personal data can be processed,[230] and formed a cornerstone for future data protection developments in Europe. For example, these principles require that only the minimum amount of data shall be processed. Furthermore, the purposes for which personal data are to be processed must be known before the commencement of the data collection and must be limited to those purposes. Any further processing of the data will then require a legal basis. These are laudable principles, and they began to be reflected in several resolutions of the CoE on the subject matter from the early 70s.[231] For example, in Resolution 73(22) and Resolution 74/29, while reiterating the need for a new legislative approach to preventing abuses when processing personal data in both the private and public sectors, the CoE included annexes containing specific data protection principles in electronic data processing systems in these resolutions. In 1980, the fair information principles became the basis of the OECD guidelines,[232] and soon after that, they appeared in the CoE Convention

[229] CoE, Resolution 428 (1970) Declaration on Mass Communication Media and Human Rights, para 19.

[230] See Australian Law Reform Commission, *Regulating Privacy* (n 14).

[231] See ibid; CoE, Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private section (26 September 1973); CoE, Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public section (20 September 1974).

[232] The 1980 OECD guidelines explained the principles as follows:

Collection Limitation Principle - There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. **Data Quality Principle** - Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date. **Purpose Specification Principle** - The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. **Use Limitation Principle** - Personal data should not be disclosed, made available or otherwise used for purposes other than those specified. **Security Safeguards Principle** - Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data. **Openness Principle** -

for the protection of individuals with regard to automatic processing of personal data (Convention 108) in 1981.[233]

It is notable that national-level implementation of the CoE recommendations was emerging at this time, in the form of national legislative instruments from the early 1970s.[234] For example, in 1970, the German state of Hesse passed the first local-level data protection law as a safeguard to the computerisation policy of its public administration.[235] Other German states followed suit.[236] In 1973, Sweden passed its national data protection law, which became the first of its kind globally. This law provided rules for personal data processing by both private and public entities, accords certain rights to the data subjects and instituted a Data Inspection Board to oversee its implementation.[237] Soon, other European nations started adopting

---

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller. **Individual Participation Principle** - An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended. **Accountability Principle** - A data controller should be accountable for complying with measures which give effect to the principles stated above. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980 <https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> accessed 13 May 2019.

[233] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, Chapter II.

[234] It is, however, important to note that at the regional-level, the inclusion of the right to respect for private and family life, home and correspondence and conditions under which such right could be limitation in Article 8 of the ECHR 1950 did influence the jurisprudence on privacy and data protection risk governance in Europe. The Committee of Ministers of the Council of Europe, for instance, adopted various resolutions on the protection of personal data in the 1960s in reaction to threats of emerging information technology. See Hondius (n 208); Bennett (n 212); Evelien Brouwer, *Digital Boarders and Real Rights: Effective Remedies for Third Country Nationals in the Schengen Information System* (Martinus Nijhoff Publishers 2008) 178-179; FRA, *Handbook on European Data Protection Law* (Publication office of the EU 2014) 15-16.

[235] Hessisches Datenschutzgesetz (The Hesse Data Protection Act), Gesetz und Verordungsblatt I (1970), 625.

[236] Hondius, *Emerging Data Protection* (n 208) 34-39.

[237] Ibid, 44-46.

similar national data protection laws in various sheds, such as Germany in 1977; France, Norway and Denmark in 1978; Luxemburg in 1979; and Iceland in 1981.[238] In Germany, for example, the Federal Act on Data Protection was primarily focused on 'prevention of the misuse of personal data by the governments', while establishing basic principles of data protection law.[239]

A watershed moment in the rise of personal data protection in Europe was witnessed in 1983 when the German Federal Supreme Constitutional Court interpreted two provisions of the German Basic Law—the guarantee of human dignity[240] and the right to free development of human personality[241]—as including a 'right to informational self-determination'—personal data protection.[242] This decision (further discussed in the next section) is celebrated till today, and indeed, the jurisprudence espoused by the court influenced the future development of data protection in Europe and beyond and gave clear meaning to the data protection principles and the rights of the data subjects in an unprecedented manner.

There was also appeal to and further development of the fair information principles as shown in various forms and shapes that they were incorporated at the national and regional levels. Their values lie, among other things, in the facility that the principles offer to data controllers to use their initiative to figure out the best way to implement them. Such a trend has continued to the present regime. These principles have evolved beyond those in the OCED guidelines from 1980 to include other aspects, such as the principles of transparency and accountability, as seen in Article 5 of the GDPR. Similarly, data subjects' rights began to evolve as a

[238] Frits Hondius, 'A Decade of International Data Protection' (n 237) 104.

[239] Bussche and Stamm, 'The Concept of Data Protection in Germany' (C.H Beck 2012) 104.

[240] Grundgesetz, art 1 (1).

[241] Grundgesetz, art 2 (1).

[242] See the Census case BVerfGE 65, 1. See also Wolfgang Killian 'Germany' in James Rule and Graham Greenleaf (ed), *Global Privacy Protection the First Generation* (Edward Elgar 2008); Alvar Freude and Trixy Freude, 'Echoes of History: Understanding German Data Protection' Bertelsmann Foundation (*Bertelsmann Foundation*, 1 October 2016) <https://www.bfna.org/research/echos-of-history-understanding-german-data-protection/> accessed 12 May 2019.

supporting pillar to the principles, as well as the establishment of supervisory bodies to oversee the implementation of the data protection rules.[243] These national developments continued, with divergences in content and application until the need to foster the EU common market gave rise to the idea of harmonisation of these laws.

In 1995, the EU adopted a Data Protection Directive for this purpose. The Directive also reflected the fair information principles and other proactive risk mitigation elements, such as the requirement for the Member States to prior-check data processing operations that 'present specific risks to the rights and freedoms of data subjects'; the need for data controllers to design their data processing system to be privacy-friendly; and to implement adequate technical and organisational measure to ensure the security of personal data, having regard to the 'risk' associated with such data processing.[244] Some national laws also added other proactive elements, such as the 'pre-processing audit' under the German data protection law.[245] Apart from these elements, the DPD also incorporated other measures to address the risks by way of supervision and sanctions. Article 28 of the DPD required the Member States to establish an independent supervisory authority to oversee the implementation of the Directive alongside other functions and powers. A Working Party, comprising of the supervisory authorities of each Member States, was also established to, among other things, examine the application of the national measures adopted under the DPD in order to contribute to the uniform implementation of such measures.[246] Regarding sanctions, the DPD adopted both a top-down and bottom-up approach. For the former, supervisory authorities had the power to, among other things, investigate, intervene and engage in legal proceedings where the provisions of the DPD or its

[243] See Convention 108 (n 262); Swedish Data Act, 1973.

[244] See DPD, arts 20, 17, and recital 46.

[245] See the German Federal Data Protection Act, s 11 (that implemented the DPD). See also Florian Thoma, 'How Siemens Assess Privacy Impacts' in David Wright and Paul De Hart (ed), *Privacy Impact Assessment* (Springer 2012) 282.

[246] See DPD, arts 29 and 30.

national implementation have been violated.[247] Where empowered, they could issue administrative fines for a breach of the data protection law. For the latter, a data subject who has suffered damage due to unlawful processing was entitled to receive compensation from the controller.[248] In this case, the DPD adopts a 'strict liability' approach, as indicated in Chapter One.

It is notable, though, that despite its overarching objectives and method of implementation, the DPD could not adequately cater for some of the challenges posed by modern ICTs. These challenges include the divergence in the Member States implementation of the DPD and policy choices concerning data protection, the exponential growth in the volume of personal data processed on the Internet, the emerging risks and impact of new technologies used for data processing such as cloud computing, artificial intelligence, cookies, etc., some of which are less detectable, the growth in the data market and increase in the number of intermediaries involved in data processing, the pressure on global civil liberties following government national security policies following the September 11 terrorist attacks, the cumbersomeness and ineffectiveness in the third country data transfer rules, among others.[249]

Given those shortcomings, the GDPR was proposed and adopted in its current form to fill these gaps. In a nutshell, the GDPR retained the basic structure of the DPD, but enhanced several aspects, including among others, making the processors also liable as a result of an infringement of the GDPR;[250] advancing the

[247] See also Paul Schwartz, 'Risk and High Risk: Walking the GDPR Tightrope' (IAPP, 29 March 2016) <https://iapp.org/news/a/risk-and-high-risk-walking-the-gdpr-tightrope/https://iapp.org/news/a/risk-and-high-risk-walking-the-gdpr-tightrope/> accessed 25 July 2016; Article 29 Working Party, 'Statement on the Role of a Risk-based Approach in Data Protection Legal Frameworks' (WP 218, 30 May 2014); Centre for Information Policy Leadership, 'A Risk-based Approach to Privacy: Improving Effectiveness in Practice' (June 2014).

[248] DPD, art 23.

[249] See European Commission, 'First report on the implementation of the Data Protection Directive (95/46/EC), COM (2003) 265 final; 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: 'A comprehensive approach on personal data protection in the European Union', COM (2010) 609 final; Neil Robinson et al., 'Review of the European Data Protection Directive' RAND (2009).

[250] GDPR, art 82.

risk-based approach by making it mandatory to implement data protection by design and by default;[251] to conduct a DPIA under certain circumstances as a measure towards proactive risk management– identifying the potential risks to the data subject and implementing appropriate measures against those risks.[252] Apart from these proactive measures, the GDPR also includes other reactive measures to mitigate the risk to data subjects, such as the obligation to notify them and/or the supervisory in case of a data breach. Risk assessment and treatment is also made an ongoing requirement throughout the data lifecycle. Since the adoption of the GDPR, several other data protection laws in Europe have either being reformed or are undergoing some reform, such as the Convention 108[253] and the e-Privacy Directive.[254] Several sector-specific data protection laws have also emerged following the GDPR such as the Data Protection Law Enforcement Directive (EU) 20016/680 and Regulation 2018/1725 on Data Protection in the EU Institutions and Bodies. The courts have also been very active in interpreting these data protection laws.

In summary, the rise of data protection law in Europe is a testimony of how positive law could be used to address societal risk, as well as advance human rights with moral and cultural characteristics. The discussion in this section has shown how this regulatory approach went beyond the traditional tort-based privacy protection by emphasizing a proactive (*ex-ante*) approach, instead of only offering a remedy for damage resulting from privacy breach as tort law does *ex-post facto*. Adopting statutory instruments, such as the GDPR, to protect informational privacy has introduced more certainty into the legal system, where obligations,

[251] GDPR, art 25.

[252] Some commentators argue that PIA is an instrument of risk governance and should be understood and implemented within the framework of the precautionary principle. David Wright et al., 'Precaution and Privacy Impact Assessment as Modes Towards Risk Governance' in René von Schomberg (ed), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (EU Publication Office 2011) 84; Luiz Costa, 'Privacy and the Precautionary Principle' (2012) 28:1 Computer Law & Security Review, 14; Roger Clarke, 'Privacy Impact Assessment: Its Origins and Development' (2009) 25 CLSR 123.

[253] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (128th Session of the Committee of Ministers, Elsinore, Denmark, 17-18 May 2018).

[254] European Commission, 'Proposal for an ePrivacy Regulation' <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation> accessed 23 November 2019.

rights and penalties are exposed beforehand, and leaving stakeholders with the option to either abide by the rules or face the severe consequences. In the next section, how impact assessment emerged in the European data protection framework shall be examined.

2.3.3 The Emergence of Impact Assessment in European Data Protection Framework

While the DPD envisaged that data controllers and processors should have a mechanism to manage the risks to the data subjects, it is notable that strictly speaking, there was no obligation to carry out a PIA or DPIA or to use any mandatory tool for risk assessment during that era. However, some national implementation strategies were more explicit about incorporating risk management components. For example, the Bulgarian DPA developed minimum standards for technical and organisational measures to assist data controllers and processors in establishing an appropriate level of security.[255] The provision on prior checking was implemented in various forms, including preliminary hearings, onsight inspection and consultations.[256] In Germany, where data protection officials are appointed, they were required to develop a model for privacy risk assessment and responsible for carrying out this assessment in situations where automated processing operations cause particular risk to the data subject.[257] There is also a framework for processor audit under the German system, where data controllers are required to regularly audit data processors.[258]

From a global perspective, impact assessment has long been recognised in the privacy sphere, although its historical origin is controversial. While Clarke writes that PIA has been used since 1973 in a Berkeley, California Ordinance,[259] other

[255] See Gwendal Le Grand and Emilie Barrau, 'Prior Checking, a Forerunner to Privacy Impact Assessments' in David Wright and Paul De Hert (eds), Privacy Impact Assessment (Springer 2012) 109.

[256] Ibid, 106.

[257] Florian Thoma, 'How Siemens Assess Privacy Impacts' in David Wright and Paul De Hert (eds), Privacy Impact Assessment (Springer 2012) 278-279.

[258] Ibid.

[259] Clarke, 'Privacy Impact Assessment: Its Origins and Development' (n 252) 127. A publication from the Canadian Fisheries and Oceans also claims that 'PIAs have been used as far back as the

authors could trace its origin from 1995.[260] Literature evidence, though, points in the direction that PIA became mainstream in Australia, Canada, New Zealand and the USA from the 1990s.[261] However, concerning its adoption in Europe, a presentation by Flaherty in 2000 tends to suggest that the term PIA may not have been used in the European data protection sphere before that year.[262] He writes:

> I realized at Stewart Dresner's superb Privacy Laws and Business conference in Cambridge in July, 2000 that whatever other forms of progress in data protection (such as auditing) have occurred in Europe recently, the concept of a privacy impact assessment as an instrument of data protection has not visibly taken root.[263]

Although the European Commission introduced the tool of impact assessment in 2002 for *ex-ante* estimation of the impact of its policy and regulatory proposals in economic, social and environmental terms,[264] its usage in the area of data protection (in the nomenclature of data protection impact assessment or privacy impact assessment) within the EU is of recent. The first indication of the use of the term PIA may be implied from the report done for the UK's ICO in 2007, which suggests that the Data Protection Ombudsman of Finland mentioned PIA in

1970s' without providing any evidence to back this up. Fisheries and Oceans Canada, 'Access to Information and Privacy (ATIP) Procedure Manual' (n.d) 52 <http://www.dfo-mpo.gc.ca/Library/277874.pdf> accessed 18 March 2019.

[260] See David Tancock, Siani Pearson, Andrew Charlesworth, 'The Emergence of Privacy Impact Assessments' HP Laboratories HPL-2010-63, 10 <http://www.hpl.hp.com/techreports/2010/HPL-2010-63.pdf> accessed 12 August 2015; David Flaherty, 'Privacy Impact Assessments: an essential tool for data protection' (A presentation to a plenary session on 'New Technologies, Security and Freedom', at the 22nd Annual Meeting of Privacy and Data Protection Officials held in Venice, September 27-30, 2000) <https://aspe.hhs.gov/legacy-page/privacy-impact-assessments-essential-tool-data-protection-142721> accessed 8 July 2019.

[261] See David Wright et al., 'PIAF A Privacy Impact Assessment Framework for data protection and privacy rights Deliverable D1' (Prepared for the European Commission Directorate General Justice JLS/2009-2010/DAP/AG, 21 September 2011); Tancock, ibid; Clarke (n 252).

[262] David Flaherty, 'Privacy Impact Assessments: an essential tool for data protection' (A presentation to a plenary session on "New Technologies, Security and Freedom," at the 22nd Annual Meeting of Privacy and Data Protection Officials held in Venice, September 27-30, 2000) <https://aspe.hhs.gov/legacy-page/privacy-impact-assessments-essential-tool-data-protection-142721> accessed 8 July 2019.

[263] Ibid.

[264] Commission, 'Communication from the Commission on Impact Assessment' COM (2002) 276 final.

a presentation he made in August of 2007.[265] However, clear evidence of its first application as a regulatory instrument in Europe is traceable to the UK's ICO publication of a PIA Handbook in 2007.[266] The term 'privacy impact assessment' or 'PIA' was used throughout this handbook.

The literature suggests that the term 'data protection impact assessment' first appeared in the RFID Recommendation of the EC in 2009.[267] In this Recommendation, the EC advocated for a 'privacy and data protection impact assessment' as a means of knowing the implications of the RFID application on the protection of personal data and privacy. Notably, whether the RFID application could be used to monitor an individual;[268] since then, the EC appears to have separated the two concepts of 'privacy' and 'data protection' in its use of impact assessment. In the Commission's subsequent references to the tool in 2010 in the communication for a comprehensive approach to the revision of the DPD,[269] as well as in the Smart Meter Recommendation of 2012, the term 'data protection impact assessment' was used. This term has crystallised with the adoption of the GDPR and has been referred to as such in several EU official documents.

Apart from the above, several supervisory authorities have made some remarks regarding PIA/DPIA. Notably, during the DPD era, in addition to the ICO, the French CNIL[270] and the Spanish AEPD[271] published guidelines on PIA. Since the

[265] Linden Consulting Inc. (n 34) 8.

[266] ICO, PIA Handbook in 2007 (version 1.0, December 2007), which was revised in 2009 'Privacy Impact Assessment Handbook' (Version 2.0, 2009). See also Wright, *Privacy Impact Assessment* (n 34).

[267] Commission, 'Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio- frequency identification' OJ L122/47.

[268] Ibid; see also Wright and De Hart (n 34) 7, 10.

[269] Commission, 'A comprehensive approach on personal data protection in the European Union' COM (2010) 609 final.

[270] CNIL, Methodology for privacy risk management - how to implement the Data Protection Act (June 2012) <http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf> accessed 12 May 2019.

[271] AEPD, GUÍA para una Evaluación de Impacto en la de Protección Datos Personales (2014) <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EI

adoption of the GDPR, all national supervisory authorities have issued one form of guidance or opinion in the bid to explain the provisions of the Regulation, including the DPIA provision.[272] Furthermore, all national authorities appear to have issued a list of data processing that requires mandatory conducting a DPIA according to Article 35 (4) following the EDPB's opinions on their draft lists.[273] Some others have also issued a list of processing that are exempt from DPIA.[274] Annex I contains a table that traces in more detail and sequence, the timeline of the use of the impact assessment in Europe.

Although the use of PIA to manage privacy risks was largely voluntary during the DPD era, it nevertheless attracted many European data controllers. Many organisations adopted PIA as a self-regulatory risk management tool;[275] or as 'one way of proactively addressing privacy principles'. [276] However, no consensus emerged within this period regarding the systematic procedure for conducting PIA, as each data controller freely devised a suitable method. Now that the GDPR has made the conduct of impact assessment explicit, the value of such tool could be summed up by the remarks in ISO 29134:2017:

> A PIA is more than a tool: it is a process that begins at the earliest possible stages of an initiative, when there are still opportunities to influence its outcome and thereby ensure privacy by design. It is a process that continues until, and even after, the project has been deployed.

PD.pdf> accessed 12 May 2019.

[272] See Chapter 4 for a list of supervisory authorities' guidance documents on DPIA.

[273] See EDPB, 'Opinions' <https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en> accessed 24 December 2019.

[274] As at the time of writing Spain and France have published such a list, while the Czech Republic have sent theirs to the EDPB.

[275] David Tancock, Siani Pearson, Andrew Charlesworth, 'The Emergence of Privacy Impact Assessments' HP Laboratories HPL-2010-63 <http://www.hpl.hp.com/techreports/2010/HPL-2010-63.pdf>_accessed 12 August 2015.

[276] ISO 22307: 2008 Financial Services – Privacy Impact Assessment (ISO 2008) v.

Today, sector-specific DPIA rules are emerging to ensure protection in several circumstances, such as DPIA for smart grid and smart metering environment,[277] and the RFID PIA framework.[278]

In the next section, the theory behind the development of data protection law shall be explored to see how scholars have approached it and to bridge the knowledge gap in this area as it relates to the framework of procedural transparency that data protection law envisages.

2.4 De Hert and Gutwirth's Theory of Data Protection

The discussion in the previous sections shows that data protection law has crystallised in Europe as a normative framework for protecting informational privacy and managing the risk associated with the processing of personal data. This was born out of the understanding that given the risks associated with information processing technologies, 'people should be protected by protecting the information about them' through positive law.[279] However, only a few authors have focused on the theoretical embodiment of this idea of data protection,[280] although there are several publications on the broader privacy theories, as well as on the distinction between the right to privacy and that of data protection.[281]

De Hert and Gutwirth seem to have blazed the trail in theorising data protection by exploring democratic principles in a constitutional state and how the notion of

[277] European Commission, 'Data Protection Impact Assessment for Smart Grid and Smart Metering Environment' <https://ec.europa.eu/energy/topics/markets-and-consumers/smart-grids-and-meters/smart-grids-task-force/data-protection-impact-assessment-smart-grid-and-smart-metering-environment_en> accessed 12 January 2020.

[278] See BSI, 'Technical Guidelines RFID as Templates for the PIA-Framework' <bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03126/TG_RFID_Templates_for_PIA_Framework_pdf.pdf?__blob=publicationFile&v=1> accessed 12 January 2020.

[279] Hondius 'A Decade of International Data Protection' (n 209) 109.

[280] Researching on the topic of personal data transparency, Siebenkäs and Stelzer identified 11 theories that are either generic or adapted to privacy research. See Anette Siebenkäs, Dirk Stelzer, 'Assessing Theories for Research on Personal Data Transparency' in Eleni Kosta et al. (eds), *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data* (Springer 2019).

[281] See footnote 59.

'control', a dominant conception of privacy, applies to data protection.[282] The authors explain the roles of privacy and data protection as tools of power control: on the one hand, privacy is represented as a legal tool that 'limits' power—'protects individuals against interference in their autonomy' by government and private entities ('tool of opacity').[283] On the other hand, data protection 'tend[s] to guarantee the transparency and accountability of the powerful' ('tool of transparency').[284] Data protection allows personal data to be processed. However, it compels those responsible for this processing to abide by specific standards, that is, to process such data by adhering to 'good practices'.

In proposing this theory, the authors noted that blanket prohibition of personal data processing is problematic to the modern economy because governments and businesses need personal data for several beneficial purposes in furtherance of governmental obligations or the advancement of commerce and economics. Moreover, as privacy is not an absolute right, there is a need to balance such interests against other interests of social importance, such as public security and freedom of information. Therefore, as there are genuine needs for processing personal data, data protection is the normative tool to check compliance with the data processing rules. This 'transparency tool' provides a practical alternative to the limitations embodied in the 'opacity tool' as explained by the authors:

> [The tool of transparency] assumes that private and public actors need to be able to use personal information and that this in many cases must be accepted for societal reasons. The 'thou shall not kill' that we know from criminal law, is replaced by a totally different message: 'thou can process personal data under certain circumstances'. [285]

Data protection tool incorporates 'various specific procedural safeguards' and promotes 'accountability'. Such safeguards are found in the content of a set of principles and obligations to be observed by data controllers and processors; the

[282] De Hert and Gutwirth, 'Privacy, Data Protection and Law Enforcement' (n 46).

[283] Ibid, 66-68.

[284] Ibid.

[285] Ibid, 77.

nature of the rights accorded to the data subjects; and more importantly, the mandate of a supervisory authority to ensure the implementation of these rules.[286] Notably, De Hert and Gutwirth's theory can be reconciled with the German jurisprudence on the right to informational self-determination, which also embodies the above-mentioned safeguards.[287] In the famous Census case, the contention was the constitutionality of certain provisions of the Census Act of 1983, which included the possibility of crosschecking the census data collected for statistical purposes with population register for purposes of administrative enforcement. After reviewing the nature of the data processing contemplated in the Act, the Court ruled that certain provisions were unconstitutional for improperly infringing on the right to informational self-determination without adequate safeguards.[288] The Court faulted the Census law because it strips the data subjects of the requisite control:

> This information can also be combined—especially if integrated information systems are set up—with other collections of data to assemble a partial or essentially complete personality profile without giving the party affected an adequate opportunity *to control* the accuracy or the use of that profile.[289]

The Court, however, pointed out that this right is not absolute; it could be restricted in cases where there is an overriding public interest:

> Such restrictions must have a constitutional basis that satisfies the requirement of legal certainty in keeping with the rule of law. The legislature must ensure that its statutory regulations respect the principle of proportionality. The legislature must also make provision for

[286] These safeguards are reflected in Article 8 of the CFREU as well as in the defunct DPD and the GDPR.

[287] See Axel Freiherr von dem Bussche and Markus Stamm, *Data Protection in Germany* (n 239) 2.

[288] Ibid. See also Antoinette Rouvroy and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth et al. (ed), *Reinventing Data Protection?* (Springer 2009) 45.

[289] Decisions of the Federal Constitutional Court (Entscheidungen des Bundesverfassungsgerichts – BVerfGE) 65, 14. See an English translation of this judgement by German Konrad-Adenauer-Stiftung (Hanover 2013), 7 <https://freiheitsfoo.de/files/2013/10/Census-Act.pdf> accessed 15 June 2019 (Italics is mine).

> organisational and procedural precautions that preclude the threat of violation of the right of personality. [290]

Although this decision was against the government, it indirectly binds private entities who need legal permission before processing personal data. Above all, the influence of this decision in subsequent developments of data protection law in Germany and the wider European continent has been variously acknowledged.[291] The principles espoused therein undoubtedly influenced De Hert and Gutwirth theory, which offers a more comprehensive articulation of the philosophical embodiment of the concept of data protection.

What is, however, missing in De Hert and Gutwirth's work is an elaboration of the procedural aspects of this transparency tool. Although they rightly identified that data protection laws 'suggest heavy reliance on notions of procedural justice', they never dealt with this issue further.[292] Procedural transparency here refers to being able to evaluate the steps or processes adopted by data controllers and processors in compliance with the rules and safeguards of data protection law before the actual processing and during the processing lifecycle. This notion is important in the context of this study because 'the process', it is often said, 'is more important than the product',[293] and there is a growing understanding that proactive decisional procedure is linked to the transparency of a process (an element also crucial for achieving procedural justice).[294] This is in line with an understanding of transparency as one of the 'privacy protection goals', as explained by Hansen:

> Transparency aims at an adequate level of clarity of the processes in privacy relevant data processing so that the collection, processing and use of the information can be understood and reconstructed at any time. Further, it

[290] Ibid, 3.

[291] See Gerrit Hornung and Christoph Schnabel, 'Data Protection in Germany I: The Population Census Decision and the Right to Information Self-determination' (2009) 25 Computer Law & Security Report, 84; von dem Bussche (n 239) 3; Rouvroy (n 288).

[292] De Hert (n 46) 78.

[293] Jay Mendell and W. Lynn Tanner, 'Process Is More Important Than Product; Or Throw Out the Plan and Keep the Planner' (1975) 3:16 North American Society for Corporate Planning 3.

[294] See Klaus Röhl and Stefan Machura (eds), *Procedural Justice* (Routledge 2018).

> is important that all parties involved can comprehend the legal, technical, and organizational conditions setting the scope for this processing. This information has to be available before, during and after the processing takes place. Thus, transparency has to cover not only the actual processing, but also the planned processing (ex-ante transparency) and the time after the processing has taken place to know what exactly happened (ex-post transparency).[295]

Given that most substantive provisions of data protection law are not self-executing (e.g. rules relating to privacy by design, or data protection impact assessment), *ex-ante* transparency becomes relevant in order to make the public aware of the substance, facts and procedure through which their rights are to be protected. [296] This point is highlighted in Recital 78 of the GDPR, where 'transparency with regard to the functions and processing of personal data' is part of the measures to enable 'the data subject to monitor the data processing'. The WP29 also stresses that '[t]ransparency is another fundamental condition [for data processing], as it gives the data subject a say in the processing of personal data, '*ex-ante'*, prior to processing.'[297] It is this missing link in De Hert and Gutwirth's theory that this study seeks to articulate through its focus on the application of procedural transparency in the context of an *ex-ante* DPIA.

In particular, it shall be argued that a DPIA is an avenue to show accountability and transparency. As such, it should be objective and systematic to allow the envisaged control by the data subjects. This, perhaps, explains why data subjects should be consulted in appropriate cases during a DPIA. Furthermore, in arguing this position, the anatomy of transparency as conceptualised by Heald[298] is explored to illuminate further the fundamental elements of transparency that De Hert and

[295] Marit Hansen 'Top 10 Mistakes in System Design from a Privacy Perspective and Privacy Protection Goals' in Jan Camenisch et al. (eds), *Privacy and Identity Management for Life* (Springer 2012) 25.

[296] Jenny de Fine Licht, Daniel Naurin, Peter Esaiasson and Mikael Gilljam, 'Does transparency generate legitimacy? An experimental study of procedure acceptance of open and closed-door decision-making' (QoG Working Paper Series 2011:8) 3.

[297] WP29 'The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal' (adopted 1 December 2009, WP 168) 16.

[298] David Heald, 'Varieties of Transparency' in Christopher Hood and David Heald (eds), *Transparency: The Key to Better Governance?* (British Academy Scholarship 2006).

Gutwirth proposed. The following section zooms in further on the notion of transparency, first from a general perspective and later as a principle of EU data protection law to understand the various connotations of the term and its application in an *ex-ante* DPIA process.

Furthermore, the ISO 31000 shall be adapted to design a methodology for conducting a DPIA, including the risk assessment process, to achieve procedural transparency in this process. First, this exercise aims to suggest how the contours of risk assessments can be delineated and factors to consider within this process. Secondly, transparency, as it relates to stakeholders' consultation and its implications in terms of foreseeability and knowledge-based for assessing risk, shall be discussed.

2.5 Construing Transparency in Data Protection Risk Assessment

In its day-to-day usage, transparency is associated with openness. The Cambridge dictionary defines transparency as 'the characteristic of being easy to see through'.[299] However, as Koops points out, it has broader implications; it also 'comprises simplicity and comprehensibility'.[300] In the context of data protection, this implies that it should be clear to the data subjects how their data is processed. In other words, they should not only be informed, but also should understand what is happening with their data. Before dwelling on the specifics of transparency in data protection law, it is helpful to highlight the attributes of transparency as propounded by Heald in his 'anatomy of transparency', where he identifies 'four directions' and 'three dichotomies' of transparency.[301]

[299] Cambridge Dictionary, 'Transparency' <https://dictionary.cambridge.org/dictionary/english/transparency> accessed 17 December 2019.

[300] E.J. Koops, 'On Decision Transparency, or How to Enhance Data Protection after the Computational Turn' in Mireille Hildebrandt and Katja de Vries (Eds.), *Privacy, Due Process and the Computational Turn* (Routledge 2013) 199.

[301] Heald, 'Varieties of Transparency' (n 298).

The four directions of transparency, he explains, using two axes: vertical (upwards and downwards) and horizontal (inwards and outwards) (see a venn diagram of these four directions in Figure 5 below). The vertical axis represents a transparency perspective in which the object being scrutinized can be seen by the party below or above. For example, transparency downwards occurs when the object can be seen from below— 'when the "ruled" can observe the conduct, behaviour, and/or "results" of their "rulers"'. Transparency upwards means that the object is visible from above (for those looking down)—here 'the hierarchical superior/principal can observe the conduct, behaviour, and/or "results" of the hierarchical subordinate/agent'.[302] Regarding the horizontal axis, transparency outwards occurs when an organisation can observe what happens outside the organisation, and transparency inwards is when persons outside can observe what happens inside the organisation.[303]

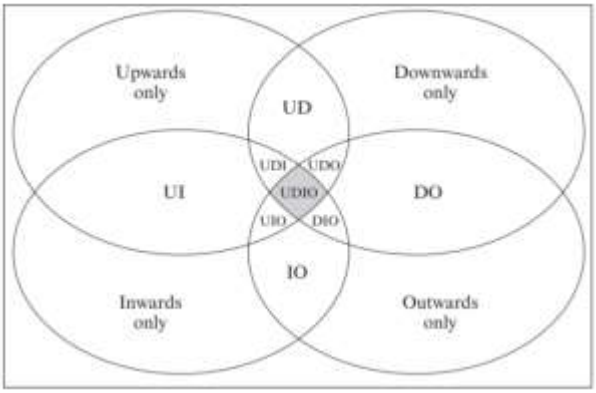


Figure 5: Heald's Venn Diagram of Four Directions of Transparency

Heald also identifies a set of three dichotomies of transparency, which represent how transparency could be characterised:

i. **event versus process transparency**: is concerned with whether the input or output or result is transparent, or whether the procedural and operational process of producing a result is transparent;
ii. **transparency in retrospect versus transparency in real-time**: focuses on where an organisation releases information relevant to its performance *ex-post* on which it will be assessed or where this assessment is a continuous internal process;

[302] Ibid, 27.

[303] Ibid, 28.

iii. **nominal versus effective transparency**: centres on transparency illusion, is that, even when transparency appears to be increasing, as measured by some index, the reality may be quite different.

The conceptual framework of 'transparency downwards' and 'event versus process transparency' dichotomy provide a plausible springboard for applying De Hert and Gutwirth's theory of data protection as a tool of transparency in an *ex-ante* DPIA. Firstly, Heald's vertical 'transparency downwards' illuminates De Hert and Gutwirth's idea that data protection is a tool of control where the data subjects 'can observe the conduct, behaviour, and/or 'results' of how the data controllers are processing their data.[304] This could easily be correlated to various rights accorded to the data subject in the GDPR, such as the right to information, access, objection, etc. Secondly, for this exercise to be useful, it is essential that both the 'event transparency', that is, the inputs, outputs and outcomes of the measures adopted by data controllers, as well as the 'process transparency', that is, the procedure and operational process used to get the results, are visible to the data subjects. In these cases, the events and process have to be 'reasonably well-defined and understood' by the subjects.[305] Heald further argues that there should 'be quality assurance procedures' which, among other things, should be used to check 'whether the procedures have been consistently followed'.[306] These characteristics bring out the intent of De Hert and Gutwirth's theory as it relates to procedural transparency. Though not elaborated by these authors, it should be seen not only in appearance but also in the context of the implementation of data protection law.

Let us consider further how the GDPR synchronises these elements. The principles of transparency and accountability are embedded in the GDPR. Article 5 (1)(a) requires that 'personal data shall be processed lawfully, fairly and in a *transparent* manner in relation to the data subject'. [307] Although the term

[304] See also Koops, 'On Decision Transparency' (n 300) 5.

[305] Heald, 'Varieties of Transparency' (n 298) 30-32.

[306] Ibid, 32.

[307] Italics are mine for emphasis.

'transparency' is not defined in the GDPR, it has been mainly espoused within the context of the information to be provided by the data controller to the data subjects in relation to fair processing; how this information is communicated to the data subject; and how the controller facilitates the exercise of the data subjects' rights.[308] This, however, does not mean that the value of transparency is limited to these instances; instead, the notion of transparency is nuanced and contextually dependent, as shall be seen in the following analysis.

Transparency is inextricably linked with accountability; both are essential principles through which compliance can be demonstrated. Article 5 (2) of the GDPR sets out the accountability principle, which requires that 'the controller shall be responsible for, and be able to demonstrate compliance with' the Regulation. Compliance could be demonstrated in several ways depending on the complexity and nature of data processing. These include observing the principles of data protection and complying with the obligations imposed by the Regulation during the lifespan of data processing, such as conducting a DPIA; documenting and creating a personal data inventory; implementing data protection by design and by default; developing a data privacy governance structure which may include appointing a Data Protection Officer; among others. The transparency requirements in the GDPR 'apply irrespective of the legal basis' advanced by the data controller for data processing and subsist 'throughout the life cycle of processing.'[309]

Arguably, transparency permeates every aspect of data protection — it applies both to the *ex-ante* and *ex-post* procedures aimed at data protection compliance. However, as it relates to the procedural context of a DPIA, transparency is to be understood in a more restricted manner for this study. It is seen here as requiring that the processes, reasons and way a risk assessment is carried out be understood by data subjects, and by extension, the supervisory authorities. This interpretation accords with the definition of transparency by Reed, Kennedy and Silva as 'the property of a system, organisation or individual of providing visibility of its

[308] WP29 'Guidelines on Transparency under Regulation 2016/679' (Adopted on 11 April 2018) 4.

[309] Ibid, 6.

governing norms, behaviour and compliance of behaviour to the norms'.[310] In Heald's work, this is exemplified by the 'transparency downwards' and the 'event versus process transparency' dichotomy.[311]

This attribute of transparency and the value it brings to risk assessment is vital, given that no methodology has been mandated in the GDPR for risk assessment and guidelines on DPIA from the supervisory authorities seem to place less emphasis on the methodological framework for a risk assessment process. The need for clarity in this respect, therefore, arises in the light of Kloza et al.'s remark that impact assessments conducted in the area of data protection usually lack transparency: 'i.e. the process as a whole is opaque, hard to understand for the layperson (due to a high level of technical complexity) and final results and recommendations are difficult, if not impossible, to find.' [312] A corresponding statement is also seen in the CILP privacy risk management project,[313] all of which suggest the need for well-defined DPIA processes that is understandable. Such will eliminate the 'black box' nature of many DPIA reports and templates and solve the issue of verifiability of risk assessments.

Moreover, the visibility of procedural transparency in a DPIA could have a broader positive impact on 'legitimising' the process through which data protection is implemented. For the latter point, in his systems theory, Luhmann offers insight into this role in his work *Legitimation durch Verfahren* (legitimation through procedure).[314] He argues mainly that procedural fairness could form the basis for

[310] Chris Reed, Elizabeth Kennedy and Sara Nogueira Silva, 'Responsibility, Autonomy and Accountability:
legal liability for machine learning' Queen Mary University of London, School of Law Legal Studies Research Paper No. 243/2016, 7.

[311] Heald, 'Varieties of Transparency' (n 298).

[312] Kloza et al., (n 70) 2.

[313] CIPL suggests: 'regulatory guidance could provide an important source of relevant data and regulatory expectations relating to likelihood and seriousness of particular harms, including those affecting fundamental rights and freedoms. The point has already been made that both assessments must be applied objectively, using the reasonable person test'. See CIPL, 'A Risk-based Approach to Privacy' (n 13) 8.

[314] Niklas Luhmann, *Legitimation durch Verfahren* (Willy Fleckhaus und Rolf Staudt 1983). For example, the political-administrative system (e.g. legislative or the court system), he posits, procures legitimacy for its decisions through the procedure it adopts in reaching the decision.

the acceptance of a decision by the public. Although Luhmann's theory was developed in the sociological context of a democratic society, its main idea exposes the importance of transparent procedure in other areas. For example, in the context of implementing data protection safeguards, procedural transparency is essential for the data subjects to understand (at least on the surface) the nature of the data processing system and sub-system to facilitate their control or secure their consent (which may seem illusory if they do not even understand how the data is to be processed and protected). This ties nicely with the dichotomy of the event versus process transparency explained earlier.

Apart from the element of visibility discussed above, foreseeability and inferability are other attributes linked to transparency, which are relevant for the procedure adopted by data controllers and processors when assessing risk *ex-ante.* Foreseeability in the context of a risk assessment process is linked with the manner and scope of how risks are identified; whether the requisite stakeholders' knowledge has been utilised to foresee or predict and treat risk during its assessment (see a fuller discussion of the notion of foreseeability below). Also, Michener and Bersch note that the effect of transparency in decision-making processes, as well as in the quality of decisions, has evolved to include conditions of visibility and inferability (visibility refers to the degree to which information is complete and findable, inferability deals with the degree to which information is disaggregated, verified and simplified).[315] These qualities show that the modern understanding of transparency extends beyond the informational provisioning to the data subjects concentrated in data protection discussions.

From our discussion above, overarching elements of transparency in data protection risk assessment stand out: such assessments must be evaluable, reasonably well-defined and understandable. To be adjudged as transparent, it is suggested that the following elements must be seen in a data protection risk assessment:

[315] See Greg Michener and Katherine Bersch, 'Identifying Transparency' (2013) 18 Information Policy 233, 238.

I. There should be a clear indication of the methodology used for assessing data protection risk, which specifies the processes and criteria for risk assessment in a systematic and identifiable manner.

II. The relevant stakeholders consulted during the process should be clear and their suggestions identified and reflected where appropriate. The scope or extent to which ex-ante risk is foreseen or identified from these stakeholder consultations should be clear.

Below, these two elements shall be further looked at individually.

2.5.1 Transparency with Respect to Methodology

It is undoubtedly the case that transparency in the course of a DPIA will require clarity about the methodology or steps (procedure) that the data controller adopted in identifying the risks, how these risks are analysed, evaluated and mitigated to arrive at the final risk level. The WP29 flagged this point in its first opinion regarding the proposed RFID PIA template in 2010.[316] In rejecting the initial template sent to it for approval, the WP29 noted:

> Indeed, whereas the proposed Framework contains scattered references to risk assessment (mainly in its introductory parts) no section explicitly requires the RFID Operator to identify or 'uncover privacy risks associated with an RFID Application'. It follows that it is not possible to 'evaluate the steps taken to address those risks' [...] A privacy and data protection impact assessment framework should, by definition, propose a general methodology containing a risk assessment phase as a key component.[317]

This statement implies the need for procedural transparency and calls for the design of a DPIA tool that has practical relevance. Regrettably, when the WP29 issued its guidelines on DPIA, it failed to elaborate this element, nor did it provide clear guidance on how to complete Article 35 (7)(c) of the GDPR (which is the portion that deals with the risk assessment phase).[318] Several other guidelines from the national authorities have not solved the problem, and there is no agreement on the steps and content for completing risk assessment during a DPIA, as pointed

[316] WP 29 'Opinion 5/2010 on the Industry Proposal' (n 33).

[317] Ibid, 7.

[318] WP29, 'Guidelines of DPIA' (n 56).

out in Chapter One (see further Chapter Four). There is also a lack of normative explanation indicating how the authorities would review a DPIA's risk assessment part. This gap has motivated this study to suggest a recoupling of transparency in this context by emphasising vital elements of procedural framework—a more proactive approach to rule compliance—where the steps or components for completing each process of DPIA is known beforehand.

Against this background and given that a DPIA is a form of risk management tool, which presupposes that it is a 'transparent and inclusive' exercise,[319] this study proposes to map the requirements of the GDPR regarding a DPIA with the ISO 31000:2018 process (see further Chapter Five for operationalisation of this process). Through such an exercise, the risk assessment processes (made up of risk identification, analysis, and evaluation) can be isolated, and the steps to completing them clarified. Therefore, it is crucial that the relevant components, steps, information or data that should be the basis of a data protection risk assessment be carefully designed and identified and make the criteria for measuring the risk level known (all forming the normative standard). The output of this approach will provide consistency, clarity, and the yardstick to measure the correctness or otherwise of an *ex-ante* risk assessment contained in a DPIA. It will also make the process repeatable.

2.5.2 Transparency with Respect to Stakeholder Consultation and Scope of Foreseeability

On the element of stakeholder consultation and scope, one should recall that the GDPR requires that specific stakeholders shall be consulted where appropriate during a DPIA, including data protection officer (DPO), data subjects and supervisory authorities.[320] The rationale behind this, it could be argued, is to ensure that the correct information and expertise are gathered to make an informed decision about the risk, ranging from its identification to mitigation. This consultation framework of the GDPR gives a first indication of the scope of knowledge envisaged during a risk assessment. It is conceivable that the data

[319]See ISO/TR 31004 Risk Management – Guidance for the Implementation of ISO 31000 (First edition 2013), 17.

[320] See GDPR, arts 35 and 36.

controller who has consulted persons within the appropriate categories of stakeholders would get the right opinion during a risk assessment (e.g., threat identification).

What is not clear, though, from the GDPR is the standard of knowledge required of these stakeholders to measure how well the data controller identifies and mitigates risk. This relates to the scope of necessary foresight in predicting risk since this is an *ex-ante* exercise. Here, we suggest that the foresight of a 'reasonable man' should be used as a transparent and common yardstick to measure the degree of foreseeability in risk assessment. A reasonable man in this context refers to a person knowledgeable about data processing and the means of such processing within the specific context at issue. In this case, this study suggests, then the doctrine of foreseeability can be relied upon to systematise the relevant aspects of risk assessment, in terms of circumscribing the extent to which risk assessors ought to identify or foresee threats or harm posed by a proposed data processing operation. This doctrine shall be explored in the following discussion.

Foreseeability is an essential ingredient in determining negligence and represents one of the filters through which the courts answer both the question of culpability and compensation.[321] One dictionary definition of foreseeability refers to it as '[t]he facility to perceive, know in advance, or reasonably anticipate that damage or injury will probably ensue from acts or omissions.' [322] In the common law tort of negligence, for example, certain elements have crystallised over the years in determining whether the defendant is at fault and, therefore, liable:

i. the defendant must have owed the claimant a duty of care;
ii the defendant's conduct must have fallen below the standard of care (breach of duty); and
iii. the claimant must have sustained damage which was caused by the defendant's breach of duty (causation).[323]

[321] The Australian Law of Negligence Review Panel, 'Review of the Law of Negligence: Final Report' (October 2002)101-119, <https://treasury.gov.au/review/review-of-the-law-of-negligence> accessed 15 December 2019.

[322] The Free Dictionary, 'Foreseeability' <https://legal-dictionary.thefreedictionary.com/Foreseeability> accessed 15 December 2019.

[323] See Reed, 'Responsibility, Autonomy and Accountability' (n 310) 7.

In answering the question of whether there is a duty of care owed to a person who suffers harm as a result of the action of another, Lord Atkin, in the English case of *Donoghue v Stevenson,* propounded the 'neighbour principle' to lay down the foundation of a duty of care.[324] A duty of care exists to 'persons who are so closely and directly affected' by one's actions that he or she 'ought reasonably to have them in contemplation as being so affected' by the acts or omissions in question.[325] The qualification of foreseeability with 'reasonableness' (often referred to as 'reasonable foreseeability') is to aid the court when measuring the scope of the duty of care. Thus, the person causing the injury 'should as a reasonable person have foreseen the general consequences that would result because of his or her conduct'.[326] In this foresight lies the value of the doctrine and what it has been deployed to do in this study, a point to be reverted to later (see also Chapter Five).

Apart from finding that a duty of care exists, it is equally pertinent in negligence cases to ascertain if the defendant has acted in such a way that does not live up to the standard of care expected of the defendant. For example, in situations where a person has held himself or herself out as possessing a particular skill, the standard of reasonable care is determined by reference to 'what could reasonably be expected of a person professing that skill' at the time of the alleged negligence.[327] Concerning the third element, the issues of causation, here again, the principle of foreseeability is relevant. The factual causation question is 'whether the

[324] *Donoghue v Stevenson* [1932] UKHL 100.

[325] Ibid, 8.

[326] Amir Tikriti, 'Foreseeability and Proximate Cause in a Personal Injury Case' (*AllLaw,* n.d*)* <https://www.alllaw.com/articles/nolo/personal-injury/foreseeability-proximate-cause.html> accessed 12 October 2019.

[327] The Australian Law of Negligence Review (n 321) 102. In the English case of *Nettleship v Weston* [1971] 3 WLR 370., the issue was whether a defendant learner driver should be held to a lower standard of care than an experienced driver. However, in rejecting this, the court held that the standard of measure was the same standard that would be applied to any 'reasonably competent person undertaking that activity'. There are however some exceptions to this rule such as where children are involved and are not held to the standard of an adult; or where due to some medical conditions, a person's cognition is impaired, among others. See All Answers ltd, 'Breach of Duty Lecture' (*Lawteacher.net,* December 2019) <https://www.lawteacher.net/modules/tort-law/negligence/breach-of-duty/lecture.php?vref=1> accessed 15 December 2019.

defendant's breach of duty played a necessary part in the claimant's injury'.[328] It is necessary to find this link between the breach and injury so that only liability for harm resulting from the defendant's action or inaction will be imposed and not otherwise (i.e. where the harm would have occurred anyway). However, as a further filter, the courts also ask if the defendant's action was the 'proximate cause' (to solve the issue of the remoteness of damage). For example, where due to an intervention of another human agent or nature, which has led to or contributed to the injury, the defendant should not be held liable for those.[329] It is notable that causation is not difficult to determine in several cases, especially where the natural and probable consequence of the defendant's action is familiar and straightforward.[330] In such cases, the courts will find that 'but for' the action of the defendant, the injury would not have occurred.[331]

Apart from its role in negligence cases, the principle of foreseeability has been applied in different settings and for various purposes in multiple other areas of law, such as criminal law, contract law, product liability, data security, etc. For example, in *Bell v Michigan Council*, where theft of personal data occurred, the defendant was found in breach of a duty of care because the theft (and the associated harm) was foreseeable.[332] However, as could be deduced from the cases above, foreseeability has been relied upon in ex-*post* situations where physical, financial or psychological harms had already occurred and identifiable. In these *ex-post* cases, the nature of the injury (as could be perceived by the senses and/or shown by documentary evidence) significantly assists the courts in determining whether the risk is foreseeable (a sort of hindsight). A court, for example, could easily find a foreseeable link between a data breach and the financial loss that affected the data subjects if some money had been withdrawn from the victims' account illegally.

---

[328] Marc Stauch, 'Risk and Remoteness of Damage in Negligence', (2001) 64 (2) MLR 191.

[329] See *Robinson v Post Office* [1974] 1 WLR 1176. See also the *Wagon Mound* [1961] AC 388.

[330] Ibid.

[331] See Stauch, "Risk and Remoteness' (n 328).

[332] *Bell v. Mich. Council 25 of the Am. Fed'n of State, County, and Mun. Employees*, 2005 WL 356306 (Mich. Ct. of App. 2005) (unpublished). See also In re Verizon Related Reduction Claim, State of Maine Public Utilities Commission, Docket No. 2000-849 (April 30, 2003).

By contrast, this is not the case in *ex-ante* situations, where the harm has not yet occurred. This marks a significant difference. In the latter case, it may be challenging to assign the same role that the doctrine of foreseeability has played in *ex-post* instances because there is uncertainty in linking the threats as assessed *ex-ante* with the harms that may eventually result. It is conceivable that in some cases, the predicted risk or harm may not happen or may happen in a different form. Given this challenge, what role might foreseeability play in an ex-ante situation of risk assessment in data protection?

It is submitted that foreseeability principles can play essential roles in *ex-ante* data protection risk assessment. It is illuminating to consider how the three elements discussed earlier in negligence cases (duty of care, the standard of care, and causation) may apply by analogy (albeit with different weight) in *ex-ante* data protection risk assessment. First, determining the duty of care in data protection law is not controversial, as this is the crux of data protection laws. The GDPR's core role is to impose a duty on data controllers and processors to protect the data subjects from broadly foreseeable harm, which fits into the analogy. Second, the standard of care required of a data controller is that of a person knowledgeable about the data processing to the extent of determining the purpose and means of the processing. Processors are also held to a high standard since they choose to do this job on behalf of the data controller, which means that they are also reasonably knowledgeable in the field. However, matters become a little challenging when it comes to causation, that is, the third element because, at the time of the assessment, the harm is yet to occur; indeed, the aim of the assessment (and risk mitigation steps it identifies) is to reduce the likelihood of it ever happening. This makes the element of causation fluid. It may not apply on the same weight as the other elements because of uncertainty in linking predicted threats with the actual resultant harm at this stage (see also Section 1.2.2.4). However, the aspect of foreseeability of risk (understood here as a potential avenue through which harm may arise) is something that can be considered *ex-ante*.

Of course, where there is reliable historical data suggesting that specific threats lead to certain harms, it would be of immense value to rely on such causation to design the risk treatment measures. However, in some instances, the presence of unpredictability caused by *Novus actus interveniens* has to be considered in applying

the causation element. Thus, it could be concluded that the element of causation is not very helpful at this stage in analysing the principles of foreseeability.

Nevertheless, applying the doctrine of foreseeability as a whole in *ex-ante* data protection risk assessment may have particular challenges and prospects. One of the significant challenges is the limitation of the assessor's knowledge. Irrespective of how qualified an expert may be, there is still a chance that he or she may miss certain things during a risk assessment exercise. There could be instances where an ordinary person, who has specific information that the expert lacks, may predict events more accurately than an expert. Perhaps this explains why a DPIA requires a wide range of consultation and collaboration. Another challenge relates to the uncertainty in the threat-harm relationship in actual manifestation, as already noted. Unlike personal injuries, data protection risks relate to a breach of fundamental rights, which in most cases does not have a physical manifestation, but psychological.

In many cases, this is difficult to articulate *ex-ante*, and is thus more challenging to be used as a yardstick to assess risk. Moreover, there is a lack of specificity in the requirements and scope of measuring foreseeability. Finally, as no concrete guidelines exist in this area yet, there is a chance that speculations may cloud foreseeability.

Notwithstanding these challenges, foreseeability still provides a tool that can be relied upon to design a systematic and transparent risk assessment approach, particularly as it relates to the scope of predictability of risk (that is, as a potential avenue through which threats and harm may arise). The roles assigned to foreseeability here are to assist in scoping how risk should be identified, analysed, and mitigated by extension. In assigning this role, the study draws inspiration from the Institute of Occupational Safety and Health (IOSH) training manual, which suggests a three-test approach in defining the scope of reasonable foreseeability in identifying risk within a work environment—common knowledge, industry knowledge and expert knowledge.[333] In a nutshell, common knowledge refers to where any reasonable person would identify the risk; industry knowledge refers

[333] RRC, *IOSH Managing Safely* (3rd ed, Autumn 2018) Module 4.

to where in a particular industry, the risk is well-known by persons in that industry; while expert knowledge refers to where the risk is outside the knowledge of most of the competent persons in the industry, only experts could recognise such risk.[334] The application of this knowledge test to data protection risk assessment is further explored in Chapter Five.

Finally, it is notable that emerging thinking in data protection legislation is explicitly using the language of foreseeability to describe the obligation of risk assessment.[335] For example, one provision in the Kenyan Data Protection Act 2019 requires data controllers and processors to secure personal data under their control. In doing so, they should consider measures to 'identify reasonably foreseeable internal and external risks to personal data'.[336] Such language brings to the fore the importance of the doctrine, which undoubtedly will assist data controllers and processors in defining the scope of their assessment. For example, foreseeability may require a risk assessor to consider not only the risk to the immediate data subjects, but also others who may be affected by the processing (e.g., those in their social network or even society at large) because they could fall within the categories of persons affected by a particular data processing as seen in the Cambridge Analytica saga. [337]

2.6 Conclusion

The risk to informational privacy was instrumental in the development of European data protection law as a tool to manage the threats posed by information technologies. This European approach has flourished into a more proactive and regulatory framework, exposing principles and procedures that will guide personal data processing. Anyone who decides to process such data must comply with those rules. This is the fulcrum of the theory of data protection as a tool of transparency as propounded by De Hert and Gutwirth—a tool that permits data controllers to process data subject to certain conditions. This chapter has shown

[334] Ibid.

[335] See Kenyan Data Protection Act 2019 (signed 11 November 2019).

[336] Ibid, s 41(4)(a).

[337] See footnote 17.

further how *ex-ante* risk assessment has become part of these conditions under Article 35 of the GDPR.

However, De Hert and Gutwirth's theory do not elaborate on the procedural aspect of this transparency tool. This gap has been explored here through the conceptions of transparency anatomy by Heald. Two key elements of transparency related to ex-ante risk assessment have been identified, primarily relating to the elements of methodology and stakeholder involvement, which directly relates to the scope of foresight in risk assessment. For the former, the ISO 31000 was suggested to provide a systematic methodology, including the risk assessment processes—risk identification, analysis and evaluation. This compartmentalisation offers an excellent opportunity to define the steps and factors to be considered when completing each task, as represented in Figure 4 that forms the conceptual framework of this study. For the latter, the GDPR's provisions regarding stakeholder consultation and the doctrine of foreseeability have been suggested as yardsticks for determining the scope of the knowledge base and foresight required for risk assessment.

A more detailed discussion on the risk-based approach and the provisions of Article 35 of the GDPR that principally obliges a DPIA shall be made in the next chapter. This analysis provides the study's interpretation of this article to bridge the knowledge gap in its implementation.

CHAPTER THREE

3. THE RISK-BASED APPROACH AND ARTICLE 35 OF THE GDPR

3.1 INTRODUCTION

The previous chapter provided a historical background to the notion of risk, privacy and the rise of data protection law in Europe as a proactive risk governance instrument for informational privacy protection, a phenomenon that De Hert and Gutwirth explained as a tool of transparency. The notion of procedural transparency was further explored and applied in the context of DPIA, suggesting a framework to systematically design a methodology for data protection risk assessment. In this chapter, the notion of 'risk-based approach' introduced in Chapter One shall be further examined to determine its component and application under the GDPR. First, the justification for introducing impact assessment, one of the tools that implement the risk-based approach into EU data protection law, is examined. Furthermore, the provisions of Article 35 of the GDPR that create the obligation to conduct a DPIA is analysed. Afterwards, a distinction is made between DPIA and other related tools to complete the chapter.

3.2 THE RISK-BASED APPROACH UNDER THE GDPR

As noted in Chapters One, several approaches to protecting informational privacy have been combined in the European data protection framework, including the risk-based approach. A risk-based approach is an approach of using the level of risk exposure of the data subjects to associate responsibility to the data controller.[338] There have also been some attempts to link a related idea of using the potential harm to base the level of protection of the data subject (the harm-

[338] See Demetzou, 'GDPR and the Concept of Risk' (n 22); Quelle, 'Enhancing Compliance under the General Data Protection Regulation' (n 22); Macenaite, 'The "Riskification" of European Data Protection Law' (n 23); Paul Schwartz, 'Risk and High Risk: Walking the GDPR Tightrope' (IAPP, 29 March 2016) <https://iapp.org/news/a/risk-and-high-risk-walking-the-gdpr-tightrope/https://iapp.org/news/a/risk-and-high-risk-walking-the-gdpr-tightrope/> accessed 25 July 2016; WP29 'Statement on the Role of a Risk-based Approach' (adopted 30 May 2014) WP 218; CIPL, 'A Risk-based Approach' (n 13). For a criticism of the risk-based approach, see Gellert, 'Data Protection: A Risk Regulation?' (n 20).

based approach) within the risk-based discussions.[339] However, this has been criticised due to concerns that it might be an attempt to replace the established data protection rights and principles.[340] Perhaps the WP29 statement on the role of the risk-based approach was meant to clarify this doubt, noting that:

> […] the risk-based approach is being increasingly and wrongly presented as an alternative to well-established data protection rights and principles, rather than as a scalable and proportionate approach to compliance. […] It is important to note that – even with the adoption of a risk-based approach – there is no question of the rights of individuals being weakened in respect of their personal data. Those rights must be just as strong even if the processing in question is relatively 'low risk'. Rather, the scalability of legal obligations based on risk addresses compliance mechanisms. This means that a data controller whose processing is relatively low risk may not have to do as much to comply with its legal obligations as a data controller whose processing is high-risk. [341]

This position is also emphasized by the CIPL,[342] as well as Kuner et al.[343] Demtzou, however, sees the risk-based approach as 'a strategy for the enhancement of the rights-based character of the legal framework.'[344] As such, she argues that the role of risk in the whole equation is to contribute to the protection of the fundamental right to data protection instead of watering it down. One prominent thing in the entire debate about the risk-based approach is that its application is geared towards proactively identifying potential threats and harms to the data subjects and providing measures to address the risk of their materialising. As such, it is a

[339] DigitalEurope, 'DigitalEurope Comments on the Risk-based Approach' (28 August 2013) <https://teknologiateollisuus.fi/sites/default/files/file_attachments/elinkeinopolitiikka_digitalisaatio_tietosuoja_digitaleurope_risk_based_approach.pdf> accessed 12 December 2019. See also Claudia Quelle, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach' (2018) 9 European Journal of Risk Regulation 502, 513-514.

[340] See WP29, 'Statement on the Role of a Risk-based Approach' (n 247)1; Gellert (n 20), 16-19; Kuner et al. (n 13).

[341] WP29, 'Statement on the Role of a Risk-based Approach' ibid, 2.

[342] CIPL (n 13).

[343] Kuner et al. (n 13).

[344] Demetzou (n 22) 142.

plus to the data protection framework in the sense of being the first line of action towards anticipating risk and protecting the data subjects.

Although the GDPR does not define the term 'risk', many references to the notion abound therein that equate risk with adverse impacts of a data processing on the rights and freedoms of the data subjects.[345] The presence of risk is also an essential factor when implementing several obligations in the GDPR, such as:

1. The responsibility of the data controller (Article 24);
2. Data protection by design (Article 25);
3. Records of processing activities (Article 30);
4. Security of the processing (Article 32);
5. Data breach notifications (Articles 33 and 34);
6. Data protection impact assessment (Article 35);
7. Consultation with the supervisory authority (Article 36);
8. Tasks of the data protection officer (Article 39).[346]

Despite not defining risk, the GDPR constitutes 'a major source of extraction of the legal criteria' for measuring the risk associated with personal data processing.[347] Article 35 of the GDPR, which is the focus of this study, concretises one of the obligations of *ex-ante* risk assessment in the form of a DPIA. Several other provisions refer to risk, as shown in Annex 2, from which various components of the risk-based approach could be identified, such as the *threats* to the data subjects (e.g., occasioned by the processing of personal data, particularly involving the processing of sensitive data; predictive processing and profiling; the processing of data of vulnerable persons; large scale data processing; the extent and frequency of processing) assessed in terms of *likelihood and severity* of the *impact* or *harm* to the data subjects—physical, material and non-material (e.g., discrimination, identity theft or fraud, financial loss, reputational damage, damage or interference with the rights and freedoms of the natural person).[348] Recital 76, for example, further indicates the factors to consider when assessing the likelihood and severity of the threats and impact: nature, scope, context, and purpose of the data processing. An objective evaluation is also required in this exercise according to the same recital.

[345] See for example GDPR, art 35.

[346] See Annex 2 for a table of the provisions of the GDPR that refer to risk.

[347] Demetzou (n 22) 139.

[348] See for example, GDPR recitals 75, 77 and 94.

Some of the *measures* to address risks, such as 'pseudonymisation and encryption', regular testing, etc., are suggested in Recital 83 and Article 32 of the GDPR.

Another critical point to note is the overarching objective of the Regulation concerning the risk that it seeks to mitigate. In essence, the GDPR is focused on the 'risk to rights and freedoms of natural persons'. The WP29 explains that '"the rights and freedoms" of the data subjects primarily concerns the right to privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, the prohibition of discrimination, right to liberty, conscience and religion.'[349] This position could be gleaned from the statement in Recital 4 that the GDPR 'respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties'. While it is evident that the term 'natural persons' refers to the immediate data subjects, Demetzou suggests another dimension to it that extends to non-immediate data subjects of the particular processing:

> Data controllers should not limit the risk assessment to the subjects, but they have to assess whether and in what way the processing operation could negatively impact also non-data subjects (i.e. natural persons whose personal data are not being processed).[350]

She illustrates this with the saga of Facebook and Cambridge Analytica, where data of 'friends' of those who downloaded the app in question were also processed despite these friends knowing nothing about the app.[351] This argument is plausible given the discussion on the societal impact of personal data processing, as noted by the WP29 in its statement on the role of the risk-based approach.[352]

A further point to note arising from the various provisions referring to risk is that risk assessment under the GDPR is considered from two temporal perspectives—ex-ante (futuristic) and ex-post facto (retrospective). This has been illustrated in

[349] WP29, 'Statement on the risk-based approach' (n 247) 4.

[350] Demetzou (n 22) 145. Her position appear to reflect the WP 29 state that the risk-based approach should go beyond a narrow scope: 'assessed on a very wide scale ranging from an impact on the person concerned by the processing in question to a general societal impact (e.g. loss of social trust).' See Ibid.

[351] See footnote 17.

[352] WP29, 'Statement on the risk-based approach' (n 247) 4.

Section 1.2.2.1 in Figure 1. It is, however, notable that the GDPR is a mixed bag when it comes to risk and its components and requires painstaking analysis to untangle its knotty provisions. Although Article 35 of the GDPR brings to the fore the obligation of impact assessment, it is notable that this concept has been introduced into EU data protection law during the era of the DPD. The following section focuses on the justifications for such an introduction.

3.3 JUSTIFYING IMPACT ASSESSMENT AS A RISK-BASED APPROACH

While several European academics have also published articles on impact assessment, [353] only a few authors have gone further to look at the justification for adopting *ex-ante* impact assessment in data protection law. [354] This shall be examined below.

It is common nowadays to read about massive data breaches and violations of data protection rights in the media. Statistics reveal an alarming nature of the situation, with nearly 6 million records lost or stolen every day.[355] Although this number does not tell the individual stories, in reality, people have sometimes died due to these breaches (through suicide provoked by mental distress). [356] In many cases, friends, families and a large portion of society have been affected. Therefore, the idea that an *ex-ante* assessment of the impact of a proposed data processing

[353] See, Kuner et al, 'Risk Management in Data Protection' (n 13); Reuben Binns, 'Data protection impact assessments: a meta-regulatory approach' (2017) 7 (1) International Data Privacy Law 22; David Wright and Kush Wadhwa, 'Introducing a privacy impact assessment policy in the EU member states' (2013) 3 (1) International Data Privacy Law 13; Felix Bieker et al, 'Data Protection Impact Assessment: A Hands-On Tour of the GDPR's Most Practical Tool' in Marit Hansen et al (eds) *Privacy and Identity Management. The Smart Revolution* (Springer 2018)´; Lukas Feiler; Nikolaus Forgó; Michaela Weigl, *The EU General Data Protection Regulation (GDPR): a Commentary* (Global Law and Business Ltd 2018); Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, The EU General Data Protection Regulation (GDPR) A Commentary (Oxford University Press, expected September 2019).

[354] See Linden Consulting (n 34) 6-9.

[355] See Breach level index at <https://breachlevelindex.com/> accessed 30 October 2019.

[356] See Laurie Segall 'Pastor outed on Ashley Madison commits suicide' CNN Business (sept 8 2015) <https://money.cnn.com/2015/09/08/technology/ashley-madison-suicide/> accessed 30 August 2021.

operation should be carried out is born out of the need to predict these breaches and implement measures to forestall or reduce their impact on the data subjects. It represents a more proactive approach to showing accountability, especially as the hitherto goal-based and reactive approach to data protection has increasingly witnessed some cracks.

In some cases, data controllers are ignorant of the risk posed by their activities and surprised to learn that they could have discovered the threats before starting their processing operation. At times, when these threats manifest, irreversible harms may have been done, supporting the argument that reactionary measures, at times, are inadequate to manage data protection risks. This gap necessitated an 'early warning system' to assist data controllers and processors in anticipating threats and harms and adopting mitigating measures should they occur.[357] Such proactive measures are best suited where privacy concerns are assessed at the earliest possible time and safeguards baked into the data processing system (an approach captured by the concept of privacy by design).[358]

Related to the above observation is the reality that innovations in information processing technologies inherently pose significant risks due to their complex nature: they could be designed for one purpose and used for another. In such an uncertain environment, it is not surprising that adopting a precautionary approach caught regulatory attention in the area of privacy. In the understanding that there is a social responsibility on the part of the government to protect the public and to justify discretionary policy decisions in circumstances where there is the potential of harm, proactive requirements such as impact assessment is warranted.[359] Wright et al. consider such a precautionary approach as 'the best theoretical framework of action in the face of uncertain risks,' also contending that

[357] Rishi Bhargava, 'The Shifting Data Protection Paradigm: Proactive vs. Reactive' (25 July 2017) <https://devops.com/shifting-data-protection-paradigm-proactive-vs-reactive/> accessed 18 March 2019.

[358] See Ann Cavoukian, 'Privacy by Design: The 7 Foundational Principles' <https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf> accessed 18 March 2019; Bhargava, ibid.

[359] Ortwin Renn et al., *Precautionary Risk Appraisal and Management: An Orientation for meeting the Precautionary principle in the European Union* (Europäischer-hochschulverlag 2009).

PIA is an exercise of precaution and a form of risk governance tool.[360] These attributes of risk and uncertainty fit into the nature of modern data processing system that relies on advanced technologies and justifies the introduction of *ex-ante* impact assessment.[361]

As rightly observed by Costa:

> risk assessment and the precautionary principle go together. They are instruments that jointly determine the allocation of the evaluation of risks and the cost of damages caused by producers of goods and services rather than on citizens themselves. […]The precautionary principle establishes that, despite the readiness, if something goes wrong, those responsible shall not invoke scientific uncertainty to exempt their liability.[362]

Implicit in this statement is that precaution could be a reason for adopting a 'strict liability' regime under data protection law so that those who undertake 'risky' data processing should be strictly liable for harm caused to the data subjects.[363] Thus, proactive impact assessment could then be seen as a way to forewarn data controllers of the impending danger in the venture they are about to pursue.

Adopting a policy of *ex-ante* impact assessment is also a way of simplifying implementing a risk-based approach, which the European Commission believes will help data controllers and processors fulfil their accountability obligation.[364] At the same time, doing a proper assessment has a competitive advantage; it could render a product or service more attractive to would-be consumers by showing that potential risks associated with it have been considered and there are measures to reduce or eliminate those risks. This reasoning, as noted earlier, goes hand in hand

[360] Wright et al, 'Precaution and privacy impact assessment' (n 20). See also Gellert, 'Data Protection: A Risk Regulation? (n 20).

[361] See Nissenbaum, *Privacy in Context* (n 19). The risk posed by new technologies is emphasized in Article 35 of the GDPR.

[362] Costa, 'Privacy and the Precautionary Principle' (n 20) 21-22.

[363] See discussion on liability in Chapter One.

[364] Commission, 'Communication on safeguarding privacy in a connected world. A European Data Protection framework for the 21st Century' COM (2012) 9 final, 6-7. This document further explains the idea behind other proactive privacy approaches such as privacy or security by design, which aim at ensuring that data protection safeguards are taken into account during the planning stage of procedures and systems.

with the obligation to implement data protection by design because a risk assessment is required at the point of design to know how to implement safety measures in a product or service.[365] Besides, there is another advantage to data controllers and processors here: they will avoid the cost associated with re-engineering their products after completion, assuming a privacy defect is discovered afterwards. With hindsight, the impact of the Dutch government's assessment of several Microsoft services is an excellent example to buttress these points. The Ministry of Justice and Security of the Dutch government commissioned a DPIAs of Microsoft services.[366] The purposes of these DPIAs are to assist government institutions in proactively assessing the risk faced by the data subject as a result of using Microsoft cloud-based services and ensuring adequate safeguards against these risks. This proactive initiative found that the parties (the Dutch government and Microsoft) do not meet data protection requirements in some instances. For example, data that Microsoft initially regarded as non-personal data (e.g. telemetry data, diagnostic data) was indeed personal data because they include, in the case of diagnostic data, 'both behavioural metadata and data relating to filenames, file path and e-mail subject lines'.[367] More so, Microsoft assumed, wrongly, that it was only a data processor concerning the purposes for which it processed the diagnostic data. However, the DPIA showed the contrary, indicating that Microsoft is a joint data controller with the government organisations that enable Microsoft to process personal data for specific purposes. [368] The DPIA also found that 'neither Microsoft nor the government organisations have a legal ground' for some of the purposes for which diagnostic data was processed.

Apart from these findings, what though, is essential for our discussion here is how the risk assessment of the metadata of the diagnostic data revealed several threats

[365] See GDPR, art 25.

[366] These involve Microsoft Office 365 ProPlus, Microsoft Windows 10 version 1.5 and Office 365 online and mobile apps. See Rijksoverheid, 'Data protection impact assessments DPIA's Office 365 ProPlus, Windows 10 Enterprise, Office 365 online and mobile apps' <https://www.rijksoverheid.nl/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise> access 8 January 2020.

[367] See Privacy Company, 'DPIA Diagnostic Data in Microsoft Office Proplus' (5 November 2018) 4-8.

[368] Ibid, 6.

and harms just by analysing the *nature, scope, context and purpose* of the metadata processed in the Microsoft Office Proplus, for example. For clarity, we group these findings into threats and harms.

Threats:

1. The use of the behaviour of the Office user to distil a picture/create a profile of the person. For example, reconstruct the working hours through audit log, or use data for negative performance assessment.
2. Blackmailing and stalking of an employee. This could extend to spear phishing, social engineering or blackmail foreign law enforcement authorities for the employees who work with classified or sensitive materials, where they obtain such metadata.

Harms:

1. Experience of chilling effect by the employees as a result of continuous monitoring of behavioural data. This extends to data subjects who are the citizens if they know that their communications subject line is stored and further processed by Microsoft. This could also prevent them from exercising the right of communication confidentiality.
2. Inability to exercise the right to use government facility without being observed.
3. Slight embarrassment, shame and/or change to oral communication instead of written communication.
4. Fostering a culture of secrecy which undermines the core value of accountability and open government.[369]

Although some aspects of the risk assessment would benefit from further refinement and clarity, the approach and level of transparency exhibited in this DPIA report, including the structure adopted to identify and analyse the risks, are worthy of note. For example, in the portion of the DPIA report on Windows 10 relating to risk assessment, there is a division between the risk identification and the 'assessment' of the risk, representing an analysis of the identified risks.[370] This

[369] Privacy Company, 'DPIA Diagnostic Data in Microsoft Office Proplus' (5 November 2018) 76-78. Note that in the later version of the report, 'Microsoft has agreed to process all personal data, regardless of being content or metadata, only for the three authorised purposes, and only where proportionate. Microsoft has also agreed to never use these data for any type of profiling, data analytics, market research or advertising.' Ministry of Justice and Security Strategic Vendor Management Microsoft (SLM Rijk), 'DPIA Office 365 ProPlus version 1905 (June 2019) Data protection impact assessment on the processing of diagnostic data' (Version 1, 22 July 2019) 93.

[370] Ministerie van Justitie en Veiligheid, 'DPIA Windows 10 Enterprise v.1809 and preview v. 1903'

at least shows the use of a structured approach. Notably, these DPIAs have had many impacts all over Europe and have served as a reference point for other supervisory authorities to initiate their inquiries and verify the issues around the use of Microsoft software within their jurisdiction.[371] Microsoft has accordingly addressed the identified risks and revised the affected offerings to comply with the law. [372]

Furthermore, mandatory *ex-ante* impact assessment also allows society to reap the benefits of innovative technologies in a privacy-friendly manner by encouraging developers to engage the citizens in decision-making that affects them right from the start.[373] This view is highlighted in the GDPR's provisions requiring data controllers to consult data subjects and the supervisory authorities in appropriate cases during a DPIA.[374] In the light of this, a DPIA could be regarded as a tool for balancing the freedoms and rights of individual data subjects with those of the data controllers and processors whose innovative needs should not be stifled, but instead enhanced once there is an assurance that such innovation does not increase the risk to society. This is also an avenue to increase transparency, a further value that data protection law seeks to enforce.

Despite these justifications, however, some drawbacks have been associated with the introduction of impact assessment in data protection. Kloza et al. have identified a few of them, including its tendency to add to the burdens of data protection compliance; its complexity in execution; the difficulty in accessing its

(Version 1.5, 11 June 2019) 71-76.

[371] See EDPS, 'EDPS investigation into IT contracts: stronger cooperation to better protect rights of all individuals' <https://edps.europa.eu/press-publications/press-news/press-releases/2019/edps-investigation-it-contracts-stronger_en>; Kyle Brasseur, 'Microsoft updates cloud contract privacy amid EDPS probe' *ComplianceWeek* (18 November 2019); Jan Penfrat, 'Microsoft Office 365 banned from German schools over privacy concerns' *Edri* (17 July 2019).

[372] Daniel Lippman, 'Microsoft to update Office Pro Plus after Dutch ministry questions privacy' *Politico* (2 February 2019) <https://www.politico.eu/article/microsoft-to-update-office-pro-plus-after-dutch-ministry-questions-privacy/> access 12 January 2020.

[373] See Claudia Som, Lorenz Hilty and Andreas Köhler, 'The Precautionary Principle as a Framework for a Sustainable Information Society' (2009) 85 JBE 493.

[374] See GDPR, arts 35 (9) and 36.

value due to the tendency to conducting it abstractly instead of using concrete facts; its narrowness of scope and lack of transparency (as they are not always conducted with public participation), among others.[375] While these criticisms have merit, they do not detract from the fact that *ex-ante* DPIA may—when properly implemented—have a real impact in informing the decision of the data controller towards preventing harm to the data subject. In particular, if appropriate mechanisms have been put in place at the earliest stages of the initiative, this has great potential in minimising the consequences of a data breach. The result of an impact assessment may even suggest that the proposed data processing operation be discontinued, all in the bid to protect the data subjects.

3.4 THE PROVISIONS OF ARTICLE 35 OF THE GDPR

Article 35 of the GDPR is the primary provision imposing the obligation to conduct a DPIA, although carrying out a risk assessment is also envisaged in other provisions of the GDPR, as shown earlier. This article is reproduced here in its entirety for easy reference.

Art. 35 - Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

    a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

    b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

[375] Kloza et al., 'Data Protection Impact Assessment in the European Union' (n 70).

c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. [2]The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:

b) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

c) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

d) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

e) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of

operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

3.4.1 Determining Whether a Data Processing Operation Requires a DPIA

A simple interpretation of Article 35 (1) suggests that a DPIA is not required for all personal data processing operations, even when there is an element of 'risk'. A DPIA is triggered only when the processing is 'likely to result in high risk'. Although the term 'high risk' is not defined in the GDPR (which gives room for much speculation as to what the term amounts to in general), there is a strong indication that it is only a risk that is substantial, above average that requires a DPIA. Article 35 (3) provides three instances where data processing is likely to result in high risk: a systematic and extensive evaluation of personal aspects relating to natural persons (Art 35 (3) (a)); processing on a large scale of special categories of data (Art 35 (3) (b)); and systematic monitoring of a publicly accessible area on a large scale (Art 35 (3) (c)). A mandatory DPIA is required in those instances. This list is intended to be supplemented by a further list by the supervisory authorities under Article 35 (4), which cannot be exhaustive according to the EDPB.[376]

In any case, when the provisions of Article 35 are taken together, a two-tier approach to complying with the requirement of DPIA is envisaged. First, the data controller is expected to conduct a 'preliminary risk assessment' to identify if the proposed data processing involves a high risk to the rights and freedoms of the subject, and if yes, then the second tier, which is the full DPIA follows. This structure was made more apparent in the European Parliament's legislative

[376] See the opinions of the EDPB regarding the draft blacklists and whitelists, available at <https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en> access29 December 2019.

resolution during the negotiation of the draft GDPR.[377] It could also be gleaned from a diagram in the WP29 Guidelines on DPIA as shown below.

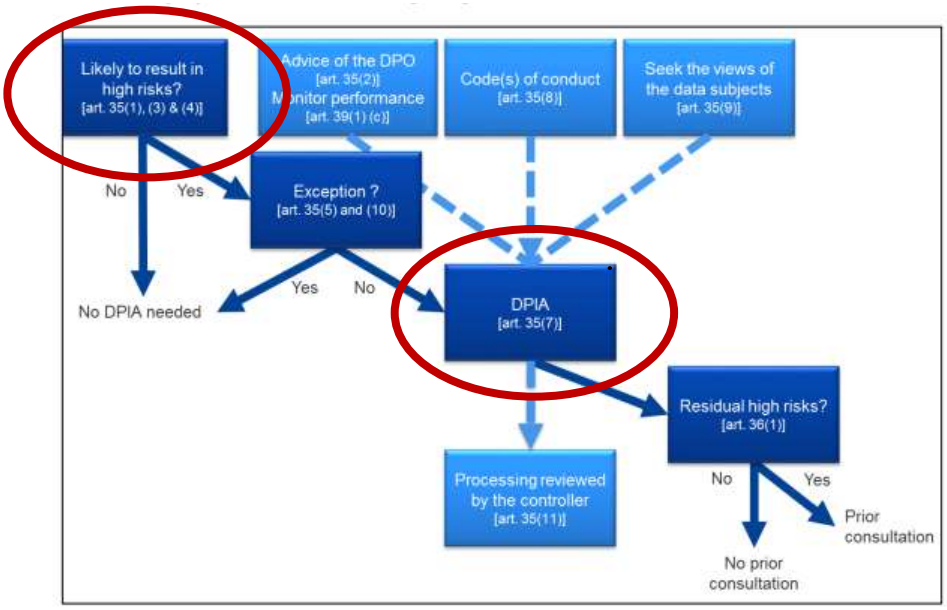


Figure 6: The basic steps related to a DPIA culled from the WP29 Guidelines on DPIA.[378]

The processes circled in red in the diagram indicate the preliminary risk assessment and the full DPIA, respectively.

3.4.1.1 Preliminary Assessment

When conducting the preliminary assessment, attention must be paid to the examples in Article 35 (3), as well as the black and white lists provided by the supervisory authorities under Article 35 (4) and (5).[379] It is not in every case that a preliminary assessment will be a complex process; in some cases, it could be as simple as looking at the applicable blacklist and Article 35 (3) to see if the proposed data processing falls within any of their items. However, in other cases, a

[377] Article 32a (1) and (3)(c). However, there are also some processing operations which by default are presumed to present specific risks in the amendment, see European Parliament, 'Report' <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BREPORT%2BA7-2013-0402%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN> access29 December 2019.

[378] WP29, 'Guideline on DPIA' (n 56) 7. The red circles in the diagram are those of the author.

[379] Blacklist means those data processing activities where conducting a DPIA is mandatory, while whitelist means those activities where a DPIA is exempt.

preliminary assessment will require a more in-depth assessment (especially where the type of processing is not clear from the examples above). As a good practice, the WP29 recommends that in such unclear situations, a DPIA should be conducted nonetheless, as it 'is a useful tool to help data controllers comply with data protection law.' [380]

It is important to point out that the WP29 has fleshed out the examples of processing activities that present a high risk by default, according to Article 35 (3). In addition, it presents some criteria for the supervisory authorities to consider when determining their blacklist and whitelist. The WP29 developed nine criteria as the triggers for a DPIA, including where the processing involves:

1. Evaluation or scoring, including profiling and predicting;
2. Automated-decision making with legal or similar significant effect;
3. Systematic monitoring;
4. Sensitive data or data of a highly personal nature;
5. Data processed on a large scale;
6. Matching or combing datasets;
7. Data concerning vulnerable data subjects;
8. Innovative use or applying new technological or organisational solutions;
9. When the processing in itself "prevents data subjects from exercising a right or using a service or a contract.[381]

The WP29 further notes:

> In most cases, a data controller can consider that processing meeting two criteria would require a DPIA to be carried out. […] the more criteria are met by the processing, the more likely it is to present a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA, regardless of the measures which the controller envisages to adopt.[382]

This 'rule of thumb' does not foreclose that 'in some cases, a data controller can consider that a processing operation meeting only one of these criteria requires a

[380] WP29, 'Guidelines on DPIA' (n 56) 8.

[381] Ibid, 9-11.

[382] Ibid, 11.

DPIA.'[383] However, where a data controller decides not to carry out a DPIA despite meeting two or more criteria, such a controller shall justify and document the reasons for not carrying it, and shall include the views of its data protection officer.[384]

Recently, the national supervisory authorities have been issuing their lists of processing activities that require DPIA (blacklist) as well as those that do not (whitelist).[385] For example, the Irish DPC published the following list of processing likely to result in high risk, and therefore requiring a DPIA:

> 1) Use of personal data on a large-scale for a purpose(s) other than that for which it was initially collected pursuant to GDPR Article 6(4).
>
> 2) Profiling vulnerable persons including children to target marketing or online services at such persons.
>
> 3) Use of profiling or algorithmic means or special category data as an element to determine access to services or that results in legal or similarly significant effects.
>
> 4) Systematically monitoring, tracking or observing individuals' location or behaviour.
>
> 5) Profiling individuals on a large-scale.
>
> 6) Processing biometric data to uniquely identify an individual or individuals or enable or allow the identification or authentication of an individual or individuals in combination with any of the other criteria set out in WP29 DPIA Guidelines.
>
> 7) Processing genetic data in combination with any of the other criteria set out in WP29 DPIA Guidelines.
>
> 8) Indirectly sourcing personal data where GDPR transparency requirements are not being met, including when relying on exemptions based on impossibility or disproportionate effort.
>
> 9) Combining, linking or cross-referencing separate datasets where such linking significantly contributes to or is used for profiling or behavioural

[383] Ibid.

[384] Ibid, 12.

[385] EDPB, 'Opinion' (n 376). See also GDPR, Art 35 (4) and (5). GDPR's Recital 91 is also important here because it contains some examples of processing that should not require a mandatory DPIA.

> analysis of individuals, particularly where the data sets are combined from different sources where processing was/is carried out for difference purposes or by different controllers.
>
> 10) Large scale processing of personal data where the [Irish] Data Protection Act 2018 requires "suitable and specific measures" to be taken in order to safeguard the fundamental rights and freedoms of individuals.[386]

A preliminary assessment must not only consider the blacklist; it is also essential to consider the whitelists to know if the proposed data processing has been exempted.[387] Examples of such whitelists are from the French CNIL,[388] the Spanish AEPD[389] and the Czech Republic SA.[390] The present author has noted that there could be hypothetical cases where there is a conflict between the blacklist and the whitelists and suggests that the blacklists should prevail given that the whitelist 'may not exempt' items in a current blacklist.[391] Apart from the blacklist and whitelist, Article 35 (10) is also essential when assessing whether a specific data processing operation is exempt from DPIA. This provision suggests that where a general impact assessment had already been carried out in the context of adopting

[386] Data Protection Commission, 'List of Types of Data Processing Operations which require a Data Protection Impact Assessment' <https://dataprotection.ie/sites/default/files/uploads/2018-11/Data-Protection-Impact-Assessment.pdf>. See also EDPB, 'Opinion 11/2018 on the draft list of the competent supervisory authority of Ireland regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)' (adopted 25 September 2018) <https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion_2018_art._64_ie_sas_dpia_list_en.pdf> accessed 12 December 2019.

[387] See Iheanyi Nwankwo, 'The "Whitelist" and its Value during a Data Protection Impact Assessment' (*DPOBlog*, (25 October 2019) <https://dpoblog.eu/the-whitelist-and-its-value-during-a-data-protection-impact-assessment> accessed 3 December 2019.

[388] CNIL, 'Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données n'est pas requise' <https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-non-requise.pdf> accessed 30 January 2020.

[389] AEPD, 'Indicative List of the Types of Data Processing that Do Not Require A Data Protection Impact Assessment Under Art 35.5 GDPR' <https://www.aepd.es/media/guias/ListaDPIA-35-5-Ingles.pdf> accessed 30 January 2020.

[390] EDPB, 'Opinion 11/2019 on the draft list of the competent supervisory authority of the Czech Republic regarding the processing operations exempt from the requirement of a data protection impact assessment (Article 35(5) GDPR)' (*EDBP* 12 July 2019) <https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-112019-draft-list-competent-supervisory_en> accessed 30 January 2020.

[391] Nwankwo, 'The "Whitelist" and its Value' (n 387).

the legal basis for data processing, involving compliance with a legal obligation (under Art 6 (1) (c), or necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Art 6 (1)(e), no further DPIA shall be carried unless a Member State deems it necessary.

It is worth re-emphasizing that no blacklist or whitelist can be exhaustive. This is premised on the interpretation that making any such list exhaustive will be incompatible with the wording of Article 35 (1).[392] Such an interpretation is plausible, given that innovative data processing technologies will continue to emerge, making it likely that new risks will also arise. Nevertheless, these lists are to be welcomed, as they provide clear indications at the moment, thereby reducing the resources spent in conducting a preliminary assessment.

3.4.1.2 A Full Data Protection Impact Assessment

As stated, if the preliminary assessment finds that the proposed data processing is likely to result in a high risk, then the second phase of Article 35 starts, which is to conduct a full DPIA. This envisages a comprehensive process that identifies the risks posed by a specific data processing operation in order to put in place appropriate safeguards against those risks. As noted earlier, the GDPR does not prescribe a precise methodology for this process; however, a cursory look at its provisions indicates a DPIA's minimum content. Article 35 (7) of the GDPR, for example, states that the assessment shall contain at least: (a) a systematic description of the envisaged processing operations; (b) an assessment of the necessity and proportionality of the processing operations; (c) an assessment of the risks to the rights and freedoms of data subjects; (d) the measures envisaged to address the risks. This provision has been expanded in the WP29 guidelines, which suggest a generic iterative process for conducting a DPIA as follows:

1. Description of the envisaged processing;
2. Assessment of the necessity and proportionality;
3. Measures already envisaged;
4. Assessment of the risks to the rights and freedoms of the data subject;
5. Measures envisaged to address the risks;

[392] Ibid.

6. Documentation.
7. Monitoring and review.[393]

Despite this suggestion by the WP29, some supervisory authorities have developed alternative processes (see Chapter Four). For consistency, however, the following analysis shall concentrate on the provisions of Article 35 (7) that provide a four-step process for a full DPIA.

3.4.2 Essential Elements of a Full DPIA

3.4.2.1 Systematic Description of the Envisaged Data Processing (Art. 37 (a))

Article 35 (7) (a) of the GDPR requires that a DPIA contain 'a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller'. In a nutshell, this will require a clear description of the proposed data processing so that an independent observer can understand what will happen in the processing. There is no hard and fast rule as to how the data controller should describe the context of data processing during a DPIA. However, any such description should be sufficient to understand the nature of data processing, scope, purpose and the technology used for the processing in order to identify the potential risk.

Some sources indicate what such a description should include. For example, in the ISO 31000 risk management framework, such a description is contained in the process of establishing the context, scope and purpose of risk management. Although the central part of the WP29 guidelines lacks an elaboration of this article, some key points were itemised in Annex 2 of the guidelines indicating what should be in this description, as shown in the figure below.

[393] WP29, Guidelines on DPIA (n 56) 16.

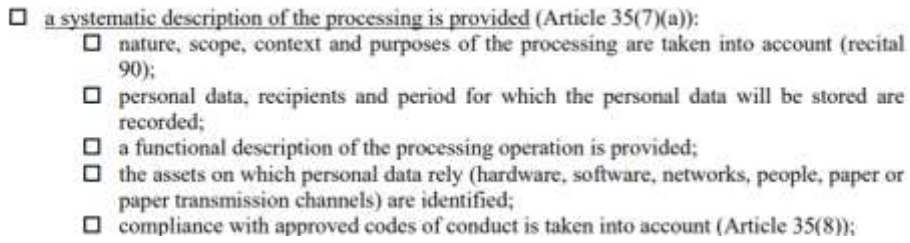

- ☐ a systematic description of the processing is provided (Article 35(7)(a)):
  - ☐ nature, scope, context and purposes of the processing are taken into account (recital 90);
  - ☐ personal data, recipients and period for which the personal data will be stored are recorded;
  - ☐ a functional description of the processing operation is provided;
  - ☐ the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified;
  - ☐ compliance with approved codes of conduct is taken into account (Article 35(8));

Figure 7: A portion of Annex 2 of the WP29 Guidelines indicating criteria to assess a DPIA

Apart from these WP29 vital points, the CNIL PIA Methodology suggests that this description should '[p]resent a brief outline of the processing under consideration, its nature, scope, context, purposes and stakes'; 'Identify the data controller and any processors' as well as list the applicable laws, approved codes of conduct and certifications regarding data protection.[394] For its part, the Spanish AEPD's suggests using a detailed description of the data lifecycle and flow, including identification of data, parties involved including third parties, systems and any other relevant elements to describe the context of data processing.[395] The EDPS interprets a similar provision under Regulation (EU) 2018/1725[396] as requiring the risk assessor to explain what they will do with the data and how they will do it.[397] The EDPS also advises data controllers to create this systematic description by starting with the information they already have in their record (where such exists) and to include the following points in the description:

> • data flow diagram of the process (flowchart): what do we collect from where/whom, what do we do with, where do we keep it, who do we give it to?
>
> • detailed description of the purpose(s) of the processing: explain the process step-by-step, distinguishing between purposes where necessary;
>
> • description of its interactions with other processes - does this process rely on personal data being fed in from other systems? Are personal data from this process re-used in other processes?

[394] CNIL, 'PIA Methodology' (n 76) 4.

[395] AEDP, 'Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD' herein after Guide on DPIA (AEDP 2018) 6.

[396] Regulation (EU) 2018/1725 (n 3).

[397] EDPS, 'Accountability on the ground Part II (n 26) 6. See Regulation (EU) 2018/1725, art 39 (7)(a).

- description of the supporting infrastructure: filing systems, ICT, etc. [398]

The examples above are not intended for the data controllers to stick to one only; instead, combining these suggestions may reveal an encompassing approach that best fits the purpose of Article 35 (7)(a). A further point to note is that where applicable, the data controller should also describe the legitimate interest that is pursued by the data processing under this provision. Such a description, by its nature, has a link with the legal basis for data processing under Article 6 of the GDPR and is closely connected with the necessity and proportionality assessment discussed in the next section.

In summary, a description of the envisaged processing is a contextual exercise. Therefore, Kloza et al. suggest that the description step in a DPIA should be a two-part account of the planned initiative: a contextual description and a technical description.[399] This perhaps captures the intention of Article 35 (7)(a).

3.4.2.2 Necessity and Proportionality Assessment (Art. 35 (7)(b)

Article 35 (7)(b) of the GDPR requires that a DPIA contain 'an assessment of the necessity and proportionality of the processing operations in relation to the purposes.' Necessity and proportionality are fundamental principles commonly used to measure whether interferences with certain fundamental rights or freedoms are necessary and proportionate to the aim they pursue. [400] These principles have frequently been applied in assessing the constitutionality of legislative or administrative measures that limit fundamental rights, and the courts have interpreted them in several cases.[401] Anđelković identifies four theoretical elements of proportionality: legitimacy, adequacy, necessity and proportionality

[398] Ibid, 7.

[399] Dariusz Kloza et al, 'Towards a Method for Data Protection Impact Assessment: Making Sense of GDPR Requirements' d.pia.lab Policy Brief 1 (2019) 3.

[400] See Luka Anđelković, 'The Elements of Proportionality as a Principle of Human Rights Limitations' (2017) 15:3 Law and Politics 235.

[401] See Digital Rights Ireland (CJEU, Joined Cases C-293/12 and C-594/12); Huber (CJEU, Case C-362/14); Schecke (CJEU, Joined Cases C-92/09 and C-93/09); Tele2 Sverige AB (CJEU, Joined cases C-203/15 and C-698/15). See also EDPS, 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit' (11 April 2017).

stricto sensu.[402] 'Necessity', he writes, 'means that the least restrictive measure should be used for achieving the aim. The least restrictive measure is the one that has the least effect on the guaranteed right.'[403] Although the principles of necessity and proportionality are not explicitly mentioned in Article 5 of the GDPR (except that the principle of data minimisation requires that processing personal data shall be limited to what is necessary), it is widely acknowledged that any limiting of the right to data protection or privacy shall adhere to these principles, and shall be justified through objective evidence.[404] Thus, according to the EDPS, '[n]ecessity is fundamental when assessing the lawfulness of the processing of personal data. The processing operations, the categories of data processed and the duration the data are kept shall be necessary for the purpose of the processing.'[405] This statement locates the principle of necessity within the established data protection principles under Article 5, such as the lawfulness, purpose and storage limitation principles.

On the other hand, proportionality restricts authorities in the exercise of their powers by requiring them to strike a balance between the means used to limit a fundamental right and the intended aim. In the context of data protection, proportionality is vital for assessing any limitation of the rights of the data subjects. It 'requires that advantages of limiting the right to personal data are not outweighed by the disadvantages to exercise this right.'[406] Like the principle of necessity, it requires a justification, including safeguards accompanying such a limitation. Also, proportionality in data protection requires that only personal data, which is adequate and relevant for the processing, is collected and processed. This equally reflects the data minimisation principles in Article 5 (c) of the GDPR.

[402] Anđelković , (n 400) 237.

[403] Ibid.

[404] EDPS, 'Necessity and Proportionality' <https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en> accessed 4 August 2019.

[405] Ibid.

[406] Ibid.

Although Article 35 (7)(b) does not elaborate on the content of the necessity and proportionality assessment, from the discussion above, there seems to be a close link between these principles and the principles of data protection contained in Article 5. This link could be seen in the statement that 'an assessment of the necessity and proportionality of the processing operations [shall be] *in relation to the purposes*' as indicated in Article 35 (7)(b).[407] As one of the principles of data protection, the purpose limitation presupposes that personal data must be collected for 'specified, explicit and legitimate' purposes (purpose specification) and not be 'further processed in a way incompatible' with those purposes (compatible use).[408] A common approach to understanding and assessing the purposes for which data is to be processed is by having a clear description of the proposed data processing, which include, among others: a description of the type of data, the collection procedure, the data flow, the purpose of the data collection, how it will be stored and when it will be disposed of, etc. Such a systematic description makes it easy to identify the legal basis of data processing as well.

Taken together, there, Article 35 (7)(b) leads to an evaluation of the data protection principles. The WP29's Annex 2 to the Guidelines on DPIA also tend to suggest that necessity and proportionality assessment shall include all the principles mentioned in Article 5.[409] This suggestion is logical because these principles—data minimisation, adequacy, lawfulness, etc., would ordinarily be implicated when assessing if a proposed data processing is necessary and proportional to the aims it seeks to achieve. The AEPD guide on DPIA equally discusses the entire data protection principles under this phase of the DPIA.[410]

However, the WP29 seems to have introduced some complexity in its interpretation of this provision when it suggests including 'measures contributing to the rights of the data subjects' as other aspects that need to be assessed during

[407] GDPR, art 35 (7)(c). Italics are by the author's for emphasis.

[408] See Art. 5 (1) (b). See WP29, 'Opinion 03/2013 on Purpose Limitation' (adopted 2 April 2013) WP 203 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> accessed 12 December 2019.

[409] See annex 1 to the WP29 DPIA Guidelines.

[410] AEPD, 'Guide on DPIA' (n 395) 18.

this phase, as seen in Annex 2 of its guidelines. These rights are primarily those mentioned in Articles 12 to 22 of the GDPR, and other rights in the European Charter and ECHR, affecting the data subject. Nevertheless, there seems to be confusion regarding under what phase to assess the rights and freedoms of the data subject, whether it is in this article or the next (Article 37 (7)(c) that talks about 'assessment of the risks to the rights and freedoms'. This issue shall be clarified in the next section.

In summary, assessing the necessity and proportionality of a proposed data processing requires a clear description of why the data processing is planned and how the data to be processed fulfils those purposes. We have argued that this invariably triggers an assessment of the other principles of data protection under Article 5 of the GDPR.

3.4.2.3 Risk Assessment Art. 35 (7)(c)

Risk assessment is a vital process in risk management. It represents a systematic process of identifying threats surrounding an object or asset and evaluating the likelihood and impact of occurrence. The GDPR requires that data controllers assess risk in several instances, as already noted (such as in Articles 24, 25, 32 and 35). These provisions do not conceptualise risk assessment in the same manner or with the same focus. It is essential to understand the differences to know the nature of risk assessment envisaged under Article 35 (7)(c) of the GDPR. For example, the Norwegian Datatilsynet noted some differences between risk assessment under Article 32 and Article 35. It rightly pointed out that the focus of the former is to gain knowledge about the data security risk emanating from 'accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed'.

In contrast, the latter focuses on the consequences of data processing that pose a high risk emanating from data security and other elements, including where there is no data breach.[411] According to the Datatilsynet, implementing security measures alone will not necessarily reduce the harm envisaged here (e.g.,

[411] Datatilsynet, 'Vurdering av personvernkonsekvenser (DPIA)' <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/?id=10361> accessed 2 January 2020. (Translation by the author).

encrypting the data may not solve the problem of discriminating against the data subject emanating from profiling). As such, the data controller must identify other risk treatment measures appropriate to the context. This interpretation ties in well with the remarks of Korff and Georges that "'risks to the rights and freedoms of natural persons" do not flow only from data breaches.'[412]

Concerning Articles 35 (7)(c), which is the provision that hosts the phase of 'risk assessment' as part of the minimum content of a DPIA, there seems to be no uniform interpretation as to what it means to complete this process. A popular approach allows data controllers to choose any method they deem appropriate, and understandably so since no universally accepted methodology exists so far. However, the lack of a clear standard has some implications relating to the content and structure of such assessments, which can potentially negate the 'objective assessment' envisaged in the GDPR. A look at the language of this provision may explain this seeming confusion. It requires that a DPIA contain 'an assessment of the risks to the rights and freedoms of data subjects [….]'. This expression tends to suggest first, a conventional risk assessment of which a central focus is on the risks to the rights and freedoms of the data subject. The WP29 has indicated that these rights span beyond the rights and freedoms of the rights of the data subjects under the GDPR (Articles 12-22) to include other rights and freedoms, such as freedom of expression, prohibition of discrimination, right to liberty, etc.).[413]

Therefore, a logical interpretation of this provision should be that it envisages conducting a conventional risk assessment, which by its nature, aims at forecasting a future event that could affect the rights and freedoms of the data subjects. The consequence here is that risk assessment must be designed to be systematic, measurable and reliable using metrics such as the rights of the data subject during the evaluation of the assessment. Assuming particular processing involves profiling of data subjects, during the risk assessment phase, it is expected that the risk

[412] Douwe Korff and Marie Georges, 'The DPO Handbook: Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation' (As approved by the Commission, July 2019)184 <https://www.garanteprivacy.it/documents/10160/0/T4DATA-The+DPO+Handbook.pdf> accessed 2 January 2020.

[413] WP29, 'Guidelines on DPIA' (n 56) 6.

assessor shall identify the threats and harm associated with this operation, and when evaluating the likelihood and impact of the identified threats and harm, shall consider not only the rights related to profiling under Article 22 of the GDPR, but also other fundamental rights such right against discrimination.[414] It is in this respect that we view Article 35 (7)(c) and the not (7)(b)–relating to the necessity and proportionality assessment, as the right place to analyse the rights and freedoms of the data subjects.

Unfortunately, the WP29 seemed reluctant to address the issue of risk assessment methodology in its guidelines. It only listed some yardsticks to measure the level of comprehensiveness of a risk assessment (reflecting Article 35 (7)(c)) in the annex.[415] This approach lacks a systematic framework, as it does not clearly indicate how to complete this aspect of the DPIA process. There are no specificities on how to quantify the residual risks to activate Article 36 of the GDPR. Giving examples of existing EU DPIA frameworks, which the WP29 did in the annex,[416] does not solve the problem or answer how to interpret and apply Article 35 (7)(c). Besides, the WP29 did not reconcile the discrepancies in those examples in the annex.

This lacuna has led to multiple interpretations of Article 35 (7)(c), as noted in Chapter One. For example, mapping the WP29 Guidelines with the CNIL PIA Methodology shows that the CNIL interprets this part of the Annex to mean an assessment of the data security risk only.[417] On the other hand, the EDPS regards a corresponding provision in the Regulation (EU) 2018/1725 on data protection by EU institutions as a process of mapping risk and control measures; and mapping the data flow with the protection targets (the data protection principles). Other supervisory authorities adopted a different approach, making it difficult to

[414] See WP29 'Statement on the role of a risk-based approach in data protection legal Frameworks' (adopted 30 May 2014) WP 218, 4; WP29 Guidelines on DPIA. See also FRA, *Handbook on European Non-discrimination Law* (FRA 2010).

[415] WP29, 'Guidelines on DPIA' (n 56) Annex 2.

[416] Ibid, Annex 1.

[417] CNIL, 'PIA Methodology' (n 76)11.

conceptualise this risk assessment from a single perspective (see further Chapter Four).

Similarly, it is not correct to limit the application of Article 35 (7)(c) to data security risk assessment as the CNIL did. Another way of putting it is that the controller needs to think about the risks posed by its planned use of the data, not just about unplanned uses (such as the data being misused by a third party). The reason for CNIL's limitation of this article to data security is not apparent. It appears to be contrary to the view of the EDPS to the effect that information security risk does not cover all aspects of data protection:

> [Information security risk management] ISRM tends to focus on risks that stem from unauthorised system behaviour (e.g. unauthorised disclosure of personal data), while parts of the risks to data subjects and compliance risks stem from the authorised system behaviour for which you do the DPIA.[418]

This point is also highlighted by Korff and Georges when they argue that risk assessment is 'not just the security risks in a narrow sense – i.e., the likelihood and impact of a data breach'.[419] They further note that although data security is one major category of data protection risk assessment, the GDPR contemplates other risks as well, such as those stemming from profiling, large scale processing of special categories of data as well as large scale and systematic monitoring of a publicly accessible area, of which the risks posed by them can materialise without any data breach per se. The risks considered here stem from 'the inherently dangerous features of the processing operations themselves, even if performed in accordance with their specifications and without a data breach as defined in the GDPR.'[420] As such, the risk assessment to be done during a DPIA extends beyond data security. Gellert has criticised this part of the CNIL's approach for being 'merely a data security methodology'.[421] There is merit in this critique because

[418] EDPS, 'Accountability on the Ground Part II' (n 26) 9.

[419] Korff and Georges, 'The DPO Handbook' (n 412) 179; 184 ff.

[420] Ibid, 185.

[421] Raphael Gellert, 'Understanding the notion of risk in the General Data Protection Regulation' (2018) 34 Computer Law & Security Review 279, 283.

limiting Article 35(7)(c) to only data security risk unnecessarily waters down the effect and purpose of this provision. Besides, the ISO 29134:2017 suggests other threats of data protection:

a. excessive collection of PII (loss of operational control);
b. unauthorised or inappropriate linking of PII;
c. insufficient information concerning the purpose for processing the PII (lack of transparency);
d. failure to consider the rights of the PII principle (e.g., loss of the right of access);
e. processing of PII without the knowledge or consent of the PII principle (unless such processing is provided for in the relevant legislation or regulation);
f. sharing or re-purposing PII with third parties without the consent of the of the PII principle;
g. unnecessarily prolonged retention of PII.[422]

This reasoning motivated this study to view risk assessment in the context of a DPIA as an exercise to answer three fundamental questions: 'What could go wrong? What is the likelihood of that happening? What are the consequences?' as posed by Kaplan and Garrick. First, by assessing what could go wrong in a proposed data processing operation, the risk assessor ought to identify the assets, threats and threat events, and the vulnerabilities (based on both the planned processing and the unplanned interference) that can potentially lead to violation of the rights and freedoms of the data subjects, as well as other potential harms they may result to if the threats materialise. Second, by addressing the likelihood of those events happening, the assessor ought to analyse the threat events within the context of the processing environment, identifying sources of the threat and the possibilities of their exploiting the vulnerabilities surrounding the data processing. Third, by addressing what will be the consequences should the threats materialise, the risk assessor ought to evaluate the level of the impact or harms to the data subjects (the severity in the parlance of the GDPR), again, including the harm related to the rights and freedoms of the data subjects. This calibration, arguably, makes it easy to identify the objectives of risk assessment under Article 35 (7)(c)

[422] ISO/IEC 29134:2017, 16.

and the factors to be considered when completing this process. Simply, these objectives are:

i. To identify the assets, threats, vulnerabilities and harms that may accrue from the data processing.
ii. To analyse the likelihood and severity of the threats materialising or being exploited due to vulnerabilities.
iii. To evaluate the possible controls and their impact leading to the grading of the residual risk level. The outcome here may lead to further consultation with the supervisory authority under Article 36.

The positive side is that the GDPR already contains some indicators, albeit broadly, of how to achieve these objectives—using the nature, scope, context and purpose of the processing. These indicators could be regarded as the equivalent of the CIA-triad of information security within data protection risk assessment. The CIA triad is an acronym representing Confidentiality, Integrity and Availability.[423] Over the years, these elements have crystallised as a model to guide information security policies within an organisation. The suggestion here is that these indicators in the GDPR, if correctly analysed and further built upon, could be broken into sub-factors and form the building blocks of criteria for conducting a risk assessment during a DPIA. The EDPB has described these indicators as 'conditions' for risk assessment, noting that:

> In short, the concept of **nature** can be understood as the inherent characteristics of the processing. The **scope** refers to the size and range of the processing. The **context** relates to the circumstances of the processing, which may influence the expectations of the data subject, while the **purpose** pertains to the aims of the processing.[424]

[423] In a nutshell, confidentiality is the characteristics that information is not disclosed or accessed by authorised individuals or systems. Integrity is when information has not been corrupted, changed without authorisation, thereby affecting its accuracy and completeness. Availability is the characteristics that information is available to be accessed and used by authorised users when needed. Michael Whiteman and Herbert Mattord, *Principles of Information Security* (5th Edn, Boston, Cengage Learning 2012) 11-16.

[424] EDPB, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (Adopted on 13 November 2019) 9.

During the process of risk identification, for example, a risk assessor could identify the threat and the threat events (that could lead to the data processing operation violating the rights and freedoms of the data subjects) by using the nature, scope, context and purpose of the processing formula. These indicators could further be expanded to achieve the desired granularity; for example, the 'nature' could further be broken into 'the nature of the proposed data processing system' and 'the nature of the proposed data processing operation'.[425] Put differently, a risk assessor could ask, what threats are foreseeable or could be identified given the nature of the system, its functionalities, the data to be processed and the environment in which the system is hosted?

In a nutshell, the interpretation of Article 35 (7)(c) adopted in this study clarifies the missing links seen from other presentations. The approach to use the nature, scope, context, and purpose of data processing as criteria for risk assessment: ranging from risk identification to analysis and evaluation processes, where necessary (further discussed in Chapter Five), supplies the yardstick equivalent to the CIA in information security risk management. Although the AEPD has presented these indicators during the preliminary risk assessment phase to determine if a full DPIA is required, this study sees the value in extending them to the core risk assessment phase of the DPIA.[426] Through this approach, it would be possible for the data controller to assess the risks/threats arising from both the processing as planned (e.g. risk of profiling due to the use of the audit log), as well as the risk of things 'going wrong' in an unexpected way, e.g. the database is hacked. Chapter Five operationalises these metrics through a model of the risk assessment proposed in this study.

3.4.2.4 Measures to address the risk Art. 35 7(d)

Finally, a DPIA is expected to contain the measures mapped out to address the identified risks. Article 35 (7)(d) indicates that such measures could include safeguards and security measures and mechanisms. It is also common knowledge

[425] Compare with the four views to risk identification suggested by Oetzel and Spikermann: system, functional, data and physical environment views. See Oetzel and Spikermann (n 33).

[426] See also the Finnish Office of the Data Protection Ombudsman, 'Risk assessment and data protection planning' <https://tietosuoja.fi/en/risk-assessment-and-data-protection-planning> accessed 2 January 2020.

that measures to ensure data protection span from organisational to technical measures, and examples of such measures cannot be exhausted. The WP29 DPIA guidelines did not also spend time explaining the risk treatment measures. However, in several documents elsewhere, the authorities have talked about technical and organisational measures to address data protection, such as in the CNIL PIA Knowledge Bases,[427] the ICO's guidance on security measures,[428] among others. The EDPS, for its part, described possible approaches to minimising risks and provides some generic controls in his DPIA guidance document. According to the EDPS, such controls may target the likelihood of the threats materialising or the impact should they emerge or both, in appropriate cases. Risk responses could also involve avoiding the risk altogether. The EDPS gives the following examples of grouped generic risk control measures: preventive measures (e.g., staff awareness-raising), detective measures (e.g., logging), repressive measures (e.g., certificate revocation mechanisms to stop the use of compromised credentials), and corrective measures (e.g., keeping backups).[429]

Apart from these examples, many sources have also tried to develop privacy risk control measures, particularly in the framework of data security such as ENISA,[430] ISO,[431] LINDDUN.[432] However, in practice, it behoves the data controller or processor to contextualise the impact assessment, consider as many risk responses as possible, and devise their unique measures of controlling the risk based on the context and environment of the processing. Therefore, it is not

[427] CNIL, 'PIA Knowledge Bases' (n 93).

[428] ICO, 'Security' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/> accessed 12 December 2019.

[429] EDPS, 'Accountability on the Ground Part II' (n 26) 16-17.

[430] See ENISA, 'Risk Treatment' <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-process/risk-treatment> accessed 18 December 2019; ENISA, 'Guidelines for SMEs on the Security of Personal Data Processing' (27 January 2017).

[431] See the ISO/IEC 27000 family of Information Security Management Standards.

[432] See the LINDDUN Privayc Threat Modeling Privacy Knowledge (tables) <https://7e71aeba-b883-4889-aee9-a3064f8be401.filesusr.com/ugd/cc602e_46135199dc0d49308e76f30a1a657cf7.pdf> accessed 18 December 2019.

possible to develop a hard and fast rule on mitigating risk; this is a highly contextual exercise.

3.4.3 Consultations during a DPIA

Consultation is an essential aspect of risk management because it offers an avenue for interaction and exchanging ideas and information among the stakeholders involved in the exercise. The outcome of communication and consultation is used, among other things, in describing the context of the risk assessment, identifying the risks, as well as considering the options for addressing those risks. The GDPR has identified some stakeholders for consultation during a DPIA. These are the DPOs, the data subjects and the supervisory authorities. However, this does not preclude consultation with any other persons or entities once the intention is to gather as much valuable input as possible for the success of the DPIA. Below, the various inputs expected from these stakeholders shall be examined.

3.4.3.1 DPOs

The GDPR requires data controllers and processors to designate a data protection officer in certain circumstances, who shall be responsible for ensuring that their organisation is aware of, and complies with, its data protection responsibilities.[433] Article 39 creates the tasks of the DPO, which includes, among other things, providing advice regarding a DPIA and monitoring its implementation as required by the GDPR. This function is also reiterated in Article 35 (2) to the extent that it is mandatory to obtain the advice of the DPO in the course of conducting a DPIA, where such a position is designated. These advisory and monitoring tasks are essential so that the expertise of the DPO can be leveraged in the best possible ways to protect personal data. In performing these tasks, the DPO shall 'have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing'.[434]

[433] See GDPR, art 37; see also Detlev Gabel and Tim Hickman, 'Chapter 12: Impact Assessments, DPOs and Codes of Conduct – Unlocking the EU General Data Protection Regulation', *White & Case* (5 April 2019) <https://www.whitecase.com/publications/article/chapter-12-impact-assessments-dpos-and-codes-conduct-unlocking-eu-general-data> accessed 31 August 2019.

[434] See GDPR, art 39 (2).

The WP29 has fleshed out this provision and recommends that the controller should seek the advice of the DPO in the following cases:

> • whether or not to carry out a DPIA;
> • what methodology to follow when carrying out a DPIA;
> • whether to carry out the DPIA in-house or whether to outsource it;
> • what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects;
> • whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR.[435]

The recommendation goes further to state that if the controller disagrees with the advice of the DPO, such should be documented and justified in writing. While this reinforces the notion that it is the controller who is ultimately responsible for the DPIA, decisions contrary to the advice of the DPO may have a negative effect, especially in circumstances where a breach occurs in a situation that the DPO has advised against. In practice, though, the data controller and the DPO are likely to work hand-in-hand, with the DPO playing a substantial role during a DPIA. Therefore, it is submitted that the DPO's contribution to the foreseeability of risk plays is a crucial role in determining whether the data controller used the right expertise to identify and address risks during a DPIA. This argument is exemplified in Chapter Five. On this premise, it is logical to attribute a critical role to the DPO during a DPIA, a duty they should discharge without undue influence by the data controller.

3.4.3.2 Data subjects

The role of data subjects during a DPIA is indicated in Article 35(9), which provides that where appropriate, the controller shall seek their views or that of their representatives on the intended processing. The language of this provision suggests that it is not in all cases that the data subjects should be consulted. The WP29 interprets it this way when it wrote that the view of the data subjects 'could be sought […] depending on the context'.[436] Although there is no hard and fast rule

[435] WP29, 'Guidelines on Data Protection Officers ('DPOs')' (Adopted on 13 December 2016) WP 243, 17 <http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf> accessed 31 August 2019.

[436] WP29, 'Guidelines on DPIA' (n 56) 15.

as to when to consult the data subjects, it is important to consult them nevertheless because they have the first-hand experience of what harms have resulted or could result from processing their data, and could bring their experiences to bear in threat and harm identification. Consulting the data subjects also shows transparency on the data controller and the desire to consider their interests right from the start of the proposed data processing.

There are various ways of consulting with the data subjects, including a survey, opinion poll, public forum and conferences or workshops, individual consultation, etc. The WP29 notes that the process of seeking the consent of data subjects for data processing does not qualify as consultation within the meaning of this provision. However, consultation should be evident as to its purpose, although the data controller may disagree with the views of the data subjects in the end.

3.4.3.3 Supervisory Authorities

Recital 94 of the GDPR states that the supervisory authority should be consulted before starting any processing activities where a DPIA:

> indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation.

This is reinforced by Article 36 (1) of the GDPR. Although there seems to be confusion about when to consult a supervisory authority, Recital 84 suggests that the authorities shall be consulted only when the residual risk is still high after treating the inherent risks. It is our view that such a position represents a correct interpretation of Artice 36 and accords with the WP29 recommendation that '[i]t is in cases where the identified risks cannot be sufficiently addressed by the data controller (i.e. the residual risks remain high) that the data controller must consult the supervisory authority.'[437] Otherwise, they would be consulted in almost every case, and this will be too burdensome for them and may defeat the aim of a DPIA.

[437] WP29 Guidelines on DPIA (n 56) 19.

When reviewing a DPIA upon consultation, the supervisory authority shall, among other things, consider whether the 'controller has insufficiently identified or mitigated the risk'.[438] The authority shall also advise the data controller regarding the DPIA, given its expertise and may request information from the data controller or processor in order to issue an opinion on the proposed data processing or other tasks.[439] Equally, the data controller shall inform the supervisory authority of 'the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation'.[440] The authorities can order the controller to adopt specified measures for the proposed processing operation or even prohibit the proposed processing, among other options, as per their powers under Article 58(2)(d) and (f) of the GDPR.

Apart from the cases where the supervisory authority is consulted because of the 'residual high risks', Member States national law may require such consultation on other grounds.

3.4.3.4 Other Stakeholders

Apart from the stakeholders mentioned above, a data controller could still consult others in appropriate cases, such as workers, experts, processors, etc., who know the nature of the data processing system. Overall, communicating and consulting with relevant stakeholders during a DPIA is vital for any risk management framework. It could be leveraged to tap into the experiences and expertise of these stakeholders. Moreover, the GDPR undoubtedly encourages such consultations as it is an avenue to identify and mitigate the risks to the data subjects.

3.4.4 Documentation of DPIA

Documentation is an important aspect of the GDPR's compliance framework. There is a general obligation for data controllers and processors to keep a record of processing activities under their responsibility according to Article 30 of the

[438] See GDPR, art 36 (2).

[439] See GDPR, arts 58(1)(a) and (e).

[440] See GDPR art 36 (3) (c) and (e).

GDPR. Documenting the process of a DPIA is a natural consequence of its purpose; it enables the data controller to demonstrate compliance and therefore has to be presented as evidence when required. Moreover, as Korff and Georges rightly note, DPIA records are essential 'in dealing with any queries from DPAs, whether acting in their general supervisory capacity or in response to a complaint.'[441]

The GDPR does not provide a precise format for drafting a DPIA report. However, Article 35 (7) indicates a minimum content of a DPIA, which invariably ought to reflect in a DPIA report. Publishing a DPIA is not mandatory, as pointed out by the WP29 in the DPIA guidelines. However, it recommends that to foster trust and demonstrate accountability and transparency (especially where a public authority is involved), data controllers should publish their DPIA or part of it.[442]

3.4.5 Consideration of Codes of Conduct

Another relevant factor to consider when conducting a DPIA is compliance with approved codes of conduct (Article 35 (8)). Such consideration is based on the premise that several sectors use codes of conduct to implement specific rules practically. If adhered to, it is more likely to improve the rule execution.[443] Thus, specific codes of conduct that are relevant and tailored for data protection per Article 40 of the GDPR should be considered in the course of a DPIA, given that such codes would have been made through collaborative efforts of experts in the sector concerned. For example, there is the EU Cloud Code of Conduct for cloud computing service providers.[444] Also, the WP29 suggests that data protection certifications, seals and marks, as well as Binding Corporate Rules, should be considered during a DPIA.[445]

---

[441] Korff and Georges, 'The DPO Handbook' (n 412) 205.

[442] WP29, 'Guidelines on DPIA' (n 56) 18.

[443] See FRA, *Handbook on European Data Protection Law* (2018 edition, Publication office of EU) 181-182.

[444] EU Cloud CoC, 'About EU Cloud Code of Conduct' <https://eucoc.cloud/en/home.html> accessed 12 January 2020.

[445] WP29 'Guidelines on DPIA' (n 56) 16.

3.4.6 Review and Change of the Risk

Article 35 (11) requires a review of the DPIA by the data controller, mainly when there is a change in the risk presented by the data processing operation. This provision points to the fact that risk assessment is a continuous process and not a one-off product. As such, constant monitoring of the system is necessary to identify both internal and external changes that could affect the risk assessment.[446] For example, a change in the purpose of the use of data is a factor that can necessitate a review of the DPIA. So too might a change in the surrounding technology, e.g. if a new security vulnerability becomes known that renders the existing way of safeguarding the data no longer as secure.

There was an attempt by the Parliament during the negotiation of the GDPR to require a review of a DPIA 'periodically at least once every two years, or immediately when there is a change in the specific risks presented by the processing operations'.[447] Unfortunately, the suggestion was not reflected in the final text of the Regulation. However, in the context of interpreting Regulation (EU) 2018/1727 on data protection by EU institutions, the EDPS recommends a review cycle of two years, although it leaves it ultimately to the data controller to choose the length depending on the risk. As a rule of thumb, the EDPS suggests that 'the higher the risk, the shorter the review cycle should be'.

In summary, the provisions of Article 35 and allied articles, as discussed above, expose what data controllers ought to do to comply with the DPIA obligation. The table below breaks down these provisions into five columns, representing aspects that the data controller should consider when planning or conducting a DPIA.

[446] Ibid, 14.

[447] See Article 33a of the text adopted by the Parliament <https://edri.org/files/EP_Council_Comparison.pdf> accessed 2 September 2019.

Table 1: Breakdown of five essential parts of the provisions of Article 35 GDPR

A	B	C	D	E
What data processing operation will require a DPIA or not?	***Whom to consult when carrying out a DPIA?***	***What to consider when carrying out a DPIA?***	***What will be the minimum content of a DPIA?***	***When to review the DPIA?***
Art. 35 (3)	Art. 35 (2) – DPO	Art. 35 (1)	Art. 35 (7)	Art. 35 (11)
Art. 35 (4)	Art. 35 (9) – Data subjects	Art. 35 (8)		
Art. 35 (5)	When the residual risk is still high, Art. 36 applies – SA			
Art. 35 (10)				

The basic framework of a DIPA under Article 35 could also be represented diagrammatically, as shown in the figure below.

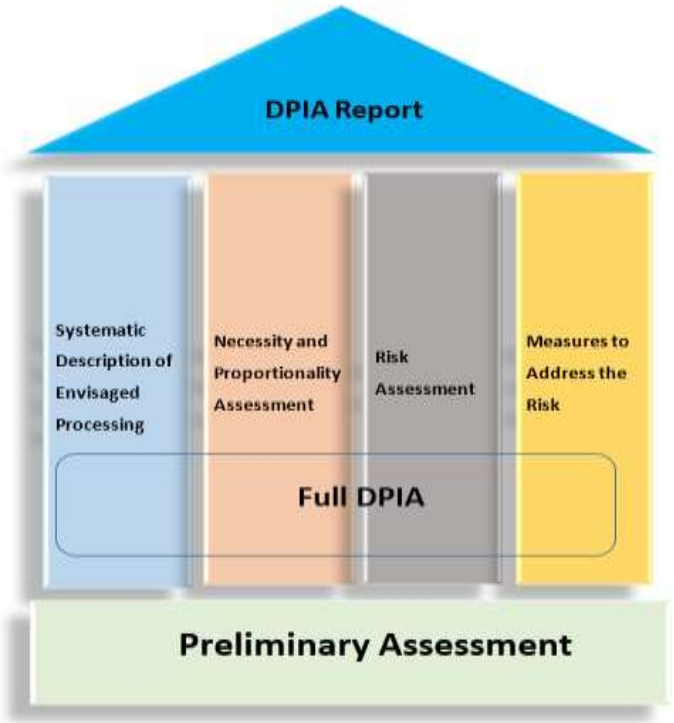


Figure 8: The basic framework of a DPIA under the GDPR

The diagram shows that a DPIA flows from the outcome of a preliminary assessment. Where the outcome indicates that the processing involves a high risk,

then a full DPIA shall be conducted, reflecting the minimum requirement under Article 35 (7) of the GDPR. Finally, the whole exercise of the DPIA is documented in a report.

3.5 NON-COMPLIANCE WITH ARTICLE 35

Similar to other provisions of the GDPR, non-compliance with the obligation created by Article 35, that is, to conduct a DPIA, is a violation of the Regulation and attracts penalty, which spans from compensation to the data subjects to fines by supervisory authorities (see Articles 82 and 83). Article 84 indicates that penalties shall be effective, proportionate and dissuasive. Furthermore, the amount of fines has been increased under the GDPR. Article 83 (4) indicates that an infringement of Article 35 can 'be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.'

A few instances could be cited to buttress this point. The Norwegian Datatilsynet recently fined Rælingen municipality 800 000 NOK concerning the data breach in the school app Showbie. The fine was based, among others, for not conducting a DPIA according to Article 35 GDPR before processing special categories of personal data.[448] Similarly, the French Conseil d'Etat noted that non-compliance with the DPIA obligation could attract a sanction by the CNIL under Article 20 of the French Data Protection Act of January 6, 1978.[449] The court rejected the plea of ignorance by the data controller. It noted that a DPIA must be carried out prior to the processing operation and updated after the process started to ensure that data subjects are always protected against the risks to their rights and freedoms.

[448] Datatilsynet, 'Varsel om vedtak om overtredelsesgabyr Rælingen kommune' (19/01478-6/KBK, 26 February 2020). See also GDPRhub, 'Datatilsynet - 19/01478-6' (GDPRhub, last updated 11 March 2020) <https://gdprhub.eu/index.php?title=Datatilsynet_-_19/01478-6> accessed 28 March 2020.

[449] Case N° 434376 (ECLI:FR:CECHR:2019:434376.20191106) <https://www.legifrance.gouv.fr/affichJuriAdmin.do?oldAction=rechJuriAdmin&idTexte=CETATEXT000039335911&fastReqId=1217807024&fastPos=1>. See also GDPRhub, 'CE - N° 434376' (GDPRhub, last updated 17 January 2020) <https://gdprhub.eu/index.php?title=CE_-_N%C2%B0_434376> accessed 28 March 2020.

Furthermore, the District Court of Hague noted that a DPIA carried out before the entry in force of the GDPR could not meet the requirements under the national data protection act and Article 35 GDPR.[450] The above examples show that non-compliance with the provision of Article 35 exposes a data controller or processor to sanction involving a significant amount. Non-compliance, arguably, can result from not conducting DPIA appropriately. As we await further decisions in this area, it is notable, as we had argued in Chapter One, that the positive impact of an appropriate DPIA is not clearly pronounced in the current framework. It is suggested that future developments in this area should consider incentivising good practices around DPIA.

The following section will distinguish DPIA and related data protection tools such as PIA, prior checking, privacy audit, and data protection by design. This aims to understand the similarities and differences among these tools and the synergy that exists among them.

3.6 Distinguishing DPIA from Related Data Protection Tools and Concepts

Although DPIA has been presented in the sections above as a risk management tool, other tools of a similar nature exist under European data protection law. The discussion below shall attempt to distinguish these tools from a DPIA.

3.6.1 DPIA vs PIA

When a DPIA is mentioned, a question is whether it is the same thing as a PIA. This question could be understood in light of the differences between the philosophical dimension of privacy and data protection, which scholars have tried to answer from various angles. However, a simple answer to the above question is that PIA and DPIA share similar concepts and familiar features, though different in their scope of application (a PIA is broader in scope).[451] Both could be regarded as instruments of risk management aimed at discovering problems that may affect

[450] Case No. ECLI:NL:RBDHA:2020:1878. See also GDPRhub, 'Rb. Den Haag - C/09/550982/HA ZA 18/388' <https://gdprhub.eu/index.php?title=Rb._Den_Haag_-_C/09/550982/HA_ZA_18/388> accessed 28 March 2020.

[451] See David Wright and Charles Raab, 'Privacy Principles, Risks and Harms' (2014) 28 (3) IRLCT 277, 294.

personal data undergoing processing and finding solutions to those problems. Both are also 'anticipatory in nature' in terms of focusing on what is yet to happen (e.g., ideally carried out before a project begins, before the risk occurs). Perhaps, because of these common features, most authors tend to use both terms interchangeably. For example, the WP29 notes that 'the term "Privacy Impact Assessment" (PIA) is often used in other contexts to refer to the same concept [DPIA],'[452] and the CNIL states that DPIA 'is more commonly referred to as a Privacy Impact Assessment (PIA)'.[453]

However, it is essential to point out that despite this interchangeability, historically, PIA could be said to be the forerunner of DPIA, and appears broader in scope, as earlier noted, if we consider privacy as a multi-dimensional concept with fluid boundaries. In that case, a PIA encompasses other dimensions of privacy, of which informational privacy or data protection is one aspect.[454] As Clarke suggests, the scope of a PIA is broader concerning 'the perspectives reflected in the process'.[455] The confusion in the usage of these terms has arisen mainly as observed by Wright and Raab because various frameworks for PIA implementation only consider the informational privacy or data protection aspect.[456]

[452] WP29 (n 56) footnote 2 at page 4.

[453] CNIL, 'PIA Methodology' (n 76) 2. The ICO guidance on DPIA also notes that 'DPIAs are very similar to PIAs'. See ICO, 'What's new under the GDPR?' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-s-new-under-the-gdpr/#whatsnew1> accessed 31 July 2019.

[454] Clarke, 'Privacy Impact Assessment: its Origin and Development', (2009) 25 Computer Law and Security Review, 124; Roger Clarke, 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms', http://www.rogerclarke.com/DV/Intro.htmlhttp://www.rogerclarke.com/DV/Intro.html; Wright and Raab (n 474); see also Chapter 2 of this Dissertation.

[455] Clarke, 'Privacy Impact Assessment: its Origin', ibid, 124-125; See also Roger Clarke, 'Approaches to Impact Assessment' <http://www.rogerclarke.com/SOS/IA-1401.html> accessed 31 July 2019.

[456] Wright, 'Privacy Principles, Risks and Harms' (n 451) 293, eg the RFID PIA framework considered only principles for data protection.

It could then be argued that a DPIA is an aspect of a PIA that concentrates on personal data protection.[457] This view is supported by the fact that Article 35 of the GDPR streamlines the impact assessment it instructs to 'protection of personal data', indicative of the limited scope of its application. A PIA, it has to be said, has no similar detailed provision in EU data protection legislation.

3.6.2 DPIA vs Prior Checking

DPIA and prior checking have a lot in common; both have similar objectives, and their timing is the same (before the processing starts). However, the addressees of the two requirements are not the same. During the life of the DPD, the entity responsible for prior checking under Article 20 of the DPD was the Member States' supervisory authorities upon notification by the data controller or by 'the data protection official'. Here, data protection authorities were expected to check any data processing operation that may pose a risk to the rights and freedoms of the data subjects, and give their opinion or authorisation regarding such processing. Prior checking may also take place regarding legislative measure taken by a Member State that involves personal data processing.[458] On the other hand, the GDPR directly places the obligation of carrying out a DPIA on the data controller or, where appropriate, a processor. 'Prior consultation' with a supervisory authority only happens as a second step if the residual risk remains high, according to a DPIA carried out under Article 35.[459]

In fact, it is notable that under the DPD regime, only a few Member States implemented the prior checking provision. This was done differently, ranging from onsite inspection by the supervisory authority to completing a questionnaire by

[457] In general, there have been a lot of publications on the differences between privacy and data protection which could help in shaping this discussion. See footnote 59. See also Maria Tzanou 'Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a not so New Right', International Data Privacy Law, 2013, Vol. 3, No. 2; András Jóri, 'Data Protection Law - An Introduction' <http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.Privacy> accessed 31 July 2019.

[458] See DPD, recital 54.

[459] See GDPR, art 36.

the data controller or carrying out a PIA.[460] On the other hand, a DPIA is uniformly implemented under the GDPR, which also provides its minimum content. Furthermore, unlike the DPD era of prior checking, where only a few data controllers notified the authorities of such risky ventures, supervisory authorities have published lists of processing activities requiring a DPIA and those that do not (so-called blacklist and whitelist), making the situation more systematic and precise.[461]

3.6.3 DPIA vs Privacy Audit

Privacy audit or compliance check[462] is a tool for checking the compliance exposure of an existing information system used for processing personal data.[463] Neither the DPD nor the GDPR expressly requires or defines a privacy audit. However, the tool is regarded as a systematic and independent process, which gathers evidence about a data processing system and compares it with specific criteria to measure the system's compliance with data protection law.[464] Just like audits in other areas, a privacy audit also follows a defined procedure and pattern. It shows the data flow throughout the data life-cycle phases: from collection to destruction, as well as mechanisms and policies adopted to ensure compliance with relevant laws. [465]

---

[460] See Wright, *Privacy Impact Assessment* (n 34) 97-116.

[461] See the discussion in Section 3.4.1.

[462] Privacy audit and a compliance check share common attributes, and in fact used interchangeably in some quarters. See Wright, *Privacy Impact Assessment* (n 34) 151.

[463] The UK ICO Data has defines a data protection audit as: 'A systematic and independent examination to determine whether activities involving the processing of personal data are carried out in accordance with an organisations data protection policies and procedures, and whether this processing meets the requirements of the Data Protection Act 1998.' See for example the ICO Data Protection Audit Manual (Version 1, June 2001) 4 <https://www.cmpe.boun.edu.tr/~ozturan/etm555/dataaudit/html/download/pdf/audit_all.pdf> accessed 12 December 2019.

[464] See ISO/IEC 19011:2002; Jeremy Rissi and Sean Sherman, 'Cloud-Based IT Audit Process' in Ben Halpert (Ed), *Auditing Cloud Computing – A Security and Privacy Guide* (John Wiley & Sons 2011); R Pompon 'IT Security Risk Control Management: An Audit Preparation Plan' (Apress, 2016); P Duscha 'Audit, Continuous Audit, Monitoring
und Revision' in Sowa/Duscha/Schreiber (Eds), *IT-Revision, IT-Audit und IT-Compliance – Neue Ansätze für die IT-Prüfung* (Springer, 2015).

[465] Muzamil Riffat, 'Privacy Audit—Methodology and Related Considerations'

A DPIA and a privacy audit share some similarities: they are process-oriented, geared towards ensuring compliance with data protection law and showing accountability.[466] Both tools could be used to evaluate a process or a product, as well as for the whole system, and could be carried out by internal or external experts (auditors, a third party). However, they are distinguishable in the timing and, to some extent, in scope. While a DPIA is expected to be carried out before the data processing begins (although it could also be conducted for ongoing processing), a privacy audit always takes place when the data processing system is already running,[467] and may be targeted at only a limited scope of compliance sources such as enablement of data subjects rights or international data transfer. Wright et al., also note that while an impact assessment is used to identify risks and mitigate those risks, a privacy audit 'is used to check that the PIA was properly carried out and its recommendations implemented'.[468] To that extent, the two processes may be seen as complementary.

3.6.4 DPIA vs Privacy/Data Protection by Design and by Default

The idea of using technology that threatens privacy to safeguard privacy interests at the same time metamorphosed into the notion of privacy by design, a concept that centres on embedding privacy consideration into the design specifications of technologies that process personal data or could affect privacy in general.[469] Ann Cavoukian, one of the concept's originators, believes that 'privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organisation's default mode of operation.'[470]

<https://www.isaca.org/Journal/archives/2014/Volume-1/Pages/Privacy-Audit-Methodology-and-Related-Considerations.aspx> accessed 31 July 2019.

[466] See ibid; ISO/IEC 19011:2011.

[467] Nigel Waters, 'Privacy Impact Assessment – Great Potential Not Often Realised' in David Wright and Paul De Hert (eds), *Privacy Impact Assessment* (Springer, 2012) 151.

[468] PIAF Deliverable D1 (n 34) 189.

[469] Lee Bygrave, 'Hardwiring Privacy' University of Oslo Faculty of Law Research Paper No. 2017-02.

[470] Ann Cavoukian 'Privacy by Design: The 7 Foundational Principles' (2009, revised 2011) <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf> accessed 31 July 2019.

This, she suggests, may be achieved by building the principles of fair information practices into the design, operation and management of information processing technologies and systems. She further develops seven fundamental principles of privacy by design.[471]

Over the last decade, privacy by design has been promoted in various data protection discussions.[472] The European Commission, the WP29 and EDPS, have made several policy pronouncements recommending privacy by design. [473] Currently, it seems to be an integral part of EU data protection law under the nomenclature of data 'protection by design and by default' (a term used in the GDPR), although some commentators maintain that both terms have some differences in meaning and scope.[474] This point is also highlighted in the recent preliminary opinion of the EDPS, which designates the term 'privacy by design' to the broad concept of technological measures for ensuring privacy as it has developed in an international debate over the last few decades, while 'data protection by design' and 'data protection by default' refer to the specific legal obligations established by Article 25 of the GDPR.[475] Subtle as this demarcation might be, common usage of both terms suggests that they convey a similar philosophy, primarily focusing on the measures undertaken to protect privacy.

Although the DPD did not explicitly use the term privacy by design or data protection by design, it reflected the practical intent of the concept in several provisions. It may be recalled that Recital 46 of the DPD required that 'appropriate

[471] Ibid.

[472] In 2010, the 32nd International Conference of Data Protection and Privacy Commissioners unanimously passed a resolution recognising it 'as an essential component of fundamental privacy protection' and encourage 'the adoption of Privacy by Design's Foundational Principles […] as guidance to establishing privacy as an organization's default mode of operation' International Conference of Data Protection and Privacy Commissioners 'Resolution on Privacy by Design' (27-29 October 2010) 2 <https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf> accessed 31 July 2019.

[473] See for example: EDPS, 'EDPS opinion on privacy in the digital age: "Privacy by Design" as a key tool to ensure citizens' trust in ICTs', <https://edps.europa.eu/press-publications/press-news/press-releases/2010/edps-opinion-privacy-digital-age-privacy-design_en>.

[474] See Bygrave, 'Hardwiring' (n 469).

[475] EDPS, 'Opinion 5/2018 Preliminary Opinion on privacy by design', (31 May 2018) 1.

technical and organisational measures be taken, *both at the time of the design of the processing system and at the time of the processing itself*.'[476] This statement was further buttressed in Article 17 of the DPD that focused on data security. Also, the e-Privacy Directive contains a related provision requiring that privacy is given due consideration right from the design of the system.[477] As noted, Article 25 of the GDPR now incorporates the concept of data protection by design and by default explicitly. It requires that 'the controller shall both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures' to meet the requirements of the GDPR and protect the rights of the data subjects. A similar duty is laid down in Article 20 of the Directive 2016/680 on Data Protection and Law Enforcement.

Data protection considerations must be factored into a product, service or project by default (data protection by default) where pre-configuration is set before releasing the product or service. Such pre-configurations or settings must be carefully chosen to the advantage of the data subjects so that only necessary personal data shall be processed to achieve specific purposes—data minimisation principle.[478] Data subjects should also be able to reset this at their choosing, an approach that shall continue throughout the life cycle of the data processing operations.[479]

Under the GDPR, data protection by design and DPIA share a lot in common. Their implementation time is the same (at the time of determination of the means for processing; prior to data processing), enabling both tools to identify and assess the data protection risks proactively and suggest mechanisms to be engineered

[476] Italics are for emphasis.

[477] See Recital 30, Articles 4 (1) and 14 (3).

[478] See EDPB, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (Adopted on 13 November 2019).

[479] See Lee Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements', (2017) 4:2 Oslo Law Review.

into the system's architecture to mitigate those risks.[480] In this regard, a DPIA is an integral part of taking data protection by design approach because the output of a DPIA forms input in designing the system. As such, both tools are complementary and used to show accountability. For example, for an organisation to implement appropriate measures both on an organisational and technical level by default, a DPIA is necessary to identify what measures are appropriate. In the same vein, the data protection by design approach adopted by a system could equally be relied upon in the DPIA as a factor in the risk assessment and mitigation processes.[481]

Another essential feature of both tools is that several similar factors are considered during both DPIA and data protection by design, such as the nature of the data concerned; the scope, context and purposes of processing such data; the risks to an individual's privacy and the likelihood (and severity) of the risk happening during the data processing.[482] Both tools are used to check how the data protection principles are translated in the processing, and they take certification and code of conduct into account as evidence demonstrating compliance with the GDPR. A review is integral to both tools; their outcomes require regular monitoring and review through the life cycle of the system's operation. Moreover, both tools will require documentation to show how they have been implemented. In practice, there are several methodologies on how to operationalise data protection by design as well as how to carry out a DPIA.

However, there are some differences between the two concepts regarding the requirements that trigger each obligation and the execution methodology.[483] First,

---

[480] Peter Bolger and Jeanne Kelly, 'Privacy by Design and by Default' <https://www.lexology.com/library/detail.aspx?g=72cdafaa-9644-453c-b72c-3d55dc5dc29d> accessed 1 August 2019; EDPB, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (n 478) 10

[481] For example, adopting measures such as pseudonymisation and anonymization which are instances of data protection by design could be considered as a risk mitigating factor in a DPIA.

[482] See GDPR, arts 25 and 35.

[483] Bygrave points out the differences in these words:

> The 'by design' requirements of Article 25(1) differ from the 'by default' requirements of Article 25(2) in several respects. The former cover a potentially wider range of data

concerning data protection by design, Bygrave notes that the duty imposed by Article 25(1) is qualified by an extensive list of contextual factors, which will be determined to a significant extent (but not exclusively), by the output of the DPIA that the controller carries out. [484] Secondly, although both target the implementation of the data protection principles, privacy by design has achieved some foundational principles of its own since its inception, which is not the case with DPIA.[485]

3.7 CONCLUSION

This chapter has, among other things, attempted an interpretation of the various provisions of Article 35 of the GDPR and shown the feasibility of using a systematic approach to complete a risk assessment during a DPIA. Notably, it has demonstrated that Article 35 (7)(c) can achieve a functional framework that demarcates the steps of risk assessment into risk identification, analysis and evaluation, which allows for seamless threat identification and harm analysis as they related to the rights and freedoms of the data subjects. Furthermore, given the nature of the obligation created by Article 35, a distinction can also be made between DPIA and related risk management tools such as PIA, prior checking, privacy audit, data protection by design, seen in data protection law.

---

protection measures than the latter, which focus, in effect, simply on keeping data 'lean and locked up'. And while the former appear to be process-oriented to a considerable degree (this follows partly from its 'design' focus), the latter are more concerned with results that guarantee – at least as a point of departure – protection with respect to data minimisation and confidentiality. In other words, the latter go well beyond a soft paternalism that simply nudges information systems development in a privacy-friendly direction without seeking to 'hardwire' privacy enhancement in concrete ways. Bygrave, 'Data Protection by Design and by Default:' (n 504) 116.

[484] Ibid, 115.

[485] Cavoukian seven privacy by design foundational principles is good examples of the privacy by design principles. These principles are:

1. Proactive not Reactive; Preventative not Remedial;
2. Privacy as the Default Setting;
3. Privacy Embedded into Design;
4. Full Functionality — Positive-Sum, not Zero-Sum;
5. End-to-End Security — Full Lifecycle Protection;
6. Visibility and Transparency — Keep it Open;
7. Respect for User Privacy — Keep it User-Centric.

Cavoukian, 'Privacy by Design: The 7 Foundational Principles' (n 495). See also Christoph Bier, et al, 'Enhancing Privacy by Design from a Developer's Perspective' in Bart Preneel and Demosthenes Ikonomou (eds), *Privacy Technologies and Policy: First Annual Privacy Forum, APF 2012* (Springer Verlag 2014).

As previously hinted at, the data protection supervisory authorities of different EU member states have issued various guidelines on implementing the provisions of Article 35. In the next chapter, a comparison of these approaches from the DPIA guidance documents shall be made to highlight their discrepancies and gaps, as well as suggest ways of harmonising these guidelines in the future.

CHAPTER FOUR

4. APPROACHES AND GUIDELINES FOR CONDUCTING IMPACT ASSESSMENT: A REVIEW

4.1 INTRODUCTION

In the previous chapter, an analysis of the risk-based approach was further made to show the intention behind its introduction, mainly related to Article 35 of the GDPR. This involved a detailed discussion of the individual clauses of Article 35 as further elaboration on the issues identified in Chapter One regarding the operational aspect of DPIA. In this chapter, a literature review shall be made to zoom in further on the approaches and guidelines identified for conducting impact assessment from the era of the DPD to the present regime. First, a discussion on the common pathways identified shall be introduced before comparing various DPIA guidelines from EU supervisory authorities. In the end, the aim is to understand what it entails when completing an impact or risk assessment process. Similarities and differences in the approaches shall be identified, and possible room for harmonising and systematising the framework across the EU in the future shall be suggested.

4.2 APPROACHES TO CONDUCTING IMPACT/RISK ASSESSMENT IN EU DATA PROTECTION LAW

Risk assessment is now an integral part of the current EU data protection framework, whether it is for implementing data protection by design, technical and organisational data security measures, conducting a DPIA or determining whether to notify supervisory authorities or data subjects in case of a data breach. Although the GDPR has brought to the fore the relevance of risk management in the present EU data protection era, especially by mandating DPIA under certain circumstances, the use of the impact assessment tool predates the GDPR as indicated in Chapter Two. There are numerous approaches to conducting an impact assessment in practice, possibly, because no precise methodology for completing this exercise has been mandated.

Publications on the subject matter have been a mixture of both technically-focused and non-technical works, mainly designed to operationalise PIA/DPIA processes and/or explain the sequence of the processes involved in conducting a PIA/DPIA.[486] On a broad view, there is no uniform impact assessment strategy that emerged from these publications; instead, they suggest two general pathways concerning how impact/risk assessment is conceptualised. The first pathway relates to those who view informational privacy risks in terms of violation of privacy principles and suppose that impact assessment is an exercise of checking compliance with these principles and/or privacy laws that are applicable to the particular processing operation in question. The second pathway relates to those that view impact assessment as a risk management tool that traverses beyond a mere check of privacy principles and relies upon risk management procedure for conducting this assessment.

The following literature review confirms a need to systematise this process, and discusses proposals for such systematisation. It concludes that it is feasible to harmonise and systematise risk assessment procedure for a DPIA, given that the GDPR envisages consistent application of its rules across the Member States.

4.2.1 Impact Assessment Pathways

The first approach to impact assessment, as noted earlier, assumes that informational privacy has codified principles used to determine its violation, and these principles could be transposed into risk terms to determine what events might lead to their violation and the impact should they occur.[487] A statement from Wright and Raab is apt in describing this pathway:

> privacy principles are important because they form the basis for the formulation of questions that organisations can use to determine whether

[486] See Sourya Joyee De and Daniel Le Métayer, 'PRIAM: A Privacy Risk Analysis Methodology (Research Report n° 8876 — version 1.0 2016); Kloza et al, 'Towards a Method for Data Protection Impact Assessment' (n 399); Kloza et al, 'Data Protection Impact Assessment in the European Union' (n 70).

[487] Wright, 'Privacy Principles, Risks and Harms' (n 451).

> their new technology, system, project or policy might pose risks to one or more types of privacy.[488]

On this basis, Wright and Raab map examples of risks and harms from these privacy principles, although they acknowledge that it is not a compressive risk-mapping tool. They also claim to have added a 'more systematic, structured approach to privacy risk identification, assessment and management',[489] but there is no substantial evidence to validate such a claim from their work: no structured risk assessment model could be identified for quantifying the risk levels of violating these privacy principles. The significance of their work, arguably, lies in their efforts to expand the principles beyond those of informational privacy rather than developing a methodology of privacy risk assessment.

This pathway, nevertheless, has been reflected in other works. An example is De Hert's statement equating a DPIA to 'simply checking the legal requirements spelt out in the European data protection framework'. However, as we have argued in this study, a DPIA procedure extends beyond mere compliance checks with data protection principles or specific laws. It extends to anticipating future threats from the various stakeholders' perspectives—data subjects, regulatory authorities and sectoral perspective. Regrettably, several PIA templates have tended to regard an impact assessment (PIA or DPIA) as an exercise of checking compliance with data protection principles or particular data protection law. DPIA templates from the Family Link Network of the International Committee of the Red Cross,[490] the Bitkom's *Risk Assessment and Data Protection Impact Assessment Guide*[491] and PIA

[488] Ibid, 279.

[489] Ibid, 289-291.

[490] Family Links Network, 'Code of Conduct for Data Protection Template for Data Protection Impact Assessment (DPIA)' <https://www.icrc.org/en/download/file/18149/dpia-template.pdf> accessed 9 December 2019. See also DroneRulesPro, 'Data Protection Impact Assessment Template' <https://dronerules.eu/assets/files/DRPRO_Data_Protection_Impact_Assessment_EN.pdf>.

[491] Bitkom, 'Risk Assessment & Data Protection Impact Assessment Guide (Berlin 2017) 40-42 <https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2017/Leitfaden/170919-LF-Risk-Assessment-ENG-online-final.pdf> accessed 9 December 2019.

proposal by the Dutch administration [492] replicate this approach. For example, in the Red Cross template, the data protection principles were transposed into data protection issues, followed by examples of risks and mitigation measures associated with each issue. There is, however, no methodological framework regarding how the assessment of risks should be done, leaving it open to the risk assessor to rely on intuition. The proposed Dutch model takes the form of a test or questionnaire to check privacy principles, whose 'content is intended to be both direction-giving and corrective.'[493] In the end, this approach fails to highlight impact assessment as a risk management exercise, and it is challenging to distil how privacy risk is identified and mitigated after completing a set of questionnaires.

The second pathway comprises works that discuss a more or less coherent methodology for conducting a PIA or DPIA as a risk management tool, where elements of risk identification, analysis and evaluations could be identified. These publications include those that are technically oriented[494] or legally focused/or a combination.[495] For the technical works, Joyee De and Le Métayer, for example, argue that guidelines from supervisory authorities do not define how to perform the technical part of a PIA, and suggest filling this gap by developing a Privacy RIsk Analysis Methodology (PRIAM) that revolves around seven components (each with its categories and attributes).[496] Similarly, using a data science approach (a more

[492] Matthijs Koot, 'Mandatory Privacy Impact Assessments for Dutch Government IT Projects' (Infosec Island, 24 October 2013) <http://www.infosecisland.com/blogview/23441-Mandatory-Privacy-Impact-Assessments-for-Dutch-Government-IT-Projects-.html> accessed 7 July 2019. The original document is in Dutch, but an English translation was made by the author of this article.

[493] Ibid.

[494] Oetzel, 'A Systematic Methodology' (n 33); Joyee De, 'PRIAM' (n 486); Majed Alshamari and Andrew Simpson, 'Towards an Effective Privacy Impact and Risk Assessment Methodology: Risk Analysis' in Joaquin Garcia-Alfaro et al (eds) *Data Privacy Management, Cryptocurrencies and Blockchain Technology* (ESORICS 2018 International Workshops, DPM 2018 and CBT 2018, Barcelona, Spain, September 6-7, 2018, Proceedings); Isabel Wagner and Eerke Boiten, 'Privacy Risk Assessment: From Art to Science, by Metrics' in Joaquin Garcia-Alfaro et al (eds) *Data Privacy Management, Cryptocurrencies and Blockchain Technology* (ESORICS 2018 International Workshops, DPM 2018 and CBT 2018, Barcelona, Spain, September 6-7, 2018.

[495] See footnote 35; Felix Bieker et al, 'A Process for Data Protection Impact Assessment under the European General Data Protection Regulation' in S. Schiffner et al. (eds) APF 2016 LNCS 9857, 29-30.

[496] Joyee De, 'PRIAM' (n 486).

technically oriented approach), Oetzel and Spiekermann suggest a seven-step PIA methodology based on the German BSI risk method.[497] They frame a description of a system for privacy risk identification in four views: system view, functional view, data view, and physical environment view;[498] translate the privacy principles into concrete objects or actions identified as 'privacy targets', and further suggest that these targets should be ranked and prioritised based on the impact of the risk.[499] They also quantify the consequences of privacy breach qualitatively—three levels of consequences: limited and calculable; considerable; and devastating consequences. Correspondingly, they rank impacts of the consequences as low, medium or high protection demand.[500] Surprisingly, they depart from the conventional approach of using probability to determine the threat events, arguing against 'a gradual determination of threat probability as is done in security assessments'; instead, they prefer to consider whether a threat exists rather than the probability of a threat because in their view, 'if the threat is likely to exist, a control must be determined to mitigate it.' This position seems to depart from the provisions of the GDPR, which require that the likelihood and severity of the threat and harm be considered in determining the risk.[501] Nevertheless, the duo's contributions are significant in terms of risk identification; their four-view approach reinforces that risk identification could be calibrated to a high degree of granularity.

Other works that fall within this category of using a more technical model for PIA include, but are not limited to, Makri, Georgiopoulou, and Lambrinoudakis'

[497] Oetzel, 'A Systematic Methodology' (n 33) 11.

[498] Ibid, 12.

[499] Based on seven privacy principles derived from the DPD the proposed GDPR, they developed an example of 24 privacy targets. This list is not exhaustive. Ibid, 15.

[500] Ibid, 16. Furthermore, Oetzel and Spiekermann's work contain damage scenarios, although they appear incomplete, especially, for the data subjects whom they assume would suffer damage to reputation, freedoms or finances. Other harms such as societal damage are missing in their scenario. More importantly, they did not indicate or explain the factors that were used in distinguishing the consequence levels.

[501] It is noteworthy that this work was based on the proposed version of the GDPR which significantly changed in the final version. However, see CIPL, 'A Risk-based Approach to Privacy' (n 13).

proposed PIA method using organisational characteristics metrics,[502] the LINDDUN Privacy Threat Modeling,[503] and the NIST privacy engineering model.[504] Apart from these works with a more technical feature, significant research in informational privacy risk that combines both technical and legal dimensions has been done by the CIPL.[505] In a 2014 white paper, the CIPL proposes some objective descriptors of privacy harms and threats.[506] The white paper also developed a matrix to align privacy threats and harms and argues rightly that identifying threats and harms should be contextual in real scenarios. The CIPL did not develop a risk assessment method, but noted that '[t]here is a particular benefit in developing a common and objective approach to risk management and an objective notion of harm or adverse impact to individuals that are acceptable and useful to as many businesses and regulators as possible'.[507] However, surprisingly, in another white paper in 2016, it tends to recommend the opposite:

> The actual process or methodology of risk assessment, i.e. how the various risky activities or threats and harms should be assessed, weighed and evaluated, should largely be left to individual organisations […][508]
>
> We do not believe that risk assessment processes or any weighting or scoring methodology can or should be made uniform, one-size-fits-all and harmonised across different organisations.[509]

---

[502] Eleni-Laskarina Makri, Zafeiroula Georgiopoulou, and Costas Lambrinoudakis, 'A Proposed Privacy Impact Assessment Method Using Metrics Based on Organizational Characteristics' in Sokratis Katsikas et al. (eds) *Computer Security*. CyberICPS 2019, SECPRE 2019, SPOSE 2019, ADIoT 2019 (Lecture Notes in Computer Science, vol 11980. Springer 2019) 122-139.

[503] LINDDUN Privacy Threat Modeling <https://distrinet.cs.kuleuven.be/software/linddun/linddun.php> accessed 9 December 2019.

[504] Sean Brooks et al., 'An Introduction to Privacy Engineering and Risk Management in Federal Systems' (NISTIR 8062, 2017) (n 36).

[505] See footnote 35 for a series of articles in the CIPL project: CIPL, 'Privacy Risk Management'.

[506] CIPL 'A Risk-based Approach to Privacy' (n 13) 6-8.

[507] Ibid, 4; see also CIPL, 'The Role of Risk Management' (n 35)19.

[508] CIPL, 'Risk, High Risk, Risk Assessment' (n 35) 7.

[509] Ibid, 36. Contrast these statement to another where the CIPL stated: 'As a starting point, initial consensus on the nature of "privacy risks", in terms of the threats and harms, would be useful, together with agreed methodologies for assessing likelihood and seriousness and balancing the results against the benefits. […] Tangible damage will be objective and usually easier to assess but, even for intangible distress, assessments cannot be based on subjective perceptions. CIPL, 'A Risk-

Although not much attention has been drawn to whether privacy risk assessment should be standardised, this recommendation raises a few questions and requires further probing to contextualise its scope. In the first place, the CIPL is right to point out that a broad attempt to amalgamate all the areas where risk assessment is required under the GDPR is not feasible, as they may not always synchronise. For example, the risk assessment for a DPIA (mainly ex-ante) and that of a data breach notification (*ex-post*) may not merge; they focus on different contexts. However, the second aspect of the statement, which suggests that risk assessment methodology (we assume including the one for DPIA) should not be harmonised, but instead remain at the individual or organisational level, needs to be further tested. Some scenarios could be envisaged here. First is a situation where all the risk assessment processes (risk identification, risk analysis and risk evaluation) are left open for the risk assessor to develop. The second is a situation where some aspects of the risk assessment are partly standardised, and a set of criteria that indicate the essential requirements or input data leading to a risk-level quantification are established. The risk assessor could improvise here, using the standards. The third is where the entirety of risk assessment processes are standardised, leaving no room for manoeuvre by the risk assessor.

Suppose the CIPL intends the first scenario, which is meant to foreclose the authorities from issuing any systematic or objective risk assessment methodology, even those that organisations could adapt. In that case, we respectfully differ, as this will introduce a high level of uncertainty and inconsistency in the process. Moreover, the data controllers may choose to suppress factors that may not favour them. This will potentially make DPIA a mere fulfilment of the wishes of the risk assessor if they are given unfettered freedom to develop the rules. The question then is, would such a subjective method realise the goals of the GDPR?[510] This question is pertinent given that under Article 36 (2), the supervisory authorities shall consider whether the 'controller has insufficiently identified or

based Approach' (n 13) 5, 8.

[510] Bieker et al. believe that a standard DPIA procedure is necessary in the GDPR era to ensure effective implementation of the legislation, noting that such will help DPAs to find weaknesses and legal infringements as well as allow the emergence of best practices that will benefit data controllers. Bieker et al., 'A process for data protection impact assessment' (n 495) 36.

mitigated the risk' when consulted, as well as the 'the intentional or negligent character of the infringement' when imposing administrative fines under Article 83 (2)(b). Therefore, an open approach, as suggested, may not be in the best interest of the data controllers because it has a higher tendency of leading to substandard performance.

The third scenario, which contemplates a rigid risk assessment method, is also not supportable. There is a need for the data controllers to bring their system expertise when assessing risk, such as in risk identification and when developing mitigation strategies. Any approach that limits this freedom is likely to affect the quality of the risk assessment and may fail to take advantage of the contextual knowledge of the data controller. Therefore, the second option appears most viable, as it will be possible to adopt a hybrid model, combining both subjective and objective approaches when concretising how a risk assessment should be made. The important thing here is that it is done systematically, which is the focus of this study.

Several other works favouring this second pathway have been published since the adoption of the GDPR, where authors evaluate DPIA requirements under Article 35 of the GDPR.[511] A few of these works have indeed developed a precise method for completing a DPIA, particularly the risk assessment phase. For example, Bieker et al., whose work is technically and legally oriented, proposes a DPIA process consisting of three broad stages: the preparation, evaluation, and report and safeguard stages. They define four criteria for evaluating whether a high risk is likely to occur and also identify six protection goals: transparency, confidentiality, integrity, unlinkability, availability and intervenability.[512] Kloza et al. recently attempted to develop a methodology for operationalising a DPIA in line with the

[511] See Raphaël Gellert, 'Understanding the notion of risk in the General Data Protection Regulation' (2018) 34 (2) Computer Law & Security Review 279; Katerina Demetzou, 'GDPR and the Concept of Risk: The Role of Risk, the Scope of Risk and the Technology Involved' in Eleni Kosta et al (Eds) *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data (*Privacy and Identity 2018. IFIP Advances in Information and Communication Technology, vol 547, Springer); Claudia Quelle, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach' (2018) 9 European Journal of Risk Regulation 9).

[512] Bieker et al., 'A Process for Data Protection Impact Assessment' (n 495).

GDPR after conducting a comparative analysis of impact assessment approaches in multiple areas and identifying general best practices.[513] However, these academic efforts at explaining DPIA and what it entails to complete its risk assessment phase have not yielded the desired results in our view. The quest to understand the phenomenon of impact assessment and the right strategy for implementing it still remains. For example, Phase II of Kloza et al.'s model—titled 'Risk Assessment'—does not elaborate on what it means to implement Article 35 (7)(c), even though their work recognises that appraisal of impact typically 'consists of—at least—a detailed identification, analysis and evaluation of impacts'.

On the other hand, despite the debate whether risk assessment should be standardised or not, supervisory authorities have weighed in by developing several guidelines to assist data controllers in conducting a PIA or DPIA, although their approaches have been divergent. As already mentioned, during the DPD era, three DPAs—the UK's ICO, the French CNIL and the Spanish AEPD—published PIA guidance documents. The adoption of the GDPR has seen updates of these documents. New ones have also emerged, such as the conference of the German data protection authorities' (DSK) short paper on DPIA according to Article 35,[514] the guidelines from the defunct WP29,[515] and the others listed in Table 2 in Section 4.3.2. Before going into details about these guidelines, the following section shall consider developments around automating the impact assessment process as this has an implication on whether risk assessment should be standardised or not.

4.2.2 Automation of the Impact Assessment Process

Another exciting development in the area of DPIA is the automation of impact assessment tools. Traditionally, PIAs are completed manually, where the risk assessor undertakes some manual analysis and calculations using a word processor like MS Word and Excel to write the PIA report. In this context, most risk

[513] See Kloza et al, 'Towards a Method for Data Protection Impact Assessment' (n 399); Kloza et al, 'Data Protection Impact Assessment in the European Union' (n 70).

[514] DSK, 'Kurzpapier Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO' (17 December 2018) <https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf> accessed 12 December 2019; see also DSK, 'Kurzpapier Nr. 18' (n 79).

[515] WP29, 'Guidelines on DPIA' (n 56).

management processes, such as communication between the stakeholders participating in the PIA, occur through meetings and e-mail exchanges. In recent times, however, several software tools have been developed that aim at automating such processes.[516] These tools have emerged in both commercial and open-source models, with regular updates, as their uses mature. An excellent example of a free and open-source PIA software is the CNIL PIA software tool (a supporting tool of the CNIL's PIA methodology) with features for creating PIA templates and allowing users' customisation to suit their purpose.[517] The tool has been updated regularly, and the current version (at the time of writing) is version 2.2 (January 2020), with 18 language translations. According to the CNIL record, this tool was downloaded over 130,000 times within the first year of its release and had received two awards in 2018.[518]

Automating the PIA process has several advantages. First, it is notable that automation presupposes a level of standardisation of the process. In cases where carrying out a PIA is recurring, automation can make it easy for performing this process—this is indeed the intention of the GDPR, as it is envisaged that DPIA shall be a recurrent and ongoing process. It can also assist in improving 'both the efficiency and quality of the process because activities are performed with precision and consistency.'[519] This level of systematisation is what is lacking in manual methods. Time and money could also be saved in the whole process.

---

[516] See: Ave point <https://www.avepoint.com/privacy-impact-assessment/>; CNIL PIA software <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment>; One Trust <https://www.onetrust.com/products/assessment-automation/>; Nymity ExpertPIA <https://www.nymity.com/solutions/expertpia/>; Granite <https://granitegrc.com/granite-privacy-impact-assessment/>; The CNRFID-CSL Privacy impact Assessment software <http://rfid-pia-en16571.eu/why-use-the-software/how-it-works/>; Privaon Privacy Impact Assessment Tool <https://privaon.com/services/privacy-impact-assessment-tool/> access 29 November 2019.

[517] CNIL, 'The PIA Software 2.0 Available and Growth of the PIA Ecosystem' (06 December 2018) <https://www.cnil.fr/en/pia-software-20-available-and-growth-pia-ecosystem>; CNIL, 'The Open Source PIA Software Helps to Carry Out Data Protection Impact Assessment' (25 June 2019) <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment> accessed 14 December 2019.

[518] Ibid.

[519] Pavon, 'PIA Privacy Impact Assessment' (*Pavon,* Whitepaper 15.4.16) <http://privaon.com/wp-content/uploads/2014/10/What-is-a-Privacy-Impact-Assessment-PIA.pdf> accessed 14 December

Nevertheless, it must be noted that there is no agreed standard for DPIA automation tools and these tools are at different maturity levels[520] (see Annex 3 for a non-exhaustive list of PIA/DPIA automation tools). The CNIL PIA software is a portable and web version generation tool that uses questionnaires and pre-defined fields to elicit information for generating the PIA report; however, it does not include the preliminary assessment phase envisaged under Article 35. An examination of the tool shows that it is highly dependent on human input, which means that the output's quality is subject primarily to the correctness and details provided by the user. Given this gap, Zibuschka has proposed a 'next-generation' tool that could directly integrate with the target system, thereby enabling automatic data and metadata capture.[521] While this has a potential for reducing human error, in general, the decision-making process based on algorithms usually contain an element of 'black box'—a system or component for which we can observe inputs going in and outputs coming out, but we cannot follow the internal mapping of the inputs to the outputs.[522] Suppose such next-generation tools could request data from the system and perform the assessment automatically, using models like the threat models seen in the information security industry. In that case, there is a clear need to understand the algorithm behind the model, given the issues with algorithm bias.[523]

Although the CNIL PIA software tool is customisable and follows definite steps as designed by the developers, it is notable that specific processes required by the GDPR, such as consultation with stakeholders (e.g., data subjects, DPO), cannot

---

2019.

[520] See Jan Zibuschka, 'Analysis of Automatio Potentials in Privacy Impact Assessment Processess' in Sokratis Katsikas et al. (eds) *Computer Security*. CyberICPS 2019, SECPRE 2019, SPOSE 2019, ADIoT 2019 (Lecture Notes in Computer Science, vol 11980. Springer 2019) 280-286.

[521] Ibid.

[522] See Dallas Card, 'The "Black box" Metaphor in Machine Learning' (*Towards Data Science,* 5 July 2017) <https://towardsdatascience.com/the-black-box-metaphor-in-machine-learning-4e57a3a1d2b0> accessed 26 December 2019.

[523] See Nicol Turner Lee, Paul Resnick and Genie Barton, 'Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms' (Brookings, 22 May 2019) <https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/> access 12 December 2019.

be automated because such process requires actual interaction with humans. While the CNIL tool has a column that provides for a summarised outcome of these consultations, Zibuschka's comment that certain aspects such as the evaluation of risk or the proportionality of processing 'can hardly be performed in an unsupervised fashion' is also on point regarding the limitation of automation of DPIA.[524] Indeed, automation may achieve the systematisation of the DPIA processes; it does not solve the problem identified in this study. Furthermore, issues such as transparency in the underlying architecture and parameters for risk assessment by the system are yet to be adequately addressed since the software developers determine these aspects to a large extent. The situation may even worsen if the data controller cannot review or adjust the parameter set by the software developers for analysing and evaluating risk. For example, suppose the data controller is unable to add or remove some indicators or categories of data fields. In that case, this may affect the holistic nature of the process because the contextual nature of a DPIA may be sacrificed for automation.

However, given the benefits of applying automation, in general, there is a potential that as these software tools mature and improve in the future, more explanations and theoretical knowledge behind the system will emerge. Moreover, the impact of producing a quick PIA report using these tools can attract more users in the future and expand the market for such tools. However, until this vision is achieved, such tools should be used with caution and allow human intervention where necessary. Furthermore, outputs produced from them should be reviewed with the utmost care.

4.3 Comparing DPIA Guidelines by EU DPAs

Globally, several guidance documents to assist data controllers and processors in conducting PIA or DPIA have accompanied various privacy/data protection laws. However, only a few studies have compared these frameworks, one of which was commissioned by the UK's ICO in 2007. This study compared existing frameworks of PIA from Canada, the USA, Australia, New Zealand, and Hong Kong to learn

[524] Zibuschka, 'Analysis of Automation Potential' (n 520) 284.

lessons and develop the UK PIA framework.[525] The study's outcome was reflected in the first UK PIA handbook. Similarly, in 2011, the PIAF project (funded by the EU) compared the PIA framework in the countries mentioned above (but now including the UK and Ireland) using four elements: existing framework analysis, legal basis, shortcomings and efficacy, and best elements.[526] The project aimed at identifying features that may be used effectively to construct a model framework for the EU and concluded, among other things, that a PIA was more than a compliance check with existing legislation or privacy principles.[527]

Concerning the quality of PIA guidance documents, Clarke had looked at documents across several jurisdictions, using ten elements he termed the 'best practical criteria':

1. Status of the Guidance Document
2. Discoverability of the Guidance Document
3. Applicability of the Guidance Document
4. Responsibility for the PIA
5. Timing of the PIA
6. Scope of the PIA
7. Stakeholder Engagement
8. Orientation
9. The PIA Process
10. The Role of the Oversight Agency.[528]

He found that the quality of these documents fell into three categories: those with inadequate quality, those with moderate quality and finally, those with high quality. It is equally notable that various articles individually looked at PIA frameworks from several jurisdictions in the PIA book edited by Wright and De Hert.[529]

---

[525] Linden Consulting Inc. (n 34).

[526] PIAF Deliverable D1 (n 34).

[527] Ibid, 189.

[528] Clarke (n 34)113-116. The countries compare here are the USA, Canada, Australia, New Zealand, Hong Kong and the UK.

[529] Wright, *Privacy Impact Assessment* (n 34).

However, none of these works presents the desired criteria for this study to compare the current guidelines issued by the supervisory authorities since 2016 following the adoption of the GDPR. For example, while Clarke's criteria were designed to evaluate guidance documents based on different legal and normative instruments, the present study focuses on a single legal instrument, the GDPR. As such, most of the criteria suggested by Clarke, such as the criteria on responsibility for the PIA, the timing of the PIA, scope sof the PIA, stakeholder engagement, among others, are redundant because the GDPR has already taken care of them on a European level.

4.3.1 Guidelines During the Era of DPD

During the era of the DPD, as already noted, only a few guidelines were published by DPAs in the EU, and relatively little research had compared these documents.[530] Methodological differences in the strategy adopted by these DPAs is a noticeable feature of these guidelines.[531] For example, the ICO PIA Code of Practice had a six-step process; the French methodology consisted of a 4-step process, while the Spanish guide contained an 8-step process. Similarly, while the French CNIL modelled its methodology for PIA based on the EBIOS[532] (the risk management method published by the French National Cybersecurity Agency—Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)), the UK and Spanish guides, while containing elements of risk management, did not take such an approach. These latter documents instead advised the data controllers to choose any methodology they deemed fit. The UK Code of Practice, for example, stated:

[530] See Eva Schlehahn, Thomas Marquenie and Els Kindt, 'Data Protection Impact Assessments (DPIAs) in the Law Enforcement Sector According to Directive (EU) 2016/680 – A Comparative Analysis of Methodologies' (*VALCRI* White Paper WP-2017-12) <http://valcri.org/our-content/uploads/2018/06/VALCRI-DPIA-Guidelines-Methodological-Comparison.pdf> accessed 14 December 2019.

[531] It is also notable that different methodologies have been adopted in the guidelines from the authorities. For example, the CNIL adopts the EBIOS methods; the Spanish AGDP relies on ISO 31000 processes (the DSK short paper on risk also calibrates risk assessment into the three processes of ISO31000), the WP29 guidelines do not have any methodology, except transposing the provision of Article 35(7) into what it terms 'criteria for an acceptable DPIA'.

[532] EBIOS – Expression des Besoins et Identification des Objectifs de Sécurité (Expression of Needs and Identification of Security Objectives, <http://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/> accessed 23 January 2019.

> Organisations may have their own [way] of categorising or measuring risk. It may be beneficial to assess the risk in terms of likelihood and severity. Organisations may also use their own numerical scales to record risk. This can be of some assistance but organisations should guard against overly focusing on scores or using a system inflexibly, in all scenarios.[533]

The UK's approach, in general, was criticised by Oetzel and Spiekermann as 'methodologically not suited to be a process reference model', pointing out also that the lack of description of input-output factors in the handbook, the generic nature of the process steps, and the lack of conceptual tools supporting the UK PIA risk assessment weakened the UK's framework.[534] Furthermore, despite consulting the code and handbook, such omissions meant that risk assessors were uninformed about what to do and when.

By contrast, the French CNIL PIA guidelines contained a more objective risk assessment approach. They were made up of three documents, namely the PIA Methodology (how to carry out a PIA),[535] the PIA Tools (templates and knowledge bases),[536] and the Measures for the Privacy Risk Treatment Good Practice.[537] Significant features of the French model include four privacy risk components and a formula for estimating the severity and likelihood of risk.[538] The privacy principles and data subjects' rights were also used to determine 'legal controls' to comply with the law. In general, the CNIL methodology was more mature than the other two. However, it relied on a limited risk assessment scenario and lacked

[533] ICO, 'Conducting Privacy Impact Assessment Code of Practice' (Version 1.0, 2014) 26. It is notable that a set of questions that are intended to help organisations decide whether a PIA is necessary for their operations as well as a PIA template that serves as an example of how to record the PIA processes and results were included in the UK document.

[534] Oetzel 'A Systematic Methodology for Privacy Impact Assessments' (n 33) .

[535] CNIL, PIA Methodology (published first in 2012, revised in 2015) (n 270).

[536] CNIL, PIA Tools (templates and knowledge bases), June 2015.

[537] CNIL, PIA Measures for the Privacy Risk Treatment Good Practice, June 2015.

[538] The components are: (A) Risk sources (B) Personal data supporting assets (C) Personal data (D) Potential impact, which is used to estimate the risk level. The risk level is estimated by the severity of C and D and the likelihood of A and B. For example, determining the severity depends on a concrete factor: the prejudicial effect of the potential impact, while the parameters for determining the likelihood are the level of vulnerabilities of the supporting assets facing threats and the level of capabilities of the risk sources to exploit them.

comprehensive criteria for risk assessment, especially when weighed against all possible scenarios of assessing data processing risks.

The three guidelines discussed above predate the GDPR, and as such, fall short of addressing all the components of the Regulation for impact assessment, such as the preliminary assessment, necessity and proportionality assessment, among others. Therefore, as the next section examines, it is not surprising that they have been updated, and other supervisory authorities have issued other new guidelines.

4.3.2 Guidelines During the current GDPR Era

The guidelines that were published during the DPD era were inadequate to cater for the requirements of the GDPR. This led to supervisory authorities issuing new ones, although with different approaches. For example, some authorities integrated their guidance on DPIA into their general explanation of the GDPR provisions. This is in the form of either as a short section on 'how to conduct DPIA' as seen in the Luxemburg CNPD[539] and the Norwegian Datatilsynet[540] websites, or as an elaborate part, as in the case of the UK ICO, which also serves as a revision of the old PIA guidance documents.[541] Others published separate DPIA guidelines such as the French CNIL, and the Spanish AEDP, among other authorities. Equally important here is that the WP29 and the EDPS have issued guidance documents on carrying out a DPIA. The EDPS's document discusses an equivalent provision for DPIA under the Regulation (EU) 2018/1725 on data protection by EU institutions. Table 2 below shows the guidelines from the 28 EU Member States (the UK inclusive at this point) supervisory authorities as far as the literature search could reveal, as well as those from the WP29 and EDPS. This

[539] CNPD, 'Guide De Préparation Au Nouveau Règlement Général Sur La Protection Des Données' <https://cnpd.public.lu/fr/dossiers-thematiques/Reglement-general-sur-la-protection-des-donnees/responsabilite-accrue-des-responsables-du-traitement/guide-preparation-rgpd.html> accessed 18 March 2019.

[540] Datatilsynet, 'Vurdering av personvernkonsekvenser (DPIA)' <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/?id=10361> accessed 8 December 2019.

[541] ICO, 'Guide to the General Data Protection Regulation - Data Protection Impact Assessment' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/> accessed 18 March 2019.

table does not include the DPIA whitelists and blacklists from each supervisory authority. Nevertheless, it presents a good summary of the current position.

Table 2: Guidance documents from EU authorities

S/N	Supervisory Authorities	Approach to DPIA guidance	Sources
1	Austria	A part of the question and answer page on the SA's website contains an explanation of DPIA.	https://www.dsb.gv.at/fragen-und-antworten#Wann_benoetige_ich_eine_Datenschutz-Folgenabschaetzung_
2	Belgium	There is a published recommendation by the CBPL on DPIA and prior consultation.	https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/aanbeveling_01_2018_0.pdf
3	Bulgarian	No self-developed guidance document identified, the WP29 guidelines on DPIA is published on the SA's website	https://www.cpdp.bg/en/index.php?p=rubric&aid=4
4	Croatia	A brief mention of DPIA is seen on the SA's website while explaining the GDPR's obligations, and the WP29 guidelines on DPIA are published on the website as well.	https://azop.hr/info-servis/detaljnije/vodic-kroz-opcu-uredbu-o-zastiti-podataka https://azop.hr/info-servis/detaljnije/smjernice
5	Cyprus	There is an explanation of DPIA to data controllers on its website, mainly reflecting the WP29 guidelines	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page2c_en/page2c_en?opendocument
6	Czech Republic	A published general impact assessment methodology is open for public consultation as at October 2019. This document will update the initial document explaining how to carry out a DPIA (published in 2018)	https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=37330; https://www.uoou.cz/k-nbsp-povinnosti-provadet-posouzeni-vlivu-na-ochranu-osobnich-udaju-dpia/d-28385
7	Denmark	There is a published guidance document on impact analysis.	https://www.datatilsynet.dk/media/6563/konsekvensanalyse.pdf
8	Estonia	An explanation of DPIA is published on the SA's website. There is also another PDF document on the subject matter.	https://www.aki.ee/et/isikuandmete-tootleja-uldjuhendi-veebitekst#peat%C3%BCkk5.5; https://www.aki.ee/sites/default/files/inspektsioon/naidis/andmekaitsealane_mojuhinnang_naidis_1.pdf
9	Finland	The SA's website contains an explanation of risk assessment for organisations processing personal data, which include a section on how to carry out an impact assessment.	https://tietosuoja.fi/en/risk-assessment-and-data-protection-planning; https://tietosuoja.fi/en/impact-assessments; https://tietosuoja.fi/en/carrying-out-an-impact-assessment

10	France	Developed own PIA methodology with other supporting documents such a knowledge-base and template	https://www.cnil.fr/en/cnil-publishes-update-its-pia-guides
11	Germany	The DSK has published two short papers (Kr 18 - on risk to rights and freedom) and (Kr 5 – on DPIA). Note however that DPA's of the länder have their instructions on the subject matter	https://www.datenschutzkonferenz-online.de/kurzpapiere.html
12	Greece	There is a short explanation of DPIA (Art.35) on the SA's website	https://www.dpa.gr/portal/page?_pageid=33,239286&_dad=portal&_schema=PORTAL
13	Hungary	A link to the CNIL PIA software is published on the SA's website	https://www.naih.hu/adatvedelmi-hatasvizsgalati-szoftver.html
14	Ireland	There are published guidelines on DPIA in addition to the explanation on the SA's website	https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Guide%20to%20Data%20Protection%20Impact%20Assessments%20%28DPIAs%29_Oct19_0.pdf; https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments
15	Italy	The SA has a tutorial on impact assessment, identification and risk management, in addition to an explanation of DPIA that reflect the WP29 guidelines on DPIA on its website.	https://www.garanteprivacy.it/regolamentoue/DPIA/gestione-del-rischio; https://www.garanteprivacy.it/web/guest/regolamentoue/dpia
16	Latvia	There is a downloadable document that explains the DPIA sample on the SA's website.	https://www.dvi.gov.lv/lv/datu-aizsardziba/organizacijam/ieteikumi/
17	Lithuania	There are guidelines for public consultation on personal data security measures and risk assessment on public consultation till 1 October 2019. At the time of this publication (December 2019), there is no news about this document	https://vdai.lrv.lt/lt/naujienos/valstybine-duomenu-apsaugos-inspekcija-viesosioms-konsultacijoms-pateike-asmens-duomenu-saugumo-priemoniu-ir-rizikos-vertinimo-gaires
18	Luxemburg	There is a guide on GDPR that contains a portion on identifying and managing risk on the SA's website.	https://cnpd.public.lu/fr/dossiers-thematiques/Reglement-general-sur-la-protection-des-donnees/responsabilite-accrue-des-responsables-du-traitement/guide-preparation-rgpd.html
19	Malta	There is a short explanation of DPIA on the SA's website (which refers to the WP29 guidelines as well). Also, there are 'guidelines' (in the form of a template) developed by the SA outlining the minimum requirements upon which data controllers may develop their own DPIA template.	https://idpc.org.mt/en/Pages/dpia.aspx; https://idpc.org.mt/en/Documents/Guidelines%20on%20DPIA%20template.pdf

20	Netherlands	There is a page indicating the views of the SA on DPIA. There is also a link to both the English and official Dutch translation of the WP29 guidelines on DPIA.	https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#wat-zijn-de-criteria-van-de-ap-voor-een-verplichte-dpia-6667
21	Norway	The SA explains DPIA as part of the duties of data controllers on its website	https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/?id=10361
22	Poland	There are guidelines on the risk-based approach that deals with DPIA	https://uodo.gov.pl/data/filemanager_pl/706.pdf; https://www.uodo.gov.pl/data/filemanager_pl/707.pdf
23	Portugal	Comments relating to DPIA are seen on the FAQ page of the SA's website.	https://www.cnpd.pt/bin/faqs/faqs.htm
24	Romania	Explains DPIA as part of the FAQ on the SA's website that also contains a link to the WP29 guidelines on DPIA.	https://www.dataprotection.ro/?page=IntrebariFrecvente1
25	Slovakia	The SA has published a procedural methodology of DPIA	https://dataprotection.gov.sk/uoou/sites/default/files/zz_2018_158_20180615.pdf
26	Slovenia	The SA has given some opinions relating to DPIA on its website; however, no guidelines could be identified.	https://www.ip-rs.si/vop/
27	Spain	There are practical guides on DPIA as well as on risk analysis published by the SA	https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf; https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf
28	Sweden	As part of the explanation of the provisions of the GDPR, there is an explanation of how to carry out a DPIA. A link to the WP29 guidelines on DPIA is also published on the SA's website	https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/konsekvensbedomningar-och-forhandssamrad/sa-har-gor-man-en-konsekvensbedomning/; https://www.datainspektionen.se/other-lang/in-english/the-general-data-protection-regulation-gdpr/impact-assessments-and-prior-consultation/
29	United Kingdom	The ICO's website contains a section on DPIA as part of its GDPR guidance. The page is also downloadable as a PDF document.	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/
30	WP29 (now EDPB)	The WP29 published Guidelines on DPIA, which the EDPB adopted.	http://ec.europa.eu/newsroom/document.cfm?doc_id=47711
31	European Data Protection Supervisor	The EDPS published a guidance document on how to carry out a DPIA as part of the	https://edps.europa.eu/sites/edp/files/publication/18-02-06_accountability_on_the_ground_part_1_en.pdf

		'accountability on ground' toolkit	

Given that the criteria in the literature that earlier compared PIAs do not fit into the focus of this study, alternative criteria shall be used for comparing these current guidelines to suit the focus and scope of this study. These criteria are:

1. The terminology used in these guidelines;
2. Steps for carrying out a DPIA; and
3. Factors relevant to completing the risk assessment process.

4.3.2.1 The Terminology used in the Guidelines

The Oxford Lerner's Dictionary defines terminology as 'the set of technical words or expressions used in a particular subject'.[542] Over time, specific terminology around risk management has assumed some conventional meaning among stakeholders, of which several glossaries exist today.[543] However, there is no such agreed glossary in data protection risk management, a point already identified as one issue to be tackled for the successful implementation of DPIA across the board. Evidence from various publications on privacy and data protection risk management, including the guidelines by various EU supervisory authorities, show such discrepancies in the vocabulary used to represent risk and associated terms, at least when compared with the conventional understanding of these terms in the risk management lexicon. The instances looked at below buttress this point.[544]

Starting with the definition of the core term DPIA, there is no uniformity in how the authorities have defined this term (see also Section 1.2.2.1). A few examples shall be highlighted to show this. In the Irish and the UK guidelines, for example, a

[542] Oxford Learner's Dictionaries, 'Terminology' <https://www.oxfordlearnersdictionaries.com/definition/english/terminology?q=terminology> accessed 25 December 2019

[543] See ISO/Guide 73:2009(en) Risk management — Vocabulary; Riskope, 'Glossary of Risk-related Technical Terms' <https://www.riskope.com/wp-content/uploads/2017/08/Glossary-of-risk-related-technical-terms.pdf> accessed 25 December 2019.

[544] However, it is essential to note that the comparison here has a limitation to the extent that some of the publications on DPIA from these supervisory authorities are not written in English. They had to be translated, and as such, there is a possibility that some meanings may be lost in translation. Care has, however, been taken to first focus on the publications that are in English, and where translated texts are considered, this fact is noted in the footnote.

DPIA is defined similarly as 'a way for you to systematically and comprehensively analyse the personal data processing you engage in or plan to engage in and help you identify and minimise data protection risks.'[545] The Cypriot supervisory authority defines a DPIA as 'a process that helps organisations to identify and minimise risks resulting from the processing operations.'[546] In the WP29 guidelines, a DPIA is seen as 'a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them'.[547] Most other supervisory authorities seem to have adopted the WP29 definition. Although these definitions present a DPIA as a risk management tool, there are differences in their focal points. While the Irish/UK definition highlights the analysis, identification and mitigation aspects of the risk, the WP29 definition goes further to incorporate other features of Article 35, such as the necessity and proportionality assessment, also highlighting that the focus of risk assessment is strictly on the rights and freedoms of the data subjects as opposed to those risks facing the data controller's business per se. In Chapter One above, the definition of a DPIA was discussed, and a granular approach was suggested so as not to confuse the provision of Article 35 with a proper definition of the term DPIA. It seems that the authorities have not devoted much attention to harmonising their definitions to reflect the core meaning of this tool but have instead focused on the provision of the law that demands it, as seen in the WP29 approach.

Apart from discrepancies in the definition of DPIA, there is also inconsistency in using the term 'risk' and its associated terms, such as 'harm' and 'threat'. The EDPS

[545] This is culled from the Irish DPC, 'Guidance Note: Guide to Data Protection Impact Assessments (DPIAs) (October 2019) 2. The ICO defines is as 'A DPIA is a way for you to systematically and comprehensively analyse your processing and help you identify and minimise data protection risks.' ICO, 'Data Protection Impact Assessment' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/> accessed 13 December 2019.

[546] Office of the Commissioner for Data Protection Cyprus, 'Data Protection Impact Assessment' <http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page2c_en/page2c_en?opendocument#> accessed 13 December 2019.

[547] WP29 'Guidelines on DPIA' (n 56) 4.

guidance document, which does not explicitly define a DPIA, defines 'risk' as 'a possible event that could cause harm or loss or affect the ability to achieve objectives.'[548] It goes on to say that '[r]isks have an impact – "how bad would this be?" and a likelihood – "how likely is this to happen?"'[549] However, the rest of the document tends to use the conventional vocabularies indiscriminately, sometimes interchanging the term risk to mean threat or harm as seen in the following statement: '[s]ome possible data protection risks are unauthorised disclosures of personal data or inaccurate data leading to unjustified decisions about individuals'.[550] Even though the term 'risk' is used in this statement, 'threat' is what it conveys in the risk management lexicon: an event or thing that can harm the asset (see discussion on these terms in Chapters One and Three). A similar indiscriminate use of vocabulary is also seen in the Irish DPC's statement as follows: '[t]he types of risk range from the risk of causing distress, upset or inconvenience to risks of financial loss or physical harm'.[551] Again, despite using the term risk in that statement, 'harm' is simply expressed, which is the injury or damage to the asset due to the manifestation of the threats.[552]

Other supervisory authorities also tend towards indiscriminate use of risk vocabularies.[553] Mixing up these terms may indicate a lack of proper understanding of the concept of risk in the data protection environment. Furthermore, this may affect effective communication among stakeholders, as technicians, for example, may understand what is conveyed differently. Therefore, it is crucial that the data protection community engage in research involving multidisciplinary experts and stakeholders to iron out the terminology used around data protection risk

[548] EDPS, 'Accountability on the Ground Part II' (n 26) 8.

[549] Ibid.

[550] Ibid.

[551] Irish DPC, 'Guidance Note: Guide to Data Protection Impact Assessments (DPIAs)' (n 545) 16.

[552] Similarly, the 'non-exhaustive list of the types of risks to the rights and freedoms of the data subject' largely comprise of threats in the convention language of risk management. Ibid, 18.

[553] See the Finnish document on carrying out an impact assessment, Office of the Data Protection Ombudsman, 'Carrying out an Impact Assessment' <https://tietosuoja.fi/en/carrying-out-an-impact-assessment>; See also other documents listed in Table 2.

management. Risk assessors and supervisory authorities will be on the same page when discussing issues around DPIA when such harmonised glossary is formed.

4.3.2.2 Steps for carrying out a DPIA

The current guidelines have also varied in their steps or process models for completing a DPIA. A comparison of some of these steps indicates the following:

I. the ICO DPIA guidelines contain a nine-step process diagram[554] (however, a seven-step process is seen in the DPIA template).[555]
II. the Irish and the EDPS guidance documents contain a six-step process;[556]
III. the Spanish DPIA guide contains three broad phases with a core 6-step process (however, other essential processes such as consultation with the data protection officer, review for changes in the treatment, the preliminary assessment and consultation with the supervisory authority, are visible in the framework diagram);[557]
IV. the WP 29 suggests a seven-step generic DPIA process;[558]
V. the French CNIL's PIA methodology, as well as the DSK's, contain four broad steps (with further sub-steps in each category);[559]
VI. the Finnish guidance has a five-step process.[560]

The figure below shows pictorial representations of the respective guidelines.

[554] ICO, 'Data Protection Impact Assessments' (n 547).

[555] ICO, 'Sample DPIA Template' <https://ico.org.uk/media/2553993/dpia-template.docx> accessed 23 March 2019.

[556] Irish DPC (n 545) 14; EDPS (n 26) 6.

[557] AEPD (n 395).

[558] WP29 (n 56) 16.

[559] CNIL, 'Privacy Impact Assessment (PIA) Methodology' (n 76); DSK 'Kurzpapier Nr. 5' (n 514).

[560] Office of the Data Protection Ombudsman, 'Carrying out an Impact Assessment' (n 553).

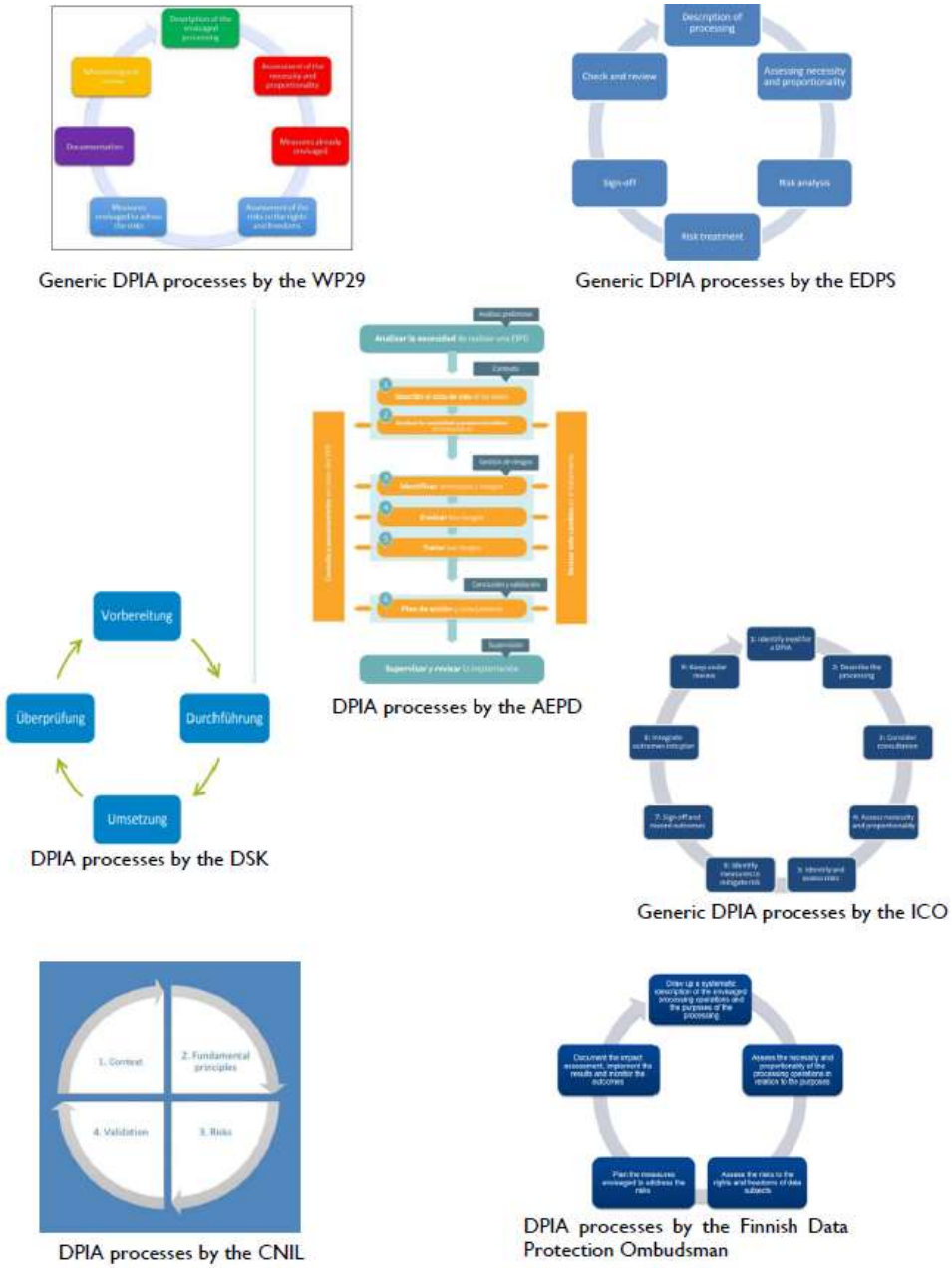


Figure 9: Diagram showing DPIA processes as suggested by some supervisory authorities

As is apparent from the above, there is no consensus on the steps to completing a DPIA. This divergence may be rationalised by the general way that the DPIA obligation is couched, as explained by the Irish DPC:

> The GDPR presents a broad, generic framework for designing and carrying out a DPIA. This allows for scalability, so even the smallest Data Controllers can design and implement a DPIA; as well as for flexibility, so

> the Data Controller can determine the precise structure and form of the DPIA, allowing it to fit with existing working practices.[561]

This flexibility, however, does not mean that consistency should be sacrificed. On the contrary, the GDPR equally promotes consistency and requires the supervisory authorities to adopt a consistency mechanism where data processing has a cross-border effect. Undoubtedly in many instances, a DPIA will have such an effect, and as such, one would expect that there should be a form of uniformity in the process requirements of DPIA. However, this seems not to be the case regarding the methodology for conducting a DPIA, in general, and risk assessment, in particular. These guidelines adopt different approaches and always allow the data controllers to decide what methodology to use in completing the DPIA.

One common aspect, though, in these guidance documents is that they all contain a risk assessment step (reflecting Article 35 (7)(c)). Here again, it seems that the 'flexible interpretation' has resulted in two broad approaches: goals-based and rule-based approaches.[562] The goal-based approach is demonstrated where the supervisory authority does not elaborate on the rules or method of completing the risk assessment process, but advises the data controllers to choose any method they deem appropriate. However, the authority may suggest some framework in an open-ended manner. A majority of the guidelines follow this path, including the UK ICO, the Irish DPA, the WP 29 and the EDPS's guidelines. The Irish DPC, for example, writes:

> Your organisation can choose the risk management approach that best suits your existing project management process. The same tools you use for identifying other regulatory or commercial risks as part of your project management process can be used to assess the data protection risks involved in a project. The key point is to ensure that a methodological approach to identifying risks is adopted, and that records are kept of this process, and of all the risks identified.[563]

---

[561] Irish DPC (n 545).

[562] For a fuller discussion on these approaches see Christopher Decker, 'Goals-Based and Rules-Based Approaches to Regulation' (2018) BEIS Research Paper Number 8.

[563] Irish DPC (n 545). See also Office of the Commissioner for Personal Data Protection, 'Data Protection Impact Assessment' <http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page2c_en/page2c_en?open

This approach has its merit and demerits: while it allows the data controller the opportunity to shop for the methodology that suits it, it could also lead to uncertainty and diminished value (or a race to the bottom) if any method could be used. There could also be a lack of objectivity in the whole exercise, as the data controller could be guided entirely by instincts. Furthermore, the nature of data protection threats and harm may not always fit into other risk assessment tools in practice; they may require expertise to transpose their components and processes into the EU data protection framework domain. Many data controllers may not possess the skill to do this.

On the other side, some supervisory authorities such as the DSK, Bavaria DPA, CNIL and the Spanish AEPD have approached the issue differently by calibrating risk assessment into sub-processes, and including a more detailed prescription of how to complete the processes (a more rule-based approach).[564] The Bavaria DPA, for example, suggests that risk assessment could be calibrated into sub-processes such as risk identification, risk analysis and risk evaluation.[565] The CNIL, on its part, has drawn on the EBIO method[566] to design its PIA methodology, although the part relating to risk assessment appears limited to the 'risks related to the security of data'.[567]

document> accessed 25 December 2019.

[564] It has to be noted that despite having a strong and specific risk management outlook, the Spanish AEPD's guide on DPIA equally states that it is not intended to be the only way a DPIA can be implemented. Organizations that have already implemented risk analysis processes and tools can use them to assess privacy and data protection as long as they cover the essential aspects that any DPIA must have, in compliance with the requirements of the GDPR. (p.2). The same could be said of the others as there is nothing indicating that they are mandatory.

[565] See, Bayerisches Landesamt für Datenschutzaufsicht, 'Musterbeispiel „Insight AG – Kfz-Telematik-Versicherungstarif" Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO in Anlehnung an die ISO/IEC 29134' (DSFA-Bericht zum Fallbeispiel des Workshops 19.07.2017) 17 <https://www.lda.bayern.de/media/03_dsfa_fallbeispiel_baylda_iso29134.pdf>; The AEPD guide also adopts a similar framework, except that it combines risk treatment as part of risk assessment, while merging risk analysis and evaluation.

[566] EBIOS (n 532).

[567] CNIL (n 76) 6-7.

Regrettably, as earlier noted, the WP29 guidelines on DPIA do not concretise how Article 35 (7)(c) risk assessment process should be carried out despite recognising the essence of this process (see the statement in this footnote).[568] As if this silence is not unfortunate enough, the criteria added in Annex 2 of its guidelines for acceptable DPIA relating to Article 35(7)(c) have created even more confusion. The criteria neither address how established risk management tools can be adapted to fulfil this task nor provide specific and unambiguous directives on identifying, analysing, and evaluating risk. Such omissions cannot be covered by merely saying that 'whatever its form, a DPIA must be a genuine assessment of risk'[569] because even when the intention is genuine, without proper methodology, an assessment will only be as good as the metrics employed.[570]

To buttress the point relating to the incompleteness of the instructions in the WP29 guidance, let us show a part of the WP29 Guidelines Annex 2—the criteria for an acceptable DPIA. A part tagged 'risks to the rights and freedoms of data subjects', which reflects Article 35(7)(c), contains the following layers:

> ☐ risks to the rights and freedoms of data subjects are managed (Article 35(7)(c)):
>
> > ☐ origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
> >
> > > ☐ risks sources are taken into account (recital 90);
> >
> > ☐ potential impacts to the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification and disappearance of data;
> >
> > ☐ threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;

[568] The WP29 recognises the essence of risk assessment as seen in the following statement: 'It has to be stressed that in order to manage the risks to the rights and freedoms of natural persons, the risks have to be identified, analysed, estimated, evaluated, treated (e.g. mitigated...), and reviewed regularly.' WP29, 'Guidelines on DPIA' (n 56) footnote 10 on page 6.

[569] Ibid, 17.

[570] Bräutigam (n 31) 269.

- ☐ likelihood and severity are estimated (recital 90);

- ☐ measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90).[571]

These bullet points are intended for the data controller's consideration during the risk assessment phase; however, the question comes around again: how should the likelihood and severity be estimated? What factors should be considered in assessing this likelihood and severity? Are illegitimate access, undesired modification and disappearance of data the only impact that could result from data protection violation? How should the measures of treating the risk be determined? What other threats should be considered apart from illegitimate access, undesired modification and disappearance of data? There could be many other questions. Despite criticising the initial drafts of the RFID and the Smart Meter DPIA templates for lacking a transparent methodology for risk assessment, the WP29 also fails to devote adequate time in explaining how this should be done in its guidelines.[572]

It is not clear why the WP29 kept this aspect vague. This gap has allowed various interpretations of what it means to complete Article 35 (7)(c) in the course of a DPIA. As already noted, the CNIL regards it as an assessment of the data security of the proposed processing. In the DPIA template by the Maltese IDPC, there are separate columns for 'data subject rights' and 'risk assessment (minimum requirements)'.[573] The guidance from the Finnish supervisory authority seems to suggest that this process involve identifying the risks associated with the processing; analysing each risk separately; evaluating the measures needed to

[571] A portion of Annex 2 of the WP29 Guidelines reflecting Article 35 (7)(c). WP29 (n 56) 22.

[572] It is noteworthy that the WP29 had earlier lamented the lack of clear methodology on the subject matter in two of its opinions. See, Article 29 Working Party, 'Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force' (2013) 00678/13/EN WP205; 'Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications' (2010) 00066/10/EN WP 175.

[573] IDPC, 'DPIA Template', 3 <https://idpc.org.mt/en/Documents/Guidelines%20on%20DPIA%20template.pdf> accessed 25 December 2019.

reduce the risks and their likelihood.[574] Further, the portion of the ICO's template for identifying and assessing risk suggests that this process is carried out by describing the 'source of risk and nature of potential impact on individuals', with other columns indicating the likelihood of harm, the severity of harm and the overall risk.[575] The AEPD considers the risk assessment phase as comprising: risk identification, risk evaluation and risk treatment (which appears to lump Article 35 (7)(c) and 35 (7)(d) together under the risk assessment phase).[576] The examples above, at least, indicate a need for a precise approach for completing a risk assessment procedure during a DPIA.

The WP29 opting to give examples of existing PIA frameworks and criteria for an acceptable DPIA rather than develop an authoritative framework for conducting risk assessment does not seem to have solved the problem. Such an approach is inadequate, which neither addressed the discrepancies in these examples nor how data controllers should synchronise them given their divergence in scope, steps, methodology, and vocabulary. For example, while the German Standard Data Protection Model (SDM) (one of the examples EU generic frameworks by the WP29) focuses more on operationalising the privacy by design principle, the other examples (CNIL PIA methodology, ICO PIA code of practice and AEPD PIA guide) are purely on impact assessment (although with significant differences).[577] Similarly, the ISO/IEC 29134:2017 is a generic tool that needs to be tailored to the GDPR, as it was not the normative framework used to design the standard. [578]

4.3.2.3 Factors relevant for completing the risk assessment process

One other remarkable feature in these guidance documents concerns the risk assessment content with respect to the parameters for consideration during this exercise. Not all of the guidelines suggest the factors or parameters necessary for

[574] Office of the Data Protection Ombudsman, 'Carrying out an Impact Assessment' (n 553).

[575] ICO, 'Sample DIA Template' (n 555).

[576] Note that the ISO 31000 also distinguishes risk assessment from risk treatment.

[577] See Annex 1 of the WP29 Guidelines on DPIA (n 56).

[578] For example, the ISO/IEC 29134:2017 used vocabulary such as personally identifying information (PII) instead of personal data as used in the GDPR.

completing the risk assessment process, for example, weighing the likelihood that a particular threat or harm may materialise or its severity. Where such criteria are reflected, they lack uniformity among the authorities. For example, in the CNIL document, only five factors could be identified for completing the data security risk assessment. Here, the determination of the impact on the data subject (based on the estimation of the **severity** of risk) depends on two parameters: 'the prejudicial nature of the potential impacts [on the personal data] and, where applicable, controls likely to modify them'; while the factors for estimating the **likelihood** are three: 'the level of vulnerabilities of personal data supporting assets, the level of capabilities of the risk sources to exploit them and the controls likely to modify them'.[579] The overall summation of the severity and likelihood factors yields the risk level.

For its part, the Irish DPC guidance contains only the factors relevant for measuring the severity of the identified risks: '[i]n assessing the **severity** of the risk, it is important to bear in mind *the sensitivity of the personal data to be processed as part of the project, the number of people likely to be affected by any of the risks identified, and how they might be affected*'.[580] It is not clear why the Irish authority only focused on the severity of the risk and ignored the likelihood part. The UK's ICO approach is even vaguer, consisting of a series of generic statements, such as '[t]o assess whether the risk is a high risk, you need to consider both the likelihood and severity of the possible harm,' which fail to concretise the parameters for this assessment.[581] In addition, although the ICO provides a risk matrix to structure this likelihood and severity of the risk, details of how to use this matrix are lacking.[582]

[579] CNIL, 'PIA Methodology, February 2018' (n 37) 7.

[580] Italics are for emphasis. It is not clear why the DPC did not also provide similar factors for the likelihood aspect. See Irish DPC (n 545) 16.

[581] ICO, 'How do we do a DPIA? <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/> accessed 6 December 2019.

[582] Ibid.

By contrast, the Spanish practical guide for risk analysis and the guide for DPIA contain several factors applicable to each phase of the DPIA. For example, when discussing how to conduct the preliminary assessment to determine whether a DPIA is required, the AEPD suggests a two-stage methodology where the controller would first analyse the list of processing operation including the blacklist and whitelist under Article 35(3), 35(4), and 35(5), and then, secondly, analyse the nature, scope, context and purpose of the data processing under Article 35(1).[583] This second phase is done using specific parameters in the form of questions to determine whether the processing will pose a high risk:

Nature of processing:
a. Are special categories of data processed?
b. Is data processed on a large scale?
c. Are people closely monitored?
d. Are different datasets combined? (different sources of information)
e. Does the data refer to vulnerable people?

Scope of processing:
a. Is there a decision-making process with legal effects?
b. Is a credit risk assessment performed?
c. Is the exclusion of social or tax benefits valued?

Context of processing:
a. Is new technology used? Are they especially invasive for privacy?
b. Are there several controllers?
c. Are there complex chains of processors?
d. Do international transfers occur?
e. Are there data transfers?

Purposes of processing:
Does the processing involve:
a. Decision-making?
b. Profiling?
c. Predictive analysis?
d. Providing health-related services?
e. Monitoring, monitoring and observation of people (monitoring)?.[584]

Although this characterisation is related to the preliminary risk assessment, it also appears relevant during the core DPIA phase. Unfortunately, the AEPD did not further emphasise this in the DPIA guidelines. The AEPD guidelines equally contain parameters for measuring the scales for the likelihood and impact of risk (a scale of 1-4 ranging as follows: 1 – Negligible Likelihood/Impact; 2 – Limited

[583] AEPD, 'Practical guide on risk analysis' (n 75) 12.

[584] Ibid, 12ff. Translation by the author.

Likelihood/Impact; 3 – Significant Likelihood/Impact; 4 – Maximum Likelihood/Impact). The parameter for each scale is described, and a matrix is included to show the interaction of likelihood and impact in determining the risk level.[585]

In a similar vein, the German DSK paper also adopts a more systematic approach, dividing risk assessment into three phases: risk identification, estimation of the probability of occurrence and severity of possible damage, and risk grading.[586] A series of questions could be answered to complete each phase; for example, to identify risk, the following questions are asked:

> a. What damage can be caused to the natural based on the data to be processed?
> b. What, i.e. by which events can this damage come?
> c. By what actions and circumstances can these events occur? [587]

Apart from explaining each question to assist the risk assessor, the DSK's short paper further identifies the nature of threat events and harms that could result from a data protection breach. For estimating the likelihood and severity of the risk, the paper sets out some assessment parameters, leading to the grading of the risk level as 'low risk', 'risk', and 'high risk'. A risk matrix is also suggested in the paper.

The Finnish guidance document does not have a straightforward procedure for risk assessment. However, it writes that the 'assessment must take into account the nature, scope, context and purposes of the processing of personal data'. It goes further to suggest elements for these factors, as shown in the diagram below.

[585] AEPD, 'Guide on DPIA' (n 395) 21– 27.

[586] DSK Short Paper No. 18, 2. However, in the DSK short paper on DPIA according to Art. 35 of the GDPR, the risk assessment procedure is not elaborated except acknowledging that risk is assessed based on the nature, scope, context and purpose of data processing. See DSK Short Paper No 5.

[587] Ibid. This is a translation from the German text.

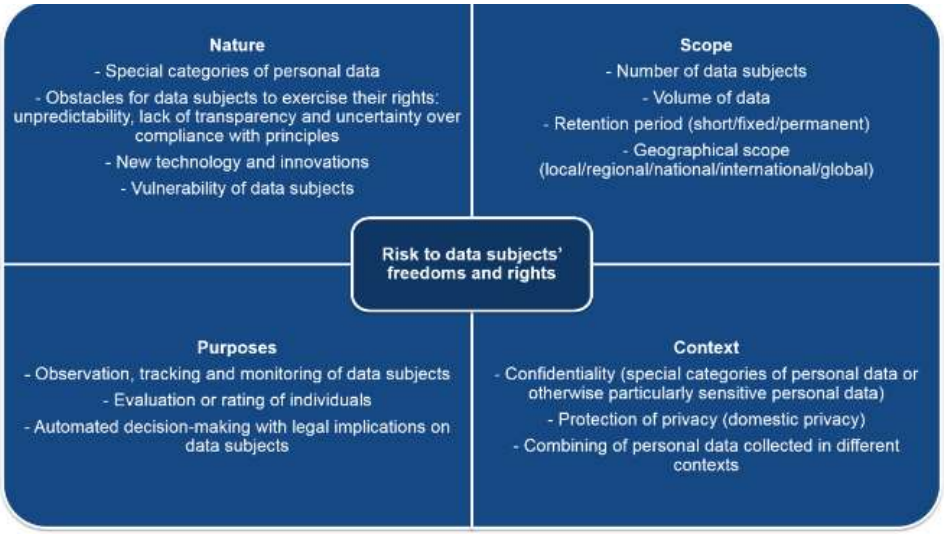


Figure 10: Diagram from the Finnish guidelines on DPIA showing elements of Nature, scope context and purpose of risk assessment

While the diagram contains examples of elements to look out for when considering these factors, they do not explain how they should be applied, for example, in determining the risk level of the identified risks.

In summary, some guidelines do not have a precise calibration of the risk assessment process, and it is difficult to rely on these to assess risk systematically. In addition, granularity is lacking in their instructions, making it difficult to identify relevant factors for risk identification, analysis, and evaluation. The guidelines that provide parameters are not uniform, as the discussion above shows: some rely on questions, while others have explicit parameters. In the next section, a suggestion will be made on how the supervisory authorities could approach their future guidelines to harmonise and clearly instruct the risk assessor performing a DPIA.

4.3.3 A Proposal for Approaching Future DPIA Guidelines regarding Risk Assessment

The above review has shown uncertainty in several areas, from terminology to steps for completing a DPIA. Research has so far been general and sparse, reflecting an imperfect understanding by the privacy community of how conventional risk management tools should be transposed in the data protection arena. Nevertheless, this study has defined the problem and shall later proceed to offer some solutions. As pointed out by the Spanish supervisory authority:

> The search for objectivity is a fundamental principle in a DPIA. It is essential to have a systematic process through a standardised working methodology

> or procedure that allows establishing common criteria to ensure homogeneity, repetitiveness and comparability in the execution of a DPIA.[588]

Given the divergences exhibited in the guidelines discussed above, it seems that the authorities have not heeded this call. This state of affairs is arguably not sustainable in the GDPR era, where consistency and objective assessment of risk are emphasised, which calls for a systematic approach. Above all, conducting an *ex-ante* risk assessment will continue to be an important accountability measure. Therefore, there is a need to get it right. Although some of the research highlighted in this study has been ongoing and some institutions such as the d.p.i.a.law, CIPL, have dedicated resources to solving the issues of DPIA, much work still needs to be done. This gap has encouraged this study to explore how the authorities should approach future guidelines.

There is no doubt that publishing guidelines on how legal rules ought to be applied is one tool for clarity and contributes to the implementation of legislative rules because high-level legal instruments, in this case, the GDPR, are not always prescriptive on the steps towards their implementation. Often, these instruments permit responsible agencies to issue soft law or directives on the application, an approach that could be explained by the principles of inner morality of law—clarity and consistency—that Fuller contemplated.[589] In contemporary legal scholarship, administrative guidelines ties with these Fuller's principles. The GDPR envisages that supervisory authorities shall issue guidelines—manuals that explain how processes are to be carried out to enhance the consistent application of the GDPR rules. Kloza et al. have suggested the need for such guidelines for DPIA, recommending that EDPB is best positioned to issue and update EU-wide guidelines. At the same time, the national supervisory authorities could adjust such guidelines for local circumstances while respecting the consistency goal of the GDPR.[590] They further recommend that the methods developed in these guidelines be adaptive, receptive, and define the conditions for oversight. These

[588] AEPD, 'Guide on DPIA' (n 395) 10. Translation to English done by the author.

[589] Lon Fuller. *The Morality of Law* (Yale University Press 1964).

[590] Kloza et al, (n 70) 4.

recommendations are plausible, as they will serve a practical purpose to the data controllers and processors and bring about certainty in the whole process of DPIA.

There is a strong case for developing harmonised guidelines in the context of DPIA. First, such will assist the authorities in weighing the reasoning and justification behind a risk assessor's analyses and evaluations, for example, to know whether the risks have been sufficiently identified. This could be gleaned from the so-called criteria for acceptable DPIA in Annex II of the WP29 guidelines. Although lacking the desired granularity, it pokes what the authorities are looking out for in a DPIA. Second, it will provide a ground for justifying the supervisory authorities' conclusions during a review of a DPIA. This has a transparency effect because the rules have been exposed beforehand. Furthermore, systematic and harmonised guidance would address other issues, such as those related to terminology.

In this respect, the general principles identified by the European Food Safety Authority (EFSA) Scientific Committee in its guidance document on the procedural aspect of transparency offer an excellent template for designing future guidelines in the area of DPIA.[591] With an emphasis on risk assessment, future guidelines by the EDPB should include, among other aspects:

1. A clear definition of what risk assessment means in the context of *ex-ante* DPIA, as well as harmonise the assessment terminology;
2. Structured steps or processes for risk assessment as envisaged in Article 35 (7)(c) of the GDPR;
3. Metrics (factors and parameters) relevant to completing each of the steps of this risk assessment;
4. Criteria for inclusion or elimination of these factors, as well as criteria for measuring the risk level; and
5. How to treat the elements of uncertainty in the whole exercise.[592]

There is a high potential that the output of a DPIA guided through these elements will be more transparent in describing the underlying assumptions and reason behind the assessment results. It will also be consistent and repeatable. Such an approach is also crucial because risk assessment is often clouded with incomplete

[591] EFSA 'Transparency in risk assessment carried out by EFSA: Guidance Document on procedural aspects' (2006) 353 *The EFSA Journal*, 1, 3. (See further discussion on this in Chapter Five).

[592] Inspiration in drawing these factors came from the Guidance Document on procedural aspects by the EFSA. Ibid.

information and subjective elements. Therefore, having a defined directive on how to complete such an assessment will introduce elements of objectivity. Moreover, as the assessment discussed here referred to a future breach, there is uncertainty as to whether it will even happen at all, how it may happen, and what the real impact may be. It is then imperative that a systematic approach is adopted to enhance transparency.

Furthermore, future guidelines from the EDPB should include good examples, sources, questions, templates, etc., in explaining what the risk assessor should do in completing each risk assessment task. Such guidelines should describe the principles by which risk assessments are to be performed, such as the foreseeability principle in terms of scoping and predicting the threats, harms and other elements during risk identification. As far as possible, these guidelines should help risk assessors interpret and reach a decision on the risk posed by their data processing operation based on objective criteria that are clear and measurable where necessary. Some components in the existing guidelines could be harnessed and further developed for each risk assessment process. The EDPB should ensure through its guidelines that, where a data controller has to consider data processing across the Member States, no national scheme should complicate this process by introducing conflicting approaches. This way, the single market would be enhanced. Therefore, further efforts are needed to harmonise these guidelines to facilitate their application in cross border settings, as well as to make it easy for domain-specific applications.

It is essential to note the potential role of the consistency mechanism of the GDPR in the area of DPIA's risk assessment. Applying such a mechanism here will make it more precise for data controllers who operate across the EU Members States to apply the same rules and know what is required of them when conducting DPIA. The EDPB's approach in reconciling the list of data processing activities requiring, or not requiring, a DPIA as envisaged under Article 35(4) and (5) of the GDPR (the blacklist and the whitelist) is an excellent example of how this mechanism could be extended to the risk assessment methodology and process.[593] With such

[593] See the EDPB Opinions <https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en> accesses 12 February 2019. See also EDPB, 'Press release: Third Plenary

a mechanism, it will be easier for the EDPB to develop EU-wide guidance around the risk assessment process while leaving room for national authorities to adapt it to specific national circumstances where necessary, as well as sector-specific applications where required.

For practical purposes, the envisaged guidelines should be designed with a hybrid approach where both objective (such as defined steps, criteria, etc.) and subjective elements are interoperable. Thus, for example, a data controller who seeks to identify the risk posed by a proposed data processing system could brainstorm to do so because he or she knows the system; however, this thought process could be defined within the compass of some objective indicators such as the nature, scope, context and purpose of data processing.

Another important reason why it is desirable to encourage procedural transparency through some systematic guidance is that whether a risk assessment has been properly carried out or not should be answered normatively (by reference to what the rule objectively requires, independent of individual opinions). As Patterson writes:

> When we set out to follow a rule, we never believe that whether we have complied with the rule is a matter of opinion. We may believe that we have complied with the dictates of a rule, but that belief cannot be grounds for our claim that we have in fact complied. This shows that rules exhibit what we might term "epistemic primacy." By this, I mean that the broad application of rules "seems to imply a standard of correctness that is independent of applications." To explain this phenomenon, the objectivist asserts the existence of a standard independent of the rule which enables rule application in a variety of contexts. [594]

Implicit in this statement is that where criteria for evaluation of the implementation of a legal rule are known beforehand, it enhances legal certainty in applying the law. When this is translated in the context of *ex-ante* risk assessment, this approach will potentially forestall assessor inconsistency—a situation where the process and outcome do not match and are difficult to repeat and predict even when similar

session: EU-Japan draft adequacy decision, DPIA lists, territorial scope and e-evidence' 26 September 2019 <https://edpb.europa.eu/news/news/2018/press-release-third-plenary-session-eu-japan-draft-adequacy-decision-dpia-lists_en> accessed 6 March 2019.

[594] Dennis Patterson, 'Normativity and Objectivity in Law' (2001) 43 Wm. & Mary L. Rev. 325, 331.

circumstances exist. Suppose risk assessors are systematically guided through the risk assessment processes by defined criteria. In that case, the outcome is more likely to be consistent and would undoubtedly differ from where the whole process is performed intuitively.

4.4 CONCLUSION

The literature review and comparison of the guidelines in this chapter have shown the fragmentation in the approaches adopted by both authors and the authorities towards impact/risk assessment. Undoubtedly, a systematic and harmonised framework is not only necessary for effective implementation of this obligation, but also for consistency and certainty of the procedure. Given that an incorrect DPIA exposes data controllers to operational risk, it is desirable that the EDPB step in at the EU level and design guidelines that fill the identified gaps from this study.

Notably, Article 35 (7) of the GDPR provides the minimum content of a DPIA. Still, the individual steps and parameters for completing each portion of this minimum content; mainly, the risk assessment step, are still imprecise. Although different factors such as the origin, nature, context, and purpose of processing, are relevant during a DPIA, how these factors operate in identifying, analysing and evaluating risk still need to be clarified and concretised. A structured and granular approach to developing these relevant factors and the criteria for weighing them during the risk assessment phase still lacks in most guidelines. In the next chapter, an attempt shall be made to map DPIA requirements with the framework of ISO 31000:2018 and operationalise the risk assessment process using a systematic methodology developed in this study. A use case shall be used to illustrate it.

CHAPTER FIVE

5. TOWARDS A SYSTEMATIC METHODOLOGY FOR DATA PROTECTION RISK ASSESSMENT

5.1 INTRODUCTION

The previous chapter reviewed relevant literature relating to the approaches and EU-based guidelines that clarify carrying out an impact assessment under the EU data protection law. Unfortunately, these documents have not resulted in a consensus or harmonised framework concerning a core aspect of DPIA—the risk assessment process. This chapter, therefore, introduces a systematic approach to risk assessment, suggesting how procedural transparency can be achieved during an *ex-ante* DPIA. In addition, this chapter includes a method of operationalising risk assessment as envisaged by Article 35 (7)(c).

5.2 THE LESSONS FROM THE SYSTEMATISATION OF RISK ASSESSMENT IN OTHER AREAS

Several fields of human endeavour adopt a systematic approach to problem-solving. In engineering design, for example, a systematic approach is adopted to reach the desired solution to a problem in the sequence of an idea, concept, planning, design, development, and launch.[595] In the construction industry, Godfrey has proposed a systematic approach as a way of managing risk: that is, making 'risks explicit, formally describing them and making them easy to manage'.[596] He further identifies several benefits of a systematic approach in such context—it helps to identify, assess and rank risks; it assists in making an informed decision; it helps to

[595] Ron Lasser, 'Engineering Method' <https://sites.tufts.edu/eeseniordesignhandbook/2013/engineering-method/> accessed 30 October 2019.

[596] See Patrick Godfrey, 'Control of Risk. A Guide to the Systematic Management of Risk from Construction' (Construction Industry Research and Information Association Special Publication 125, 1996) 9. See also Anthony Mill, 'A systematic Approach to Risk Management for Construction' (2001) 19 (5) Structural Survey 245.

clarify and formalise role, among others.[597] Other examples of sector-specific systematisation of risk assessment have resulted in a more standard methodology in these areas. Information security, and environmental protection and food safety risk assessments present such examples. In the following sections, these areas will be considered in more detail to learn lessons for adaption in data protection.

5.2.1 Information Security Risk Assessment

Information security has evolved over the years from representing a notion of securing the physical location (where the early mainframe computers were kept) to the logical security of data and information systems (hardware, software and network communication).[598] As a result, this field has progressed to the extent of having its own interpretation and vocabulary for risk, as well as several methodologies and frameworks for information security risk management (ISRM) from both national authorities (e.g., the German BSI) and international bodies (e.g., the ISO) and private entities (e.g., the FAIR Institute). Although this has not resulted in a single universally accepted tool for IT security risk management, there is a tacit agreement that the ISRM process should be systematic and clearly defined. Such a systematic approach is necessary, given that IT systems and the data they process are becoming increasingly complex. Moreover, they are facing physical threats and technical vulnerabilities and attacks, against which intuitive and unstructured assessment methods can only help to a limited extent.[599]

Therefore, in a bid to maintain a systemic structure, ISRM tools contain defined processes and steps, factors, and goals to consider during a risk assessment. For example, the ISO 31000 risk management process was adopted to describe how risk identification, analysis, and evaluation could be applied in IT security in ISO 27005:2018.[600] By such compartmentalisation, the 'input' and 'output' data, as well

[597] Godfrey, ibid.

[598] Michael Whiteman and Herbert Mattord, *Principles of Information Security* (5th Edn, Cengage Learning 2012) 3-7.

[599] Milda Macenaite, 'The "Riskification"' (n 23) 518.

[600] ISO/IEC 27005 Information technology – Security Techniques – Information Security Risk Management (3rd edition, 2018) 9-16.

as actions to be performed in each process, could easily be identified and mapped out. It is also important to note that formalised methods for information security risk assessment have a sector-specific approach in some cases. For instance, there is the Payment Card Industry Data Security Standards (PCI DSS) in the financial sector,[601] which is supported by supplementary guidance for conducting a risk assessment under the standard.[602]

In general, information security seems to have crystallised to reflect the protection of three key characteristics of data: confidentiality, integrity and availability (commonly known as CIA triad) and has developed a set of vocabularies for this purpose.[603] These characteristics mean that data must not be disclosed to unauthorised entities; it must be accurate and complete, and it must be accessible when needed by authorised entities.[604] Risk assessment of information systems has coalesced around these protection goals, although recent attempts have been made to expand these characteristics.[605] Notably, the nature and focus of information security risk assessment (on data and infrastructure) allows it to define concrete primary assets, such as data, information, as well as supporting assets (the IT and network systems used to process data).[606] This has also made it possible to narrow down defined threats, attack types, vulnerabilities, controls and impacts to some extent, which could be identified and assessed around specific data and equipment.

[601] PCI Security Standards Council <https://www.pcisecuritystandards.org/> accessed 28 August 2019.

[602] PCI Security Standards Council, Information Supplement. PCI DSS Risk Assessment Guidelines (November 2012) <https://www.pcisecuritystandards.org/documents/PCI_DSS_Risk_Assmt_Guidelines_v1.pdf> accessed 29 August 2019.

[603] Whiteman, *Principles of Information Security* (n 598) 11.

[604] See also Section 3.4.2.

[605] Whiteman, *Principles of Information Security* (n 598) 14-17.

[606] Ibid, 237. Note that the French CNIL adopted the terminology of asset and supporting asset in its PIA methodology.

Information security has a lot in common with data protection: not only is information security an integral principle of data protection law, but *ex-ante* risk assessment has always been conducted to ascertain the security risk of information systems. In recent times, some attempts have been made in the privacy sphere to reduce privacy protections to similar goals, but this has not been followed consistently and universally. For example, the Standard Data Protection Model acknowledged by the German Data Protection Authorities adopts the approach of translating some data protection law requirements into data protection goals.[607] This model expanded the information security goals mentioned earlier to include other goals such as data minimisation, unlinkability, transparency, and intervenability.[608] Although the WP29 referred to this model in its DPIA guidelines, it does not appear to have reached a full adaption in the European data protection sphere, perhaps because of the challenges in implementing such models.

Part of the challenge in strictly translating information security goals into data protection goals is the differences in the focus of risk assessment in the two areas: data protection risk assessment is mainly focused on humans—the data subjects and their fundamental rights, while IT security risks focus primarily on data and equipment (which could be valued in monetary terms). As rightly observed by Macenaite, it is difficult to express some assets such as human life in economic terms;[609] this is unlike equipment that can be valued through a cost-benefit analysis. There are also several other reasons why data protection risk assessment does not correspond with that of information security. These include the differences in the conception of an 'asset' by corporations, data subjects and supervisory authorities; the sources of data protection requirements, nature of measures required for treating data protection risks, etc.[610] Little wonder then why it has

[607] SDM, 'The Standard Data Protection Model. A concept for inspection and consultation on the basis of unified protection goals' (V.1.0 – Trial version November 2016) <https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V1.0.pdf>.

[608] These terms mean the following: Unlinkability: The obligation to process data only for the purpose for which it was collected is. Transparency: The obligation to provide the subjects with the required information. Intervenability: The data subject's rights to intervene about the data processing such as rectification, blocking, erasure and objection. Ibid.

[609] Macenaite (n 23) 520.

[610] Ibid.

not been easy to adopt the 'protection goal' approach in data protection risk assessment. The merit, though, of the SDM model could be seen in the design of an information system where these goals could be engineered into the system's design so that by default, personal data is protected (data protection by design).[611] This seems to be the approach adopted in the NIST privacy engineering model.[612]

However, it is essential to note that there are instances where there is a synergy between ISRM frameworks and the GDPR requirements for risk assessment. Article 32 of the GDPR presents such a case. It focuses on information security and refers to the CIA triad and other attributes. This provision requires the implementation of appropriate technical and organisational measures, including, among others, 'the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services'.[613] Thus, the conventional ISRM frameworks could be synchronised with data protection requirements in appropriate cases since the GDPR does not mandate any risk assessment methodology. As such, several guidelines on ISRM, particularly on the risk assessment aspect, could be exploited for data protection. Examples here include the NIST risk management framework,[614] the Factor Analysis of Information Risk (FAIR) framework,[615] the ISO 27000 family of standards (e.g. ISO 27005), etc. In addition, the European Union Agency for Cybersecurity (ENISA) has also published several guidance documents on information security.[616]

[611] Bieker et al, however, tried to apply the SDM model within a DPIA framework. See Bieker et al, 'A Process for Data Protection Impact Assessment' (n 495) 29-30.

[612] Brooks et al., 'An Introduction to Privacy Engineering and Risk Management in Federal Systems' (n 36).

[613] GDPR, art 32 (1)(b).

[614] NIST, 'Managing Information Security Risk' (NIST Special Publication 800-39, 2011) <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf> accessed 28 June 2019.

[615] Jack Freund and Jack Jones, *Measuring and Managing Information Risk* (Butterworth-Heinemann 2015); Jones, 'An Introduction to Factor Analysis of Information Risk (FAIR)' (n 83).

[616] ENISA, <https://www.enisa.europa.eu/> accessed 28 June 2019.

One lesson to learn from these ISRM frameworks is that it is possible to systematically organise risk assessment, despite how complex it seems in this environment. The NIST Guide for Conducting Risk Assessment, for example, indicate a clear purpose for risk assessments and goes on to develop four steps for completing such assessment.[617] Similarly, ISO 27005, as already noted, contains structured steps for conducting a risk assessment, dividing it into risk identification, analysis and evaluation.[618] Undoubtedly, such a structured approach can increase the 'reproducibility' and 'repeatability' of risk assessments. Again, this is something that the data protection environment could benefit from emulating.

5.2.2 Environmental and Food Safety Risk Assessment

Risk assessment has also been utilised in environmental protection and food safety to evaluate the risk associated with projects affecting the environment and food production. The United Nations Environmental Program (UNEP) notes that environmental assessment involves 'objective evaluation and analysis of information designed to support environmental decision making'.[619] However, there is no universal risk assessment method under the auspices of the UNEP. Instead, countries have devised their national approaches and rules on assessing the impact of a project on the environment. Over the years, various types of environmental assessments have emerged. Environmental Impact Assessment (EIA) is one of them, which functions to 'provide information to minimise, mitigate, or eliminate adverse impacts' arising from environmental-related projects.[620]

The National Research Council (NRC) of the United States has conducted a study of the institutional means for risk assessment to support federal policies relating to some public health-related hazards and identified four major steps in risk

[617] NIST, 'Guide for Conducting Risk Assessments' (NIST Special Publication 800-30 Revision 1, 2012) 23 <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf> accessed 28 June 2019.

[618] ISO 27005:2018, 8-16.

[619] UNEP, 'Guidelines for conducting Integrated Environmental Assessments' (2011) 7 <https://wedocs.unep.org/bitstream/handle/20.500.11822/16775/IEA_Guidelines_Living_Document_v2.pdf?sequence=1&isAllowed=y> accessed 29 June 2019.

[620] Ibid, 12.

assessment—hazard identification, dose-response assessment, exposure assessment, and risk characterisation.[621] These steps appear to have crystallised in the areas of environmental and health protection, though with various minor modifications. For example, the Australian Department of Health guidelines adopts a five-stage process which resembles the above: (1) Issue identification, (2) Hazard identification, (3) Dose-response assessment, (4) Exposure assessment and (5) Risk characterisation.[622] The UK's Department for Environment Food and Rural Affairs (DEFRA) adopts a slightly modified four-stage approach in its environmental risk assessment framework: (1) identifying the hazard(s); (2) assessing the potential consequences; (3) assessing the probability of the consequences; and (4) characterising the risk and uncertainty.[623] What is expected at each stage is explained in the guidelines issued by the DEFRA. For example, in assessing the probability of the consequences of a risk event, the guidelines identify three areas of consideration: the probability of the initiating event occurring; the probability of exposure to the hazard; and the probability of the receptor being affected by the hazard.[624] These three probabilities can be assessed together, or the later steps can be assessed conditional on the outcome of earlier steps. Scenarios could also be created to explore these probabilities according to the guidelines.[625]

Concerning food safety in Europe, EFSA, the body responsible for implementing Regulation (EC) No 178/2002[626] has equally issued guidance on risk assessment.

---

[621] National Research Council, *Risk Assessment in the Federal Government: Managing the Process* (The National Academies Press 1983) 19.

[622] Australian Government Department of Health, *Environmental Health Risk Assessment Guidelines for Assessing Human Health Risks From Environmental Hazards*, (Department of Health, 2012) 7. These processes have gone through series of modification and seems to be coupled into four stages in the 2008 revision. See page figure 2 in page 10 of the Guidelines.

[623] Áine Gormley, Simon Pollard, Sophie Rocks and Edgar Black, *Guidelines for Environmental Risk Assessment and Management Green Leaves III,* (Department for Environment, Food and Rural Affairs, UK, 2011) 22.

[624] Ibid, 27-29.

[625] Ibid.

[626] Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety [2002] OJ L 31/1.

The Regulation defines risk assessment as 'a scientifically based process consisting of four steps: hazard identification, hazard characterisation, exposure assessment and risk characterisation' and requires that risk assessment 'shall be based on the available scientific evidence and undertaken in an independent, objective and transparent manner'. [627] Pursuant to this requirement, the EFSA's Scientific Committee provided a guide on procedural and scientific aspects of risk assessment to improve its transparency.[628] Recognising that risk assessment is often faced with incomplete information and uncertainties, the guidance document advises that risk assessment be carried out systematically to describe and explain all assumptions and uncertainties. Moreover, the Scientific Committee developed 'general principles to be applied in identifying data sources, criteria for inclusion/exclusion of data, confidentiality of data, assumptions and uncertainties,' thereby providing precisely the processes and principles that the risk assessors should observe. [629] Regarding the principles relating to 'the data, methods of analysis and assumptions' that reflect how transparency is measured in risk assessment, the guidelines note:

> • Transparency is needed in all parts of the risk assessment
>
> • To be transparent, a risk assessment should be understandable and reproducible;
>
> • Where possible, harmonised assessment terminology should be used, preferably based on internationally accepted terminology;
>
> • The procedure by which a risk assessment is completed needs to be based on accepted standards of best practice;
>
> • When circumstances require that a scientific assessment is provided within a limited time period (e.g. in a crisis situation), the effect of this on the uncertainty of the response should be explained, and options and timescales for reducing that uncertainty should be described. [630]

[627] Regulation (EC) No 178/2002, Art 6 (2).

[628] Susan Barlow et al. 'Transparency in Risk Assessment – Scientific Aspects Guidance of the Scientific Committee on Transparency in the Scientific Aspects of Risk Assessments carried out by EFSA. Part 2: General Principles' (2009) 1051 The EFSA Journal 1.

[629] Ibid.

[630] Ibid.

The lessons learned from the above examples are many: first, they indicate that risk assessment has acquired a functional separation from the other components of risk management. Moreover, due to the complexity of the subject, relevant regulatory agencies have published guidelines that characterise what is expected of risk assessors during a risk assessment exercise, mainly using a process or step-by-step approach. Such step-by-step guidance is a valuable tool for risk assessors, as it limits the margin to which they could rely on intuition during the exercise. This approach also makes it easy to identify the components to consider or rely upon in completing each step. For example, in the United States NRC's report, twenty-five components were identified for hazard identification and thirteen components in Dose-Response assessment.[631]

Second, each sector tries to harmonise its risk assessment framework to develop precise vocabulary and methods/processes for conducting it. For example, in the environmental and food safety sector in Europe, these processes are hazard identification, hazard characterisation, exposure assessment and risk characterisation. In the information security sector, the risk to the information system has crystallised around three defining characteristics—confidentiality, integrity and availability. This way, it is possible for an independent observer to review whether the correct normative terms, procedures and indicators have been followed.

Third, by providing detailed guidelines on risk assessment, the regulatory authorities have demonstrated to the risk assessors their areas of priority. Such guidance will provide a clear basis for reviews by the authorities, which invariably breeds transparency. On the part of the risk assessor, such guidelines indicate a practical framework to show accountability.

These lessons should be emulated in data protection so that data controllers and processors know the exact steps to follow when assessing risk in the course of a DPIA. As already indicated, this study proposes the framework of the ISO 31000 process that calibrates risk assessment into three elements: risk identification, risk analysis and risk evaluation. This standard could not only form a template for

[631] National Research Council, *Risk Assessment in the Federal Government* (n 621) 33-34.

structuring the entire DPIA framework, but also be used as a systematic approach to implementing Article 35 (7)(c) that is currently missing in the WP29 guidelines (and has led to polarised national frameworks). In addition, the EDPB should emulate the approach of the EFSA's scientific committee in its procedural and scientific guidance for risk assessment to design a harmonised (procedural) guidance for data protection risk assessment. This should include principles for risk assessment, as well as aim at greater precision in terms of the processes, terminology, and factors for consideration during a risk assessment. Such a transplant is vital in the context of a DPIA because it will assist in identifying the problem that risk assessment seeks to solve and then construct the processes and components that will help solve this problem.

In summary, systematising the approach to data protection risk assessment would help to:

I. establish a logical structure for completing the task envisaged under Article 35 (7)(c);
II. identify the factors for consideration when undertaken each of the processes of risk assessment;
III. achieve consistency, transparency, verifiability and repeatability of the process.

In the next section, the framework of the ISO 31000 process shall be described in detail, with a mapping of its processes with the GDPR's requirement relating to DPIA to show how a systematic structure could be built.

5.3 Introducing ISO 31000 as a Tool for Systematising GDPR's DPIA Framework

There are several risk management tools and standards across the globe. The ISO 31000 is one such standard that has attained international popularity in public and private spheres. This popularity may have resulted from its development by the International Organization for Standards (ISO), comprising national standards bodies.[632] Moreover, it presents a generic tool that is adaptable to several specific contexts. Gjerdrum writes that by the end of 2015, fifty-seven national standards

[632] ISO is an independent, non-governmental international organization with a membership of 164 national standards bodies. ISO <https://www.iso.org/about-us.html> accessed 14 July 2019.

organisations had adopted this standard as their national standard for risk management.[633]

The first edition of an ISO standard on the practice of risk management was published in 2009.[634] This document contained the Principles, Framework and Process for risk management. The Principles refer to what items an organisation managing its risk must satisfy to make the risk management effective; the Framework guides the overall structure and operation of risk management across an organisation, while the Process describes the actual method of assessing and treating risk. The process comprises five sub-processes—Communication and consultation; Establishing the context; Risk assessment (involving Risk identification; Risk analysis; Risk evaluation); Risk treatment; and Monitoring and review. As risk management evolves, the standard has been updated by a technical report in 2013—ISO 31004. Recently, the ISO 31000 underwent a full-scale overhaul and review, resulting in a second and current edition of the standard, ISO 31000:2018.[635]

It is important to note that this revised edition is also free of normative references (to any specific legislation or code), allowing it to adapt to many normative environments. It retained the principles, framework and process for risk management seen in the first edition, but contains some significant changes, including a new step in the process (recording and reporting), which increases the steps from five to six, as shown in Figure 11 below.

[633] Dorothy Gjerdrum, 'A Brief History of ISO 31000 – and Why It Matters' (*Risk and Insurance,* February 9, 2016) <http://riskandinsurance.com/a-brief-history-of-iso-31000-and-why-it-matters/> accessed 12 June 2019.

[634] ISO 31000 Risk Management – Principles and Guidelines (First edition 2009).

[635] ISO 31000 Risk Management – Guidelines (Second edition, 2018). This repealed the first edition.

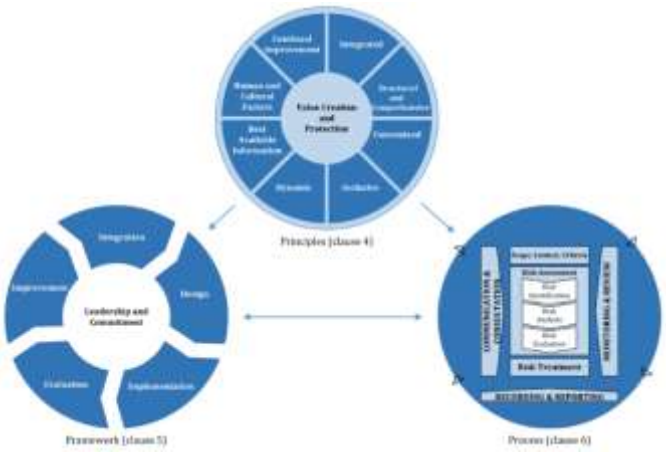


Figure 11: ISO 31000:2018 Risk management principles, framework and process

The current ISO 31000 family of standards relating to risk management include:

- ISO 31000:2018 - Risk Management – Principles and Guidelines
- ISO/IEC 31010:2009 - Risk Management - Risk Assessment Techniques;
- ISO Guide 73:2009 - Risk Management – Vocabulary;
- ISO /TR 31004: 2013 - Technical Report.

There are, however, several other standards related to risk management or that have concretised the ISO 31000 processes in a specific field, such as ISO/IEC 27005:2011 on information security risk management. Equally notable is that the ISO has published some standards on PIA, namely, ISO 22307:2008 Financial Services Privacy Impact Assessment; ISO/IEC 29100:2011 on Privacy Impact Assessment; and ISO/IEC 29134:2017 - Guidelines for Privacy Impact Assessment. The ISO 22307:2008 is a voluntary standard aimed at the financial services industry to help financial institutions identify and mitigate privacy risks to their customers.[636] It contains six common elements of the PIA process, namely, PIA plan; assessment; PIA report; competent expertise; degree of independence and public aspects; and use of proposed financial system (PFS) decision-making. In general, although the standard is meant to address, in large part, the OCED guidelines on the protection of privacy and transborder flows of personal data of 1980, it lacks a concrete explanation of how to apply the process of risk assessment. It instead recommends

[636] See Martin Ferris, 'The ISO PIA Standard for Financial Services' in David Wright and Paul de Hart (eds) Privacy Impact Assessment (Springer 2012) 307-321; Harris Hamidovic, 'An Introduction to the Privacy Impact Assessment Based on ISO 22307' 2010 4 ISACA Journal 1-7.

that 'assessment shall be performed using competent expertise identified in the PIA plan'.[637] This instruction is arguably insufficient and not suitable to be adapted in this present study. However, given the recent changes in data protection as seen in the GDPR, the modernisation of Convention 108 and the revised OCED guidelines from 2013, it is suggested that the ISO revise this standard.

The ISO/IEC 29100:2011, for its part, was developed within the framework of information technology security techniques and describes privacy safeguards in the context of protecting personal identifying information (PII). Therefore, it could be applied by any natural person or organisation that processes PII using IT systems. However, while the standard contains what it terms 'basic elements of privacy framework', it does not follow a systematic structure for risk assessment. The term privacy risk assessment is defined in the 2011 edition as the 'overall process of risk identification, risk analysis and risk evaluation when processing PII'. However, this has been changed in the 2018 Amendment 1: Clarification. Here, the term 'privacy impact assessment' is used; [638] it is unclear why this was done. In any event, the entire standard is less relevant for this study because it fails to elaborate on the process of privacy risk assessment. Interestingly, the 2018 amended version referenced ISO/IEC 29134:2017 as a source for 'privacy risk assessment'.

Finally, the ISO/IEC 29134:2017, developed within the framework of information security, presents guidelines for conducting a PIA in all types and sizes of public and private organisations. Compared to the previous two documents, this standard offers more detailed guidance on how to carry out a PIA, particularly on the process of risk assessment. It adopts the vocabulary of ISO 73 Guide, which also reflects ISO 31000. As such, its privacy risk assessment process is divided into three parts—risk identification, risk analysis and risk evaluation. Although strictly speaking, this standard does not follow the structure of ISO 31000; its content can easily be mapped onto it. Notably, the WP29 referred to this standard in its guidelines on DPIA; however, it is also vital to emphasise that to apply the GDPR

[637] ISO 22307:2008, 6.

[638] ISO 29100:2011/Amd.1:2018, Information technology — Security techniques — Privacy framework AMENDMENT 1: Clarifications (2018) 2.

requirements relating to DPIA through this standard, many adaptations would be required, not only terminologically also structurally. For example, while the GDPR uses 'personal data' to denote a human data subject, ISO 29134 uses 'personally identifying information (PII)'. Further, the GDPR envisages that a separate necessity and proportionality assessment shall be conducted as part of the DPIA, but this element is not seen in the ISO 29134.

Concerning the main subject of this study, it is notable that both ISO 31000 and ISO 29134 divide risk assessment into three sub-processes of risk identification, risk analysis and risk evaluation. However, since the source of this categorisation is the ISO 31000, this study prefers to use it as a normative reference. Moreover, as noted, ISO 31000 has enjoyed significant international recognition and acceptance over the years. Reference will, by contrast, only be made to ISO 29134 when necessary to address any residual points (not already covered). Below, we shall look closely at the individual processes of ISO 31000:2018.

5.3.1 ISO 31000:2018 Risk Management Process

As shown in Figure 11 above, the process of ISO 31000:2018 is made up of: communication and consultation; establishing the scope, context and criteria; risk assessment; risk treatment; monitoring and reviewing; and recording and reporting. These processes are iterative, although they are presented here in sequence.

5.3.1.1 Communication and consultation

Communication and consultation are two closely related activities undertaken in one process, according to the ISO 31000, that aim to promote awareness about risk (communication) and obtain feedback from stakeholders, which assists in understanding and making decisions about risk (consulting).[639] This process facilitates obtaining the relevant information for the risk assessment and takes place within and throughout all the other steps of the risk management process. Internal and external stakeholders are involved in this process where necessary, allowing different views to be considered, especially when identifying and treating

[639] ISO 31000:2018, 9.

risk, as well as when defining the criteria for risk evaluation. This process aims to facilitate informed decision-making, as expertise from various persons is utilised.[640]

The GDPR considers consultations with relevant stakeholders during a DPIA: the data protection officer must be consulted, while the data subjects and even supervisory authorities may be consulted in appropriate cases. These consultations aim to gather relevant information and expertise that would assist the data controller in making an informed decision about the risk posed by the proposed data processing and the potential impact on the data subjects. In addition, where residual risks remain high, the supervisory authority must be consulted under Article 36 of the GDPR before any processing occurs. Apart from the above stakeholders, it is also good practice to consult the relevant staff of the data controller's and/or data processor's organisation and other external experts in appropriate cases to get a clear picture of the operation. We had argued that consulting relevant stakeholders (DPO, data subjects, employees, experts, etc.) has a bearing on the scope of foreseeability in the risk assessment.

5.3.1.2 Scope, context and criteria

Establishing the scope, context and criteria during a risk management exercise is vital to customise the risk assessment to a specific context, including the normative aspect and risk treatment.[641] This process is very relevant to understanding the following: the internal and external setting in which the risk is managed, the resources and tools needed for the risk assessment, the objectives to be achieved, the risk acceptance criteria, the obligations of the organisation, and stakeholders' views, among other things.[642] ISO 31000:2018 recommends that the following factors should be considered when setting risk criteria:

- the nature and type of uncertainties that can affect outcomes and objectives (both tangible and intangible);
- how consequences (both positive and negative) and likelihood will be defined and measured;

[640] Ibid.

[641] Ibid, 10.

[642] Ibid, 10-11

- time-related factors;
- consistency in the use of measurements;
- how the level of risk is to be determined;
- how combinations and sequences of multiple risks will be taken into account;
- the organisation's capacity.[643]

These factors are essential concerning a DPIA, particularly when providing a systematic description of the processing operations. Although the GDPR is the normative reference for the legal environment upon which the assessment is made, other laws may be considered depending on the specific case. For example, a DPIA may involve the e-Privacy Directive[644] if the subject matter is on electronic communications, or the Passenger Name Record Directive[645] if it concerns passenger data. The GDPR also provides that factors such as the nature, scope, context and purposes of the data processing should be considered in DPIA. These factors could be mapped with the relevant processes of ISO 31000, such as risk identification, or when determining the likelihood and severity of a risk.

5.3.1.3 Risk assessment

Risk assessment, as earlier mentioned, refers to a systematic and overall process of risk identification, risk analysis and risk evaluation in the ISO31000. These sub-processes are iterative and require the best information for effective implementation. Below we look at them individually.

5.3.1.3.1 Risk identification

Risk identification 'is the phase where threats, vulnerabilities and the associated risks are identified.'[646] It is meant to capture all relevant threat events that can affect the object of protection (they could also be the risk sources) and record them, irrespective of the fact that some of them may already be known and under

[643] Ibid, 11.

[644] Directive 2002/58/EC (n 3).

[645] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime OJ L 119/132.

[646] ENISA, 'Risk Assessment' <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-process/risk-assessment/risk-assessment> accessed 16 July 2019.

control. This process requires up-to-date information, and ISO 31000:2018 recommends that the following factors should be considered when engaging in the process of risk identification:

- tangible and intangible sources of risk;
- causes and events;
- threats and opportunity;
- vulnerabilities and capabilities;
- changes in the external and internal context;
- indicators of emerging risk;
- the nature and value of assets and resources;
- consequences and their impact on the objective;
- time-related factors;
- biases, assumptions and beliefs of those involved.[647]

Also, historical information about the organisation or similar organisations can be 'useful as they can lead to more accurate predictions about current and evolving issues that have not yet [been] faced by the organisation.'[648] Where an organisation keeps a threat log, it should be consulted during this process.

Several techniques exist for risk identification. For example, ENISA (in the context of information security risk management) suggests the following matters: team-based brainstorming; structured techniques such as flowcharting, system design review, systems analysis, Hazard and Operability studies, and operational modelling; a more general structure such as 'what-if' and scenario analysis depending on the circumstances.[649]

Risk identification is crucial in risk management because it is only when the risks are known or anticipated that mitigation measures can be targeted at them. Of course, it is impossible to identify all risks, but the more identified or anticipated risks, the better for the organisation, as it gives a broader margin for risk treatment.

[647] ISO 31000:2018, 11.

[648] ENISA, 'Risk Assessment' (n 646).

[649] Ibid.

5.3.1.3.2 Risk analysis

Risk analysis aims at comprehending 'the nature of risk and its characteristics, including where appropriate, [finding] the level of risk'. [650] Various factors must be considered when analysing risk, such as 'uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness.'[651] Depending on the purpose, risk analysis should be as detailed and complex as possible if relevant information and resources are available. Various techniques have been used for analysing risk: quantitative, qualitative or a mixture of both when necessary.[652] The ISO 31000:2018 suggests the following factors for consideration during risk analysis:

- the likelihood of events and consequences;
- the nature and magnitude of consequences;
- complexity and connectivity;
- time-related factors and volatility;
- effectiveness of existing controls;
- sensitivity and confidence levels.[653]

This standard further notes that it may be challenging to quantify highly uncertain events. In such cases, a combination of techniques would be valuable for providing insight into the risk. It is essential to point out that risk analysis gives relevant input to risk evaluation and risk treatment.

5.3.1.3.3 Risk evaluation

Risk evaluation aims to support the overall decision about the risk; it involves comparing the risk analysis output with the criteria established at the earlier stage of the process to determine what actions are required to address the risk.[654] Risk evaluation is essential for prioritising risk and may, at times, lead to further analysis of the identified risks or reconsideration of objectives.[655] It is an excellent practice

[650] ISO 31000:2018, 12.

[651] Ibid.

[652] Ibid.

[653] Ibid.

[654] Ibid.

[655] ENISA (n 646).

to make the evaluation outcome available to relevant management authorities for validation and implementation.

It is noteworthy that the GDPR includes risk assessment as part of the minimum content of a DPIA under Article 35 (7)(c), and expects in Recital 76 that '[r]isk should be evaluated on the basis of an objective assessment'. While no specific methodology is prescribed for this objective assessment, there is an implied expectation that a systematic approach should be adopted so that the metrics and criteria for this assessment are evident in the entire exercise. Thus, a risk assessment should be able to identify and evaluate risk and show how the broad metrics suggested in GDPR have been considered in a verifiable manner. In this respect, the ISO 31000 processes of risk assessment appear systematic in fulfilling the requirement of the GDPR, given that the steps are verifiable.

5.3.1.4 Risk treatment

Risk treatment aims 'to select and implement options for addressing the risk.'[656] This process is another critical part of risk management because there are many options available to the risk manager for mitigating the risk, and selecting the best option may not be an easy task. Measures to treat risk include but are not limited to avoiding, optimising, reducing, transferring or retaining risk; removing the risk source; changing the likelihood and consequences.[657] Risk treatment usually involves a balancing of the potential benefit against the cost of treating the risk. It is also notable that risk treatment could introduce new risks; therefore, monitoring the mitigation mechanisms of the residual risks is essential.[658]

The GDPR expects that the 'impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk'.[659] This

[656] ISO 31000:2018, 13.

[657] ENISA, 'Risk Treatment' <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-process/risk-treatment> accessed 16 July 2019; see also ISO 31000:2018, 13.

[658] Ibid.

[659] GRPR, recital 90, art. 35 (7)(d).

makes risk treatment an integral part of a DPIA. The GDPR does not contain an exhaustive list of measures to be implemented in treating risks, but points in the direction that such measures should be appropriate both technically and organisationally, considering state of the art, cost of implementation, nature of the risk, among other factors.[660] Some examples of risk treatment found in the GDPR include pseudonymisation and encryption, regular testing, etc.[661]

5.3.1.5 Monitoring and review

Monitoring and review, as a risk management process, aim to assure and improve the quality and effectiveness of the risk management exercise's design, implementation, and outcome.[662] Due to the iterative nature of the risk management processes, monitoring and review should occur at all stages. The result from this exercise 'should be incorporated throughout the organisation's management, measurement and reporting activities.'[663] Where appropriate, an independent external party could be invited to review the implementation of the risk assessment measures and recommendations.

The monitoring and review process is in line with the GDPR's provision that requires that '[w]here necessary, the controller shall carry out a review to assess if [the] processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.'[664] This provision indicates that a DPIA is not a one-off process; it continues in a loop and requires appropriate updates once there is a change in the system or after some years, depending on the internal and external changes in the environment.

[660] See GDPR, art. 32; see also art. 24.

[661] See GDPR art 32 (1).

[662] ISO 31000:2018, 14.

[663] Ibid.

[664] GDPR, art. 35 (11).

5.3.1.6 Recording and reporting

Documentation is needed to show that a risk management process has been undertaken. Therefore, documentation of all the processes above should be kept and reported through the right channel.[665] While it is relevant to report the outcome of the exercise, attention should be paid to sensitive information, and such could be redacted to the public for security or commercial purposes. By recording the entire exercise, decision-makers, the staff of the organisation, and other stakeholders will be able to read and interpret the report for appropriate action or dialogue.

Finally, the GDPR also requires that a DPIA is documented, as the supervisory authority may request it at any time, particularly when consulting the authorities under Article 36. Although publishing a DPIA is not a mandatory requirement, as noted by the WP29, it is encouraging to publish at least parts of it, such as a summary or the conclusion.[666]

Overall, it is essential to reiterate that although these processes are discussed in this sequence, they are iterative and should be repeated where appropriate. Having shown from the discussion above a connection between the ISO 31000 and the GDPR provisions, the following section shall attempt to map these two sources to see the feasibility of adapting the ISO standard for the systematic application of DPIA processes.

5.3.2 Mapping ISO3100 with GDPR DPIA Provisions

As earlier indicated, there are no normative references in ISO 31000:2018, which allows the use of any legal instrument (e.g., the GDPR) as the applicable legal reference. This feature informs the consideration for the adaptation of the ISO 31000 framework as a systematic basis for applying the requirements of the GDPR during a DPIA, particularly the risk assessment process. Given that the ISO 31000 could be extrapolated to design a systematic DPIA process, several provisions in the GDPR have been considered to see the feasibility of mapping these two

[665] ISO 31000:2018, 14-15.

[666] WP29, 'Guidelines on DPIA' (n 56) 18.

frameworks. A tabulation of these relevant provisions has been made in Table 3 below to show the connection between the GDPR and ISO 31000:2018.

Table 3: A Mapping of the GDPR's DPIA requirements with the ISO 31000:2018 process

S/N	ISO 31000:2018 Process	GDPR's DPIA Requirements
1.	Communication and consultation	**Consultation:** In appropriate cases, consultation should be made with the data protection officer; data subjects or their representatives; supervisory authorities (Recital 94, Articles 35 (2), 35 (9) and 36).
2.	Scope, context and criteria	**Establishing the scope and context:** *'Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons […]'* (Article 35 (1)).
3.	Risk assessment (made up of risk identification, risk analysis and risk evaluation)	**Risk assessment:** […] '*Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk*' (Recital 76) *'[…] controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk.*' (Recital 84) '[…] *a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk'* (Recital 90); *The assessment shall contain at least: […] an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1* (Article 35 (7) (c)).
4.	Risk treatment	**Treating the risks:** '*That impact assessment should include, in particular, […] the measures, safeguards and mechanisms envisaged for mitigating that risk',*

		ensuring the protection of personal data […]' (Article 35 (7), see also Recital 90).
5.	Monitoring and review	**Review:** '*Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.'* (Article 35 (11)).
6	Recording and reporting	**Record and evidence of DPIA:** The GDPR requires that the controller maintains a record of processing activities, including, where possible, a general description of the technical and organisational security measures (Article 30). A DPIA is a document that reflects this and may be required by the supervisory authority, including when consulting under Article 36. As such, it is natural that a DPIA is recorded as evidence that it has been carried out.[667]

The table above is intended to show how some relevant provisions of the GDPR could be interpreted and plugged into the framework of the ISO 31000. This mapping is not intended to be exhaustive; it only presents an avenue to check the feasibility of systematically structuring a DPIA under Article 35 of the GDPR using the ISO 31000 risk management process. This way, each of the requirements of a DPIA could be isolated and given adequate attention during execution. Moreover, the flexible nature of the ISO 31000 allows further integration of requirements from other relevant normative sources. This point is vital in order to capture and plug in all the other DPIA requirements, such as the necessity and proportionality assessment. Figure 12 below shows how such adaptation could be designed (in a workflow) to include these missing processes from the ISO 31000 original diagram.

[667] The WP29 notes that 'a DPIA is a process for building and demonstrating compliance.' Ibid, 4. See also Korff, 'The DPO Handbook' (n 41) 201.

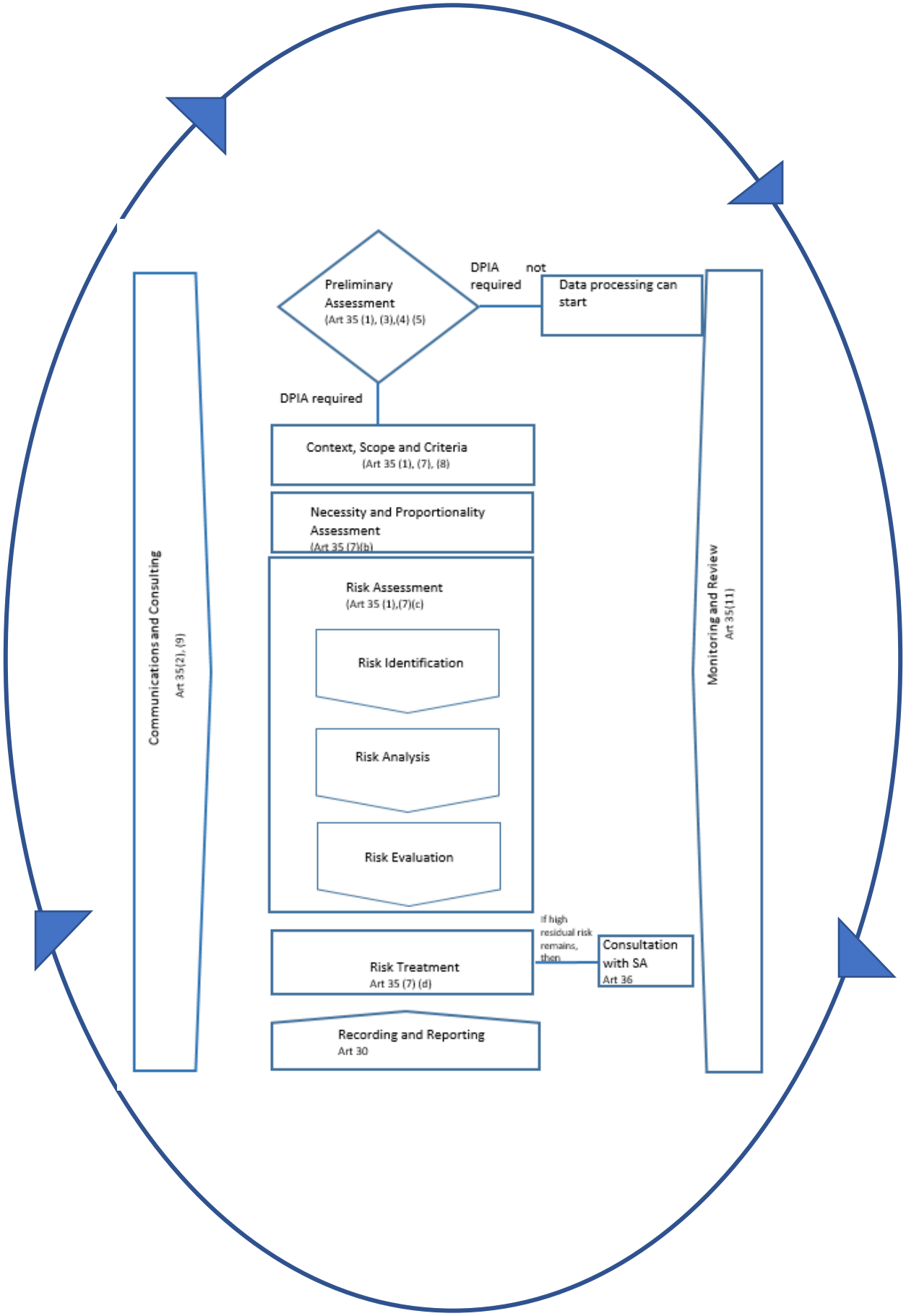


Figure 12: A systematic DPIA framework adapted from ISO 31000:2018

The diagram above illustrates the iterative processes of a DPIA plotted on the ISO 31000 framework. In addition to the initial processes in the ISO 31000:2018 discussed in the section above, the adapted figure includes other core processes to capture the complete requirements of the GDPR, namely: the preliminary assessment, necessity and proportionality assessment, as well as consultation with the supervisory authority when necessary. The preliminary assessment is required to determine whether a data processing operation requires a mandatory DPIA, while the necessity and proportionality assessment is an integral part of the minimum content of a DPIA required under Article 35 (7)(b). Consultation with the supervisory authority is only triggered when the residual risk remains high after applying risk treatment measures (Article 36).

This mapping aids the following sections to isolate the risk assessment process, which is the focus of this study, in order to operationalise it using a practical and step-by-step methodology.

5.4 An Approach to Operationalising Risk Assessment Process During a DPIA

This section shall operationalise the above-mapped framework and shall begin by reiterating and clarifying some points. First, let us address what is meant by the provision of Article 35 (7)(c), being the portion of the DPIA's minimum content that particularises risk assessment. Recall that as already argued in Chapter Three, the operative focus of this article is on the assessment of risk. The primary factors for evaluation are the rights and freedoms of the data subjects. Understood this way, it means that systematic risk identification, analysis and evaluation are *sine qua non* to undertake during the risk assessment phase. This is a logical way of uncovering what could impact the rights and freedoms of the subjects. During a risk evaluation exercise, for example, the enablement and non-violation of the rights and freedoms of the data subjects (not only the rights contained in the GDPR, but other relevant fundamental rights) shall form part of the evaluation criteria. However, to do this properly, all the relevant threats, vulnerabilities and potential harms must first be identified and analysed (in the context of their likelihood and severity of occurring). This is what a formal risk assessment purports to do. Therefore, it would be incorrect to assume that Article 35 (7)(c)

limits the risk assessment to data security risks, or as some templates imply, presupposes a regurgitation of the rights and freedoms of the data subject.[668]

Second, it is also necessary to reflect further on applying the foreseeability principle in scoping a risk assessment framework. As argued in Chapter Two, the doctrine of foreseeability could apply to *ex-ante* data protection risk assessment by analogy. The roles assigned to foreseeability in that discussion is meant to assist in scoping risk assessment in terms of how risk ought to be identified, analysed and mitigated with the appropriate knowledge base. For example, when the data subjects are consulted, they would bring their foresight in the risk assessment, thereby giving meaning to the procedural justice or transparency that De Hert and Gutwirth place at the core of their theory.

In assigning this role, the three-test approach described IOSH training manual for defining the scope of reasonable foreseeability in identifying risk within a work environment—common knowledge, industry knowledge and expert knowledge—was suggested.[669] While it is notable that the context is different and involves different risks (the risk to physical health, not privacy), this study argues that this does not affect the usefulness of transplanting this approach to data protection. This is because the level of knowledge required by a "reasonable person" to identify data protection risks maps well with the description in this manual. However, some contextual refinement may be needed, as indicated below. According to the IOSH manual, the knowledge categories are defined thus:

i. **Common knowledge** – if any reasonable person would identify the risk associated with the work then it is *reasonably foreseeable,* e.g. every reasonable person would recognise the risk associated with working on the sloping roof of a tall building.

ii. **Industry knowledge** – if a particular risk is well-known and understood in your industry then it is *reasonably foreseeable.* For example, putting a worker into an unsupported deep trench dug into the ground is commonly recognised as a risk in the construction

[668] It is also notable that the phrase 'rights and freedoms of the data subject' appeared in many places under Article 35 of the GDPR, perhaps indicating that human subjects that are the focus of the risk assessments under the Regulation.

[669] RRC, *IOSH Managing Safely* (n *333*).

industry. This risk might not be recognised by a person who does not work in construction, but it is still considered reasonably foreseeable because workers and organisations are expected to have a certain degree of industry knowledge.

iii. **Expert knowledge** – if a risk is outside the knowledge of most of the competent people working in a particular industry, then that risk might be described as not *reasonably foreseeable.* Only experts are expected to recognise such risks. For example, if a chemical is not classified as hazardous to health and is not generally recognised as harmful in a particular industry, then exposing a worker to health risk from such a chemical could be described as not reasonably foreseeable, even though there might be some research chemists who would disagree if asked for their expert opinion.[670]

The manual considers that knowledge in the first and second categories is expected of employers in most cases. However, it is rare to expect risk to be identified and managed in the third category unless the assessor is an expert. Though focused on work safety, this approach is arguably relevant in several situations, including data protection risk identification scenarios.

As earlier suggested, there are pointers in the consultation requirements of the GDPR during a DPIA that could explain this test, notably by requiring the DPO and the data subjects or their representatives to be consulted in the course of a DPIA exercise. Arguably, this implies that the foreseeability in risk identification within the scope of a DPIA should span from risks identifiable by common knowledge to expert knowledge, as the following discussion shows. In the first category, anyone who has a common knowledge about data processing would quickly identify that specific techniques pose certain threats, for example, transmitting unencrypted sensitive personal data over an open network. In this regard, it is expected that any risk assessment should identify those threats familiar to the ordinary person who has a common knowledge of the context of the data processing operation. Apart from these apparent threats, there is also a higher expectation that the data controller should be aware of the industrial practices within its sector (industrial knowledge). There are several examples of this sector-specific threat, such as those seen in the Smart Grid DPIA

[670] Ibid.

template [671] or the threat analysis for the SDN architecture by the Open Networking Foundation.[672] By requiring that the DPO must be consulted during a DPIA (and also data subjects or their representatives in appropriate cases), the GDPR envisages that a person with good technical and legal knowledge of the specific industrial practice should assist in identifying the risk (sectoral context of the data processing). Here too, staff members with technical knowledge should be consulted as well.

The third category, expert knowledge, requires a little nuance as to what the term 'expert' may mean in the context of DPIA. Several actors in data protection may be seen as experts, such as DPOs and supervisory authorities. In the context of a DPIA, DPOs are expected to have 'expert knowledge in data protection law and practice' to help the data controller conduct a DPIA. Several opinions further support their qualification as experts.[673] More importantly, there are various certification programmes for DPOs;[674] and the WP29 and the CNIL envisage that a DPO should also have some 'technical knowledge' about the system.[675] Besides the DPO, the data controller is also free or even expected to consult the data processor or external experts where the circumstances require.

---

[671] Smart Grid Task Force, 'Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems' (v.2 of 13 September 2018) 40 <https://ec.europa.eu/energy/sites/ener/files/documents/dpia_for_publication_2018.pdf> accessed 27 August 2019.

[672] ONF, 'Threat Analysis for the SDN Architecture' (Version 1.0, July 2016) <https://www.opennetworking.org/wp-content/uploads/2014/10/Threat_Analysis_for_the_SDN_Architecture.pdf> accessed 21 December 2019.

[673] See Korff, 'The DPO Handbook' (n 412)126-127; WP29, 'Guidelines on DPOs' (adopted 5 April 2017). Kloza et al finds that one of the best practice requirements of impact assessment is that the risk assessor or a team of assessors possess 'sufficient knowledge and know-how'. See Kloza et al, (n 70) 2.

[674] For example, IAPP Certification <https://iapp.org/certify/cippe-cipm/>; Irish Computer Society, 'European Certified Data Protection Officer Programme' <https://www.ics.ie/training/european-certified-data-protection-officer-programme-1>; Maastricht University, 'Data Protection Officer (DPO) Certification 2019' <https://www.maastrichtuniversity.nl/events/data-protection-officer-dpo-certification-2019> accessed 21 December 2019.

[675] CNIL, 'Guide Du Correspondant Informatique Et Libertes' (2011 edition) 7-8 <https://www.cnil.fr/sites/default/files/typo/document/CNIL_Guide_correspondants.pdf> accessed 21 December 2019.

An indication of whom to consult in this scenario could further be gleaned from the matrix for assigning responsibility seen in the AEPD guidelines on DPIA, which identify persons occupying the following responsibilities as relevant for a DPIA:

1. those responsible for performing the task (Responsible)
2. those responsible for the task being carried out (Accountable)
3. those who must be consulted to perform the task (Consulted) and,
4. those who should be informed about the completion of the task.[676]

While it may seem too high to require expert knowledge in data protection risk assessment judging from the IOSH manual, the interpretation of 'expert' in the domain of data protection, as explained above, seem to accommodate or envisage such knowledge during a DPIA. Arguably, the aim is that by consulting relevant stakeholders during a DPIA, including experts, the right information should be obtained to assess the risk. In practical terms, it is suggested that since the stakeholders in the second and third categories may be similar or merged, data controllers and processors should strive to leverage both industry and expert knowledge during a DPIA exercise. At first, it is suggested to use internal experts and involve external experts based on the technicality, sensitivity and nature of the processing.

The next section shall operationalise the potential output of this knowledge base in a risk assessment process with a use case.

5.4.1 Operationalising the Study's Risk Assessment Model

As already indicated, the risk assessment process of ISO 31000 is favoured as a model for a DPIA's risk assessment phase. Therefore, although the entire risk management process under this standard comprises six processes (see Section 5.3.1), in the following, we shall concentrate on operationalising only the process of risk assessment comprising risk identification, risk analysis and risk evaluation.

5.4.1.1 Risk Identification

A vital contribution of the process of risk identification is for the risk assessor to answer the question of what could go wrong and what are the consequences in a venture. This helps identify the principal risk contributors: the threats, threat events, vulnerabilities and possible harms should the threats materialise.

[676] AEPD, 'Guide on DPIA' (n 395) 8. Translation from Spanish by the author.

In the context of data protection, a threat refers to a thing or person or circumstance that exploits the vulnerabilities in the data processing operation with the potential to cause harm to the data subject, while a threat event refers to the actual event that materialises this threat. For example, there are vulnerabilities in transmitting unencrypted personal data over an unsecured network. A hacker (the threat) could exploit this; while the threat event is the particular event where a hacker infiltrates the networks, say through a man in the middle attack, and obtains personal data such as financial information of a data subject. Suppose this personal information is used to withdraw money from the account of a victim data subject, in that case, at least two harms may have occurred, financial loss, and psychological harm (the knowledge that one's data is in the hands of hackers). This scenario leads to another general harm, the violation of the rights and freedoms (e.g the rights to privacy and data protection) of the data subjects (the object of protection, whose data forms the assets).

In practice, risk identification should identify and describe the assets, vulnerabilities, harms, threats and events that could arise from the intended uses and foreseeable misuse of the data. They should be analysed in further steps to understand the conditions that, if exploited, could lead to harm. At least in other fields, there are many methods of threat and vulnerability identification, such as the use of checklists and brainstorming, risk register or hazard logs, hazard and operability (HAZOP) study, among others.[677] Unfortunately, no such established methods have been agreed upon in the field of data protection. Nevertheless, the following tools seem relevant for this purpose: brainstorming, use of risk register (where such exists), sector-specific threat/vulnerability glossary, opinions of the supervisory authorities, expert analysis, consultation with relevant stakeholders, etc. Arguably, the nature of data protection risk requires using a combination of methods to discover threats, vulnerabilities and harms.

Notably, the GDPR provides some generic metrics for consideration during risk assessment—nature, scope, context, and purpose of data processing. As argued earlier, these generic factors could be further fragmented and concretised at a low level to assist in the risk assessment process. For example, it seems too generic

[677] Rausand (n 156) 124-126.

and high level to talk about the nature of a data processing operation when identifying risk; this could be broken down, at least into two large units—the nature of the system used in the data processing and the nature of the data to be processed. Modelling data protection risk identification through such an approach allows each of these two units to be calibrated further into sub-units to cover the granularity of the system and data. For example, the nature of the data processing system could be expanded to include: type of technology, the hardware and software component, the technical security controls; while the nature of the data could be expanded to cover: the category of data, the vulnerability of subjects, data flows and sensitivity of data. This way, other metrics not mentioned in the GDPR could then been incorporated through such granularity depending on the context. This model is exemplified in more detail using the following use case.

Knowing what to consider when assessing risk can undoubtedly assist data controllers and processors to improve their DPIA's efficiency and effectiveness in practice. An important issue here is how to develop these metrics in the absence of any comprehensive guide or assessment performance indicators by the data protection authorities. Admittedly, this is a challenge because data protection law does not yet have defined rules or techniques to measure risk. Individual stakeholders would therefore require expertise to develop meaningful and objective metrics or factors. This study has learned lessons from information security risk management[678] and other areas where there are metrics and key performance indicators for measuring risk to introduce a generic metrics guide for data protection controllers and processors within the context of DPIA.

5.4.1.2 The Use Case Scenario

A private enterprise proposes a new and innovative intelligent personal health record system to process users' health-related data worldwide. This system will combine data, knowledge of artificial intelligence, and software tools to allow users to become more active in their healthcare. Through this system, the users can record daily life-status information, maintain a record of medical exams and define the access rights to their

[678] In information security risk management several metrics exits for diagnosing and measuring security. See Tung Sun, 'CYBER 503x Cybersecurity Risk Management Unit 5: Security Metrics' (Lecture Notes September 2021). See also section 5.2.

data. In addition, the platform will regularly monitor the psycho-emotional status of the users based on their records of everyday life experiences. Furthermore, different groups of users and their families can share information through diaries, and clinicians can also be provided with clinical information where the user permits.[679]

Assuming we take the users' sensitive and non-sensitive personal data as assets, how could the risks (e.g, in terms of threats, vulnerabilities, harms) posed by this proposal be identified and assessed using the **nature, scope, context, and purpose** metrics?

5.4.1.2.1 Identifying threats/vulnerabilities through the nature of data processing: system and data perspectives

The *nature* of data processing could be relied upon as a factor or source for threat identification. This could be viewed from two angles, as earlier suggested: the system and the data perspectives. To use the *nature of the system* as a source for risk identification, the risk assessor here ought to consider the following:

- The type of technology (whether it is old or new).
- The hardware and software components of the (proposed) system—the architectural design, the network components and hosting environment (if the system will be hosted in a public cloud, for example, this triggers more threat sources of which historical data and literature about specific cloud computing threats will help identify threats in such cases).[680]
- Furthermore, the nature of technical security controls may equally breed threats, such as when such security controls are outsourced—the link to third parties here has its weaknesses that could generate threats.
- Other factors, depending on the context of the actual scenario.

When all these metrics are contextualised, in addition to information obtained through consultations with relevant personnel, experts and other stakeholders,

[679] This scenario is adapted from the iPHR manual <https://www.iphr.care/apps/procedures/static/Tutorial.pdf> accessed 20 December 2019. The present author had the opportunity of working with the developers of this tool in the p-medicine project (EU funded, Grant Agreement 270089).

[680] See for example, ENISA, 'Cloud Computing: Benefits, Risks and Recommendations for Information Security' (ENISA 2009); ENISA, 'Cloud Security Guide for SMEs' (ENISA 2015); P.S. Suryateja, 'Threats and Vulnerabilities of Cloud Computing: A Review' (2018) 6:3 International Journal of Computer Sciences and Engineering 297.

the data controller should be able to have a clearer picture of the threats facing the proposal from the nature of the system's view.

The present scenario assumes that the proposed system will include some innovative (new) technology. Notably, the GDPR emphasises that the nature of the technology can be a source of risk. In this case, emphasis should be, among others, on whether this technology has been tested; whether there is a knowledge base regarding the threats and vulnerabilities associated with it or if it is a new technology with a 'black box'. If a new technology, the threat of failure of such new technology—not performing as expected—should be considered at this point, as that could occasion many other threats, such as bugs, supply chain threats, hackers, etc. The risk assessor should also bear in mind the significance of the uncertainty associated with new technologies, especially if there is no historical data or risk register to consult.

The other sub-categories—the nature of the hardware, software, network components and hosting environment, as well as the nature of the technical security and organisational controls, are also relevant in the present use case and closely related to the technology used to build the system. Here, research and consultations with appropriate experts and stakeholders associated with the system can help reveal these threats and vulnerabilities.

Regarding the other limb, risk identification through the *nature of personal data*, it is evident that in this use case, both special categories of data—data relating to health, vulnerable people's data such as children, the elderly, the sick, etc., and ordinary personal data—e.g., registration data, location data etc., will be processed. The data envisaged in this scenario include highly sensitive data, and the loss or unlawful alteration of such data could have a significant impact. Processing health-related data pose a higher risk than ordinary data in some ways. For example, processing inaccurate data relating to health could be colossal in some cases, such as in an emergency, and the risk is significant. In this present scenario, accuracy may not be guaranteed, partly because the data subjects will be populating the database (some of whom may not be knowledgeable about medical terms). This is a significant vulnerability. Other threats, such as unlawful access, unauthorised alteration, etc., could be identified from this scenario, primarily

because there is a possibility for users and their families and relatives to have access to data (nature of data flows). Similarly, the authentication data and others also have their relative threats that could be identified by their nature.

5.4.1.2.2 Identifying threats/vulnerabilities through the scope of data processing

Threats and vulnerabilities can also be identified by looking at *the scope of data processing*. To achieve a level of granularity necessary for this exercise, this factor could be further broken into sub-factors, such as the location of the data subjects, the number of data subjects, data retention period, the involvement of processor/sub-processors or other third parties/recipients; the scale of processing, envisaged international data transfers. The context can determine other factors. By looking at the global scope of the proposed system, the large number of expected data subjects and the large scale of the processing, among others, a risk assessor should be able to identify some specific threats and vulnerabilities. For example, a security threat could emanate from a weak link arising from the involvement of users with insufficient knowledge of security precautions. Also, international data transfers could occur depending on where the servers and the other physical infrastructures are hosted, which carry their threats and vulnerabilities. The use of processors or third parties could also pose some threats and vulnerabilities on their own. This point could be seen from the business structure and regulatory challenge faced by some enterprises with a global reach, such as Apple, Google, Facebook, etc. Their main headquarters are in the USA, while they process data from users worldwide. For example, this poses threats such as the US government subpoena of foreigners' data and/or the seizure of data and equipment of Facebook to gain access to such data.

When these sub-categories have been thoroughly analysed, more threats and vulnerabilities could become evident to the data controller given the processing context. From such results, the data controller could decide to limit the scope of the processing or localise the processing based on specific legal requirements (e.g., EU rules on data transfers). Such measures will form part of the risk treatment measures in a later stage.

5.4.1.2.3 Identifying threats/vulnerabilities through the context of data processing

By looking at *the context of the processing*, that is, the processing circumstances, which may be broken down, for example, into the legal context, the internal, and the external circumstances surrounding the processing, threats and vulnerabilities could be identified. In the present use case scenario, vulnerabilities and threats could be identified by analysing the legal context such as the legal basis of processing and data transfers including international data transfers. Within the legal framework for transferring personal data to third countries, for instance, vulnerabilities and threats emanate from processing in countries without adequate legal protection for data. Similarly, threats and vulnerabilities could be identified from the internal environment of the processing, such as from the employee (e.g., a disgruntled or negligent employee who steals or exposes data, suggesting a threat of illegitimate access to data). The external environment, such as the location and device used by the users to connect to the system, may also pose threats and vulnerabilities (e.g., hackers can access such a device). Of course, there could be other sub-categorisation, again depending on the context of data processing.

5.4.1.2.4 Identifying threats/vulnerabilities through the purpose of data processing

Finally, threats and vulnerabilities could equally be determined based on the *purpose of data processing*, with sub-categories such as the possibility of further processing. In our present case, while on the surface of it, the purpose of the processing is legitimate, that is, to allow users to keep a personal health record, there is potential for further processing by the data controller, such as for advertisement and marketing of pharmaceutical products. Such additional processing introduces other threats such as processing without consent or profiling that leads to discrimination, for example.

It is important to point out here that the above metrics are not meant to be exhaustive. The primary goal of developing such in this study is to facilitate insight on value delivery and process improvement. It will assist stakeholders in performing risk assessment, focusing their attention on causes and analysis of threats, vulnerabilities, among others relevant risk dependencies. In essence, this approach introduces a systematic and standardised framework into the exercise

and any stakeholder intending to assess risk during a DPIA could adapt it. It is suggested here that such adaptation should be contextually specific and relevant to aid in decision making and action-taking. Vague and confusing metrics should be avoided. If carried out systematically, and the appropriate consultations made, this exercise gives the assessor the first indications of the weaknesses that could be exploited by a threat (inherent from the technology, the organisation, the data, the environment or the business process). By looking at the nature, scope, context and purpose of the data processing (both from the planned activities and unplanned ones, e.g., hacking), the data controller could also envisage risk controls for possible application during the risk treatment or mitigation phase of the DPIA.

The discussion above is illustrated in the table below, indicating these four generic factors primarily.

Table 4: Factors for consideration during the risk identification process

Risk Assessment Stage	Factors for consideration	Sub-categories of the factors
Risk Identification	**1. Nature of processing**	
	-Nature of the processing system	Type of technology (old or new)
		Hardware, software, network components and hosting environment
		Technical and security controls
	-Nature of personal data	Category of data
		Vulnerability of subjects
		Data flow
		Sensitivity of data
	2. Scope of data processing	Location of subjects
		No of data subjects
		Retention period
		Use of processor/sub-processor/third parties/recipients
		Scale of processing

	International data transfers
3. Context of data processing	Legal environment and basis of processing
	Internal and external framework for processing
4. Purpose of data processing	Purpose of processing
	Possibility of further processing

From the table above, the generic factors suggested in the GDPR is used as a starting point for modelling threat/vulnerability identification. The table shows how these four generic factors could be broken down further to achieve the desired contextual level of granularity. It is also notable that these factors may yield different outcomes and could result in duplication of threats/vulnerabilities or even multiple threats/vulnerabilities. It is left for the risk assessor to determine how to combine and use their output.

As already discussed in Chapter One, what amounts to data protection threats, vulnerabilities and harms cannot be exhaustively defined; they are contextual. However, in some sectors, there are a more detailed, sectoral list of threats, and such a list should be encouraged in the data protection sphere to help risk assessors not overlook specific threats. For example, the Open Networking Foundation has identified and listed some threats to the Software-Defined Network (SDN) architecture.[681] Notably, some examples of data protection threats can be found in the literature,[682] though one must be careful with the terminology used to describe these threats as they may be mixed up.

[681] ONF, 'Threat Analysis for the SDN Architecture' (Version 1.0 July 2016) <https://www.opennetworking.org/wp-content/uploads/2014/10/Threat_Analysis_for_the_SDN_Architecture.pdf> accessed 20 December 2019.

[682] See for example, ICO, 'How do we do a DPIA' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-

The remaining question is, what potential harms could be identified from these threats? Similarly, it has to be stressed again that harm must be evaluated based on the concrete circumstances of each case. However, some examples of data protection harm gathered from the literature broadly include physical harm, financial loss, identity fraud, reputational data, societal harm, among others.[683] Again, these harms could be extracted using the aid of nature, scope, context, and purpose metrics, where applicable.

In conclusion, it is possible to rely on the nature, scope, context, and purpose of data processing for modelling risk identification and breaking them down to achieve the desired granularity given an actual scenario of a data processing operation. As the first step in the risk assessment process, the output of this exercise will be significant for the other stages and directly forms an input to them. In the next section, risk analysis shall be considered.

5.4.1.3 Risk Analysis

Risk analysis is the second stage in risk assessment according to the ISO 31000. It is the process of understanding the characteristics of the threats, vulnerabilities and harms identified earlier in terms of the possibility of their happening (individually or collectively) and the impact should they occur. In this phase, the sources and controls of the threats are analysed further to assess their effectiveness. Here too, using defined metrics for assessing this likelihood and severity is necessary to determine the risk level in the end. For example, the UK's Green Leave III notes: '[t]he likelihood of harm depends on the susceptibility and vulnerability of a receptor to the hazard, on the potency of the hazard itself, and on the amount or extent of exposure.'[684] From this comment, three factors are identified for measuring the likelihood of harm.

assessments-dpias/how-do-we-do-a-dpia/#how10> accessed 12 December 2019.

[683] See section 3.4.3.

[684] Gormley, '*Guidelines for Environmental Risk Assessment*' (n 623) 29.

The elements of likelihood and severity are prominent in the probability theory,[685] and several risk management frameworks also emphasise them. They are usually assessed using a qualitative or quantitative method or both, depending on the context. A quantitative method uses a numerical scale to gauge the probability of occurrence of each risk. For example, the likelihood of risk can quantitatively be noted as follows: Risk #1 has a 60% chance of occurring, Risk #2 has a 27% chance of occurring, and Risk #3 has a 76% chance of occurring, and so on. On the other hand, a qualitative method uses a relative or descriptive scale such as 'Low, Medium, High' to indicate the likelihood of a risk event occurring or its severity. The qualitative method is frequently used in circumstances where the risk event cannot be described in mathematical terms, such as a data protection breach. [686]

Although there is no consensus on the structure or factors for determining and measuring the likelihood and severity of data protection risk, the CIPL calls for 'objective judgments' in this regard.[687] As such, both quantitative and qualitative methods may be combined where appropriate and practicable in data protection risk analysis.[688] What matters in practical terms is that such analysis ought to assist in understanding the vulnerabilities that the identified threats could exploit and the harms that may result from that.

Returning to our use case scenario, we shall use the generic metrics provided by the GDPR (nature, scope, context and purpose of the processing) to exemplify the risk analysis process. A similar approach as used above shall be adopted here, with some adjustments to suit the context. Using the threat associated with loss

[685] Probability is defined as the likelihood that the event will occur. Cheryl Wilhelmsen and Lee Ostrom, *Risk Assessment: Tools, Techniques, and Their Applications* (1st Ed, Wiley 2012) 85.

[686] An indication of qualitative factors to measure the likelihood and severity could be seen in the risk assessment formula of Vodafone. In assessing the privacy risk associated with geolocation services, two factors were used to consider the likelihood that certain impacts would materialise: the combination of location capabilities within highly social applications, and the increase of open handsets and application development environment. Wright, *Privacy Impact Assessment* (n 34) 293.

[687] CIPL, 'A Risk-based Approach to Privacy' (n 13) 6.

[688] The usual step in this method is first to define or describe the criteria for measuring any outcome. For example, it could be said that any breach that affects more than 100 data subjects is of a severe or high risk, or any breach in which the data subject may incur financial loss below 100 Euro is of low risk or less severe.

of confidentiality to exemplify this approach, we ask the question, what is the likelihood that a vulnerability in the data processing system could be exploited to result in a user losing the confidentiality associated with the data and how severe could the impact be? In this scenario, the risk assessor should be able to analyse whether, given the *nature* of the processing—the type of technology, the components (hardware, software, etc.) involved in the proposed system, the technical and non-technical controls—there is a likelihood that this threat could occur. Historical data, stakeholder/expert consultation, and literature evidence can be relied upon for this analysis. Similarly, for analysing the severity should the threat materialise, the category of data, the nature of harm, as well as the value in terms of financial loss, could form the parameters for measuring the severity.

Regarding the *scope* of data processing, the likelihood of this threat materialising could also be analysed based on the volume of data, involvement of processors/sub-processors, data retention period, the type and location of data recipients, and the international nature of the data transfer. On the other end, Severity could be based on factors such as the number of data subjects and the age ranges.

Furthermore, likelihood analysis can be based on the *context* of the data processing. This could be centred on the following categorisation: history of past incidents, possibility of aggregating data with other available data, and prevalence of means and methods of exploiting data, while the severity could be analysed from historical data. Finally, by looking at the *purpose* of data processing, the likelihood and severity analysis could be analysed based on factors such as the purpose of data processing, e.g., whether it involves profiling, and whether there is a possibility of further processing data. The legal effect of the processing could be a parameter for analysing the severity here. The table below gives a summary of this approach and how the factors could be broken down.

Table 5: Factors for consideration during a risk analysis

Risk Identified	Factors for consideration	Risk analysis	
Loss of confidentiality		**Likelihood**	**Severity**
	1. Nature of processing	Type of technology[689]	Category of data and its sensitivity
		Technical security controls	Nature of harm
		Components involved (hardware, software, network and host environment)	Value in financial loss or likely emotional impact
	2. Scope of processing	Volume of data	No of data subjects
		Involvement of processors/sub-processors	The age ranges of the data subject
		Retention period	
		processor/third parties/recipients	
		International data transfer	
	3. Context of processing	History of the past incidents	History of the past incidents
		Possibility of aggregating data with other available data	
		Prevalence of means and methods of exploiting data	
	4. Purpose of processing	Purpose of processing	Legal effect on the data subject
		Possibility of further processing	

The parameters in the table above could be further broken to suit the context of the analysis. For example, the history of past incidents could be further broken down in time and space (e.g., whether the incident has occurred in a similar sector or another sector). Financial loss as a factor for severity could also accommodate

[689] Hardware, software, network components and hosting environment.

further division, such as the cost of implementing mitigating measures should breach occur, the cost of the inability to use service, etc. Although we have used just one threat here as an example (threat of loss of confidentiality), the same approach should be adopted to analyse other identified risks. Of course, these criteria are not exhaustive; they should be further determined during contextualising the DPIA in the earlier stage and updated as the assessment progresses.

At this stage, what is also essential is how the likelihood and severity are combined to measure the risk level for each threat. One conventional approach for this exercise is using a risk matrix to show the relationship between the likelihood and severity of impact. A risk matrix is a table or grid that indicates the likelihood (e.g. from remote to highly likely) on one side and the severity (e.g. from minor impact to severe impact) on the other side. Each of the factors in the table could be used to design the scale of the risk level. For example, using the financial value of the loss, one could range the scale of the severity or impact from 1 to 4 as follows:

Table 6: Criteria for the severity of impact

Description of impact	Severity of impact	Scale
If the financial loss is below 500 euro	Minor impact	1
If the financial loss is between 500 to 1000 euro	Significant impact	2
If the financial loss is above 1000 euro	Serious impact	3
If the financial loss is above 10000	Severe impact	4

Similarly, the likelihood of data breach (e.g., in the sector of processing) could be presented in the following scale for the likelihood of occurrence:

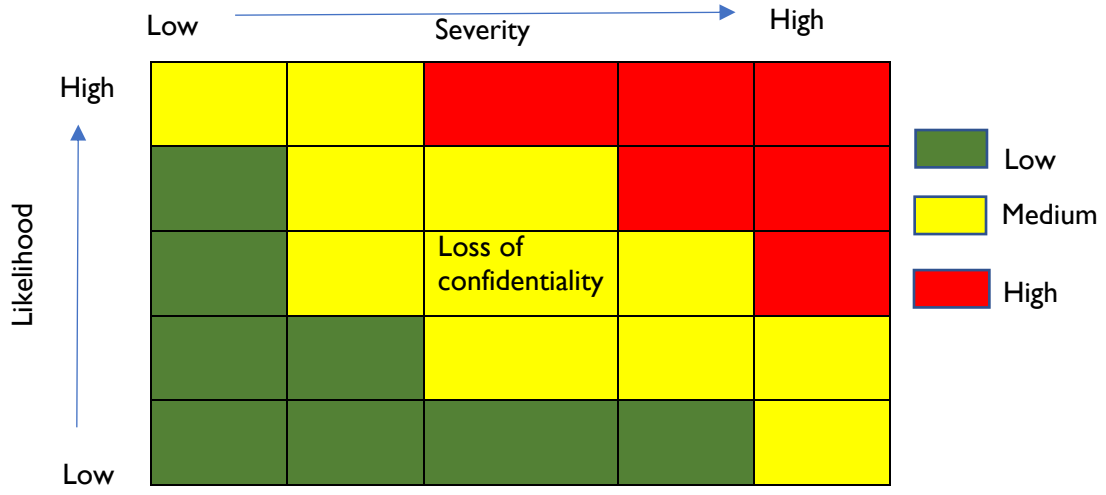
Table 7: Criteria for the likelihood of risk

Description of likelihood	Likelihood of occurrence	Scale
Breach has not occurred in the past 10 years	Remote	1
Breach has occurred in the past 5 years on less than 2 occasions	Possible	2
Breach has occurred in the past 5 years on less than 5 occasions	Significantly likely	3

Breach occurs every year on more than 5 occasions	Highly likely	4

Let us assume that after using various criteria determined by the risk assessor for each of these exercises, the risk assessor wants to have a picture of the overall risk for each threat. Using the threat associated with loss of confidentiality as an example, we assume that the likelihood of this threat is "medium" (based on the combined analysis of the factors listed in Table 5) and that the severity is "medium" (also based on a combination of factors), a risk matrix could then be plotted to picture the risk level for this threat as follows. Here, the likelihood is plotted on the y-axis, while the severity is on the x-axis, as shown in the figure below.

Table 8: Sample of a data protection risk matrix



All the other threat levels could be plotted within such a matrix to get a picture of the overall risk landscape. In sum, as shown in this section, there is a feasibility of adapting conventional practices used in measuring the likelihood and severity of a risk to the area of data protection risk assessment. While such adaption may require knowledge about data protection, literature on the conventional risk analysis approach is valuable in this quest. In the next section, the risk evaluation shall be considered.

5.4.1.4 Risk Evaluation

The final process in risk assessment is risk evaluation, which compares the results of risk analysis with the established risk criteria. This process assists in the decision making about the risk treatment (relevant risk mitigation measures to reduce or eliminate the risk), especially in prioritising risk based on its impact and the

allocation of resources. It is also relevant to apply the thresholds of risk acceptance (which must have been defined in the earlier risk management processes).

In the case of data protection, the GDPR primarily determines the criteria for risk acceptance through the various obligations imposed on the data controllers and processors. Therefore, when evaluating risk during a DPIA, the risk assessor needs to answer the following question before the risk acceptance:

- Does the evaluation indicate compliance with data protection principles?
- Does the processing violate any of the rights of the data subjects?
- Does the processing accord with the legitimate expectations of the data subject?
- Would the data controller be in breach of any of its obligations by accepting the risk as it is?
- Does the organisational risk culture accord with the risk analysis? And so on.

Of course, it will be detrimental to accept any risk that would breach the obligations in the GDPR, as there is a hefty fine associated with any such violation. Thus, possible criteria for risk evaluation should include considerations relating to:

i. The rights and freedoms of the data subjects;
ii. The views of the stakeholders;
iii. The nature of the uncertainties that can affect the DPIA;
iv. The impact of a cumulative risk materialisation;
v. The obligations of the affected data controller or processor;
vi. The risk culture and policy of the data controller;
vii. The nature of controls needed to treat the risk;
viii. Others as applicable.

Let us exemplify this with our use case, using the risk of breach of confidentiality. In evaluating this risk against the first consideration, the risk assessor should consider the possible rights and freedoms that may be affected if such materialises. For example, it could lead to discrimination; it might also affect the subject's right to dignity; right to informational self-determination, among others. Exposing all the potential rights and freedoms that could be violated will allow the risk assessor to implement appropriate measures to prevent such violations, as well as to know what level of risk to accept based on the risk acceptance criteria. Similar exercise

should also be done with the other factors and extend such to the other risks using these considerations as they apply.

In general, the systematic framework for risk assessment proposed in this study can be diagrammatically represented, as seen in Figure 13 below.

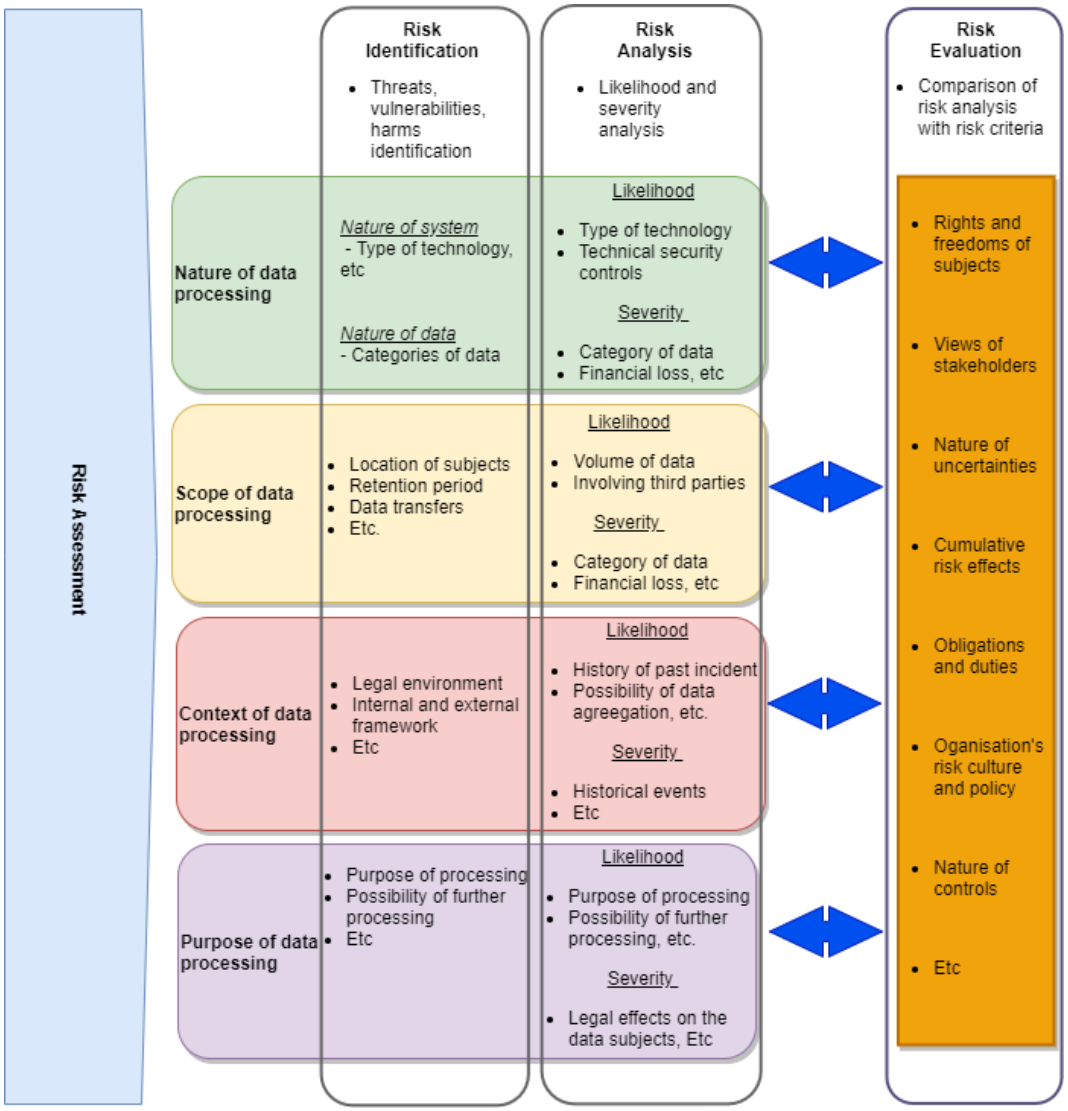


Figure 13: A proposed systematic risk assessment model

This diagram shows that the metrics of nature, scope, context and purpose of data processing as indicated in the GDPR can be used to plot risk identification and analysis, while different parameters apply for the risk evaluation to suit the purpose of the assessment. The constellations presented in this approach are not static; they could be modified based on the processing context. This model's overarching aim is to assist risk assessors in using objective and systematic criteria during the risk assessment exercise, which can be measured and repeated. This way, independent observers or supervisory authorities could evaluate whether the proper parameters have been used to assess the

risk. Overall, the metrics exposed here are generic and meant as proof of concept; they would require refinement and adaptation to suit the context.

5.5 Risk Assessment and the Close Link with Risk Treatment

It is worth emphasising that the process of risk assessment is closely linked to risk treatment in the ISO 31000 framework. The output of the former is a direct input to the latter, and assists in selecting the best options for mitigating the identified risks. In a nutshell, risk treatment options may involve one or more of the following:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- taking the risk in order to pursue an opportunity;
- removing the risk source;
- changing the likelihood;
- changing the consequences;
- sharing the risk (e.g. through contracts, buying insurance);
- accepting the risk by informed decision.[690]

During a DPIA, it is left for the risk assessor to decide which options to follow given the context of the data processing, legal requirements, as well as the risk acceptance criteria mentioned earlier. The Finnish supervisory authority, for example, suggests some data protection risk treatment measures in its guidelines as follows:

- deciding not to process certain kinds of data
- specifying or limiting the scope of processing
- shortening retention periods
- adopting additional security measures based on a specific risk
- anonymisation and pseudonymisation of personal data
- adopting written processing guidelines
- increasing human contribution to automated decision-making processes
- switching to a different technology
- adopting unambiguous agreements on the exchange of information
- giving data subjects the right to prohibit processing, where possible
- adopting systems and procedures that promote individuals' data protection rights.[691]

[690] ISO 31000:2018, 13; see also ISO/IEC 29134:2017, 19-21.

[691] Office of the Data Protection Ombudsman, 'Carrying out an Impact Assessment' (n 553); See also the CNIL, 'Privacy Impact Assessment (PIA) Knowledge Bases' (February 2018 Edition).

Notably, such a list cannot be exhaustive. Another essential point to note here is that risk treatment is not a one-off process; some mitigation measures could also introduce new risks. Therefore, it is essential to monitor and review activities designed to treat risk regularly. If any residual risks remain high after applying risk treatment measures, then a consultation with the supervisory authorities is triggered according to Article 36 of the GDPR.

5.6 Prospects and Challenges of the Proposed Approach in this Study

Developing a systematic and transparent way of conducting a DPIA is undoubtedly a desideratum for data controllers and processors. The approach suggested in this study supports such a systematic approach. However, in adopting this approach, there are possible prospects and challenges, especially given that DPIA is a newly introduced requirement at the EU level. Therefore, the community is testing various models.

On the one hand, there is a prospect that adopting the approach suggested in this study will benefit the data protection community in having a clear view of what is required when a risk assessment is conducted during a DPIA. This will save data controllers and processors from the risk of fines associated with a breach of the Regulation (in this case, for not conducting a proper risk assessment). Therefore, every data controller wishes to know the best way to comply with the Regulation, and adopting a systematic framework is a step in the right direction. Furthermore, given that risk assessment is a recurring feature in many provisions of the GDPR, such as when implementing data protection by design, there is a prospect that adopting a systematic approach will be helpful for the smooth implementation of these other obligations. Additionally, on a broader scale, adopting a systematic approach will provide the building blocks for further developing sector-specific frameworks with the requisite granularity. This will potentially save the time required for completing a DPIA in real scenarios.

On the other hand, the human characteristic of attachment to old habits poses a challenge with adopting a new approach to things. Thus, it is conceivable that some data controllers and processors may be reluctant to abandon what they are used to when conducting a risk assessment. This is coupled with the fact that some

stakeholders may not have the background to easily transpose this new method into their routine operations. Moreover, some stakeholders may prefer to wait until the authorities approve the proposed method before using it. Nevertheless, the value that the theoretical exploration of this study provides may entice many stakeholders in trying it out. Indeed, there is a prospect that the discussion this study will initiate may encourage some keen observers to attempt to use it.

5.7 Conclusion

This study has suggested systematising risk assessment during a DPIA using an eclectic approach where a transparent step-by-step approach guides a risk assessor in completing this task. Notwithstanding that they could devise factors that apply to their specific case, the relevant criteria here are essential and reflect the generic elements seen in the GDPR. Furthermore, there is a presumption here that the risk assessor would pursue the best option in this decision-making, given that if the risk assessment is incorrect, high-risk processing might be wrongly adjudged low or medium risk, potentially raising a compliance risk; conversely, low-risk processing would be incorrectly termed high risk, leading to a waste of resources, including prior consultation with the supervisory authority when, in fact, it is not required. Therefore, this study hopes that the systematic approach it proposes will go a long way in assisting stakeholders in their quest to apply the rules of data protection consistently and transparently.

CHAPTER SIX

6. CONCLUSION

6.1 INTRODUCTION

In the previous chapters, this study explored issues surrounding DPIA, particularly the risk assessment process. It has suggested a method for carrying out this assessment systematically and transparently. In doing this research, some questions were posed, first, to understand what it means to carry out a risk assessment in the course of a DPIA; second, to identify what key indicators or attributes should be considered when conducting this risk assessment. The previous chapters have tried to answer these questions, suggesting a framework that should guide the design and scope of a DPIA, in general, and risk assessment, in particular. In this final chapter, the study's key findings and their implications shall be re-emphasised to conclude the work. Recommendations shall also be made to key stakeholders such as data controllers and processors, supervisory authorities and the privacy community at large.

6.2 KEY FINDINGS AND DISCUSSION

Adopting a risk management tool in data protection frameworks has become necessary by implication of the risk-based approach incorporated in the GDPR. The key challenge, though, to data controllers is how to seamlessly integrate conventional risk management techniques when conducting DPIA, to comply with the requirements of Article 35, as well as present their assessment in an objective and transparent manner. These issues were addressed through two research questions, which were formulated to guide the study:

i. What does risk assessment entail for the purpose of conducting an *ex-ante* DPIA?
ii. What key indicators or attributes should be considered when conducting an ex-ante risk assessment during a DPIA?

In answering these questions, some findings were made, and the key ones shall be highlighted below. In addition, the broader implications that emerge from the study

shall also be discussed following the sequence of the above questions to advance readers knowledge on this subject matter.

First, in determining what it entails to carry out a risk assessment as part of a DPIA, a finding of the study suggests that although 'risk assessment' is recognised as one of the steps of a DPIA exercise (emanating from Article 35 (7)(c)), there is no uniform conception of what it means to carry it out. Data controllers and processors understand this obligation differently, ranging from those who attribute it as a call for checking compliance with data protection principles to those who adopt a conventional risk management framework to assess the threats posed to and by their data processing operations. Similarly, supervisory authorities differently interpret what it means to execute risk assessment during a DPIA. As such, no uniform approach or template exists for completing the entire process of DPIA, in general, and the risk assessment process, in particular. This has implications for the consistency required by the GDPR, especially for impact assessments with a cross-border effect.

Admittedly, the GDPR includes what could be termed 'a minimum content' of a DPIA under Article 35 (7). Nevertheless, the four paragraphs of this article have been differently interpreted in the guidelines by the supervisory authorities. As a result, the degree of objectivity and quality of the output significantly varies depending on which guidelines are followed. This fragmentation is evident from the templates and models available online, some of which have been cited in this study. One suggestion to improve this state of affairs is for the EDPB to activate the consistency mechanism in this area. Future guidelines should address this issue at the EU level and proffer a common strategy to completing Article 35 (7)(c) risk assessment during a DPIA. A leaf could be borrowed from the approach of the EDPB in harmonising the blacklist and white list under Article 35 (4) and (5). National authorities could then adapt these guidelines to suit their unique circumstances while maintaining regional harmony.

Another aspect of this subject matter closely linked to the issue discussed above and yet to be addressed consistently is the vocabulary around data protection risk management. Core terms, such as risk, threat, harm, are used indiscriminately. Furthermore, no glossary for data protection risk management has been agreed

(for which risk assessors could quickly consult when performing a DPIA). Such a glossary is needed and should form part of the update of the guidelines by the EDPB (as the authoritative body at the EU level). This would go a long way in harmonising the terminology in this area.

Second, on the question of key parameters or attributes for consideration during a risk assessment, the study found that although the GDPR requires an objective risk assessment, how to achieve this objectivity is one issue yet to be solved by the data protection community. There is a lack of clarity regarding the metrics (factors and parameters) to consider when conducting a DPIA's risk assessment exercise. While some generic indicators are mentioned in the GDPR (nature, scope, context, and purpose), there are no conscious efforts to develop these factors harmoniously and with the required granularity to instruct risk assessment. What exists in practice is polarised and diverse. Some guidelines lack explicit content as a process instruction for completing each of the risk assessment processes. As suggestive from Chapter Five above, some metrics could be developed around the provisions of the GDPR for a harmonious risk assessment. What is needed in this regard is community engagement and research to learn lessons from other sectors.

The lack of clarity concerning the risk assessment parameters has some implications regarding the transparency of the entire exercise. While much of the transparency discussions regarding the GDPR has been focused on the provision of information to the data subjects before the collection of their data or when an access request is made, the aspect of procedural transparency regarding *ex-ante* processes to show accountability (e.g., in a DPIA risk assessment) has not been emphasised as an integral part of the tool of control in data protection. However, the study has indicated that the ability of the data controller to show the steps taken and factors considered when assessing risks in the context of DPIA has a transparency effect, and undoubtedly, will positively affect the DPIA outcome, not only in content also in the form.

Given these findings, this study has suggested that data protection risk assessment should be viewed as an exercise of identifying, analysing and evaluating the vulnerabilities, threats and harms associated with personal data processing. It has

also been argued that in the context of DPIA, objective risk assessment presupposes a formal and systematic procedure for identifying these vulnerabilities, threats and harms, leading to suitable safeguards instituted against them. Although no particular methodology is mandated under the GDPR, the Regulation envisages that the data controller will choose the best method to reflect this objective. This study has suggested an adaptation of the ISO31000:2018 risk management standard to systematise DPIA and risk assessment in particular.

What then is the standard of objectivity to measure this risk assessment? The theoretical arguments made in Chapter Two suggests a strong indication that it is the standard of a 'reasonable man' within the context of the data processing environment based on the foreseeability doctrine. The pertinent question to be asked in the end would be whether a reasonable person who knows the data processing system could have foreseen the risk in the context of the data processing, given the nature, scope, context and purpose of the processing?

One other unique finding of this study relates to the role of DPIA in the liability and sanction regime under the GDPR. In this respect, while it is common knowledge that not observing Article 35 of the GDPR is a violation of the Regulation that attracts a penalty, there is no clear place for rewarding a well-done DPIA. This study has suggested that when it comes to supervisory authorities' fines, the controller's or processor's *ex-ante* DPIA should be considered in appropriate cases. Where all the reasonably foreseeable risks have been duly identified, analysed and evaluated, and adequately mitigated, and a subsequent breach happens, the fact that a prior DPIA was well designed and executed should reflect in the consideration during a fine. It should lead, at least, to a reduction of the fine. This has a broader implication of encouraging good practice in this area, and by extension reducing risk to the data subjects.

6.3 KEY CONTRIBUTIONS

This study has contributed to the GDPR's DPIA framework in the following ways:

1. Engaging in a doctrinal analysis of the structural plane of a DPIA based on GDPR provisions. This can be seen as the significant contribution of Chapter Three, where the provisions of Article 35 was discussed.

2. Designing a DPIA Architecture by mapping relevant provisions of the

GDPR with ISO 31000:2018 is another significant contribution of this study. As seen in Chapter Five, relevant requirements of the GDPR as pertains to DPIA have been translated within the ISO 31000 processes, with relevant missing portions plotted into the architecture for a more holistic outlook. This allowed the study to design a systematisation of the entire DPIA process.

3. Isolating the risk assessment process of DPIA and decomposing this process into Risk Identification, Risk Analysis and Risk Evaluation is another contribution of the study seen in Chapter Five. Risk assessment is the most crucial part of a DPIA because it is where the core risks and dependencies (vulnerabilities, threats, assets, impact, etc.) will be identified and evaluated. Therefore, such a decomposition gave room for giving risk assessment the attention it needs and also assisted in suggesting metrics for risk assessment.

4. As seen in Chapter Five, efforts have been made to articulate factors or parameters for completing each risk assessment process. This contribution of the study is an essential step towards the systematisation and standardisation of the DPIA framework. Relying on the metrics which the GDPR provide (nature, scope, context and purpose of data processing), the study suggested some granularity for the risk assessment (threat, vulnerability, etc) modelling.

6.4 RECOMMENDATIONS TO STAKEHOLDERS

The following recommendations are targeted at key stakeholders in the European data protection sphere, including data controllers and processors, supervisory authorities, and the European privacy community and researchers at large.

6.4.1 Data Controllers and Processors

- **Adopt a systematic approach to risk assessment, and conceptualise it purposively.** That is, approach risk assessment as an exercise meant to serve defined purposes of risk identification, analysis and evaluation, of which the outcome can be verifiable by an independent observer.

- **Define the criteria for risk identification, analysis and evaluation in measurable terms** to show transparency in the assessment. Moreover, avoid leaving grey areas or using vague metrics. Where a conclusion about the level of risk is made, point to the evidence or metrics

for arriving at this conclusion.

- **Incorporate the principle of foreseeability in the risk assessment exercise**. The degree of foreseeability should be that of a reasonable assessor in the data controller or processor position, given the context of the data processing. Utilise all relevant stakeholders (DPO, data subjects, employees, third parties, etc.) to help uncover and mitigate the risks. Any methodology adopted should avoid a race to the bottom, as this may affect the quality of the DPIA.

- In decisions relating to the factors or parameters to consider during the risk assessment, **adopt the best options to protect the data subjects**, given that the data subjects are the primary target of protection in a DPIA.

6.4.2 Supervisory Authorities, including the EDPB

- **The EDPB should design a harmonised procedural guidance for data protection risk assessment.** In doing this, the EDPB should apply the consistency mechanism, and clearly define the risk assessment principles, procedures and components relevant for a DPIA. Effectively, this means that future guidelines from the EDPB should not only focus on the form of risk assessment but also the content. If the building blocks are provided from an EU level, it will be easy for national supervisory authorities to adopt and adapt them where necessary, as well as data controllers to apply them in the specific contexts of their operations (see also Section 4.3.3).

- **The future guidelines should contain well-structured steps or processes for risk assessment as envisaged in Article 35 (7)(c) of the GDPR.** This gives risk assessment a functional separation from other parts of DPIA. The guidelines should include metrics (factors and parameters) for completing the risk assessment steps, criteria for inclusion or elimination of these factors, criteria for measuring the risk level, and how to treat the elements of uncertainty during the risk assessment. Importantly, the guidelines should adopt a hybrid model and contain examples and templates that risk assessors could adapt. In Section 4.3.3, a

detailed approach to future guidelines has been suggested.

- **Devise incentives to encourage systematic and transparent risk assessment practice.** This could be done by indicating that administrative fines could be eliminated or reduced when it is found that the data controller or processor has been transparent in its risk assessment and has considered all relevant and reasonably foreseeable risks during a DPIA. One approach to achieve this is by clearly indicating that when the issue relating to Article 83 (2)(b) borders on DPIA, the systematic manner of the risk assessment and the foreseeability scope adopted by the data controller shall be considered in determining negligence.

- **Strive to develop a data protection risk glossary of terms that will provide authoritative vocabulary associated with DPIA** such as data protection threats, harms, vulnerabilities, assets, etc**.** Inspiration for this exercise could be gained from the US Department of Homeland Security's *DHS Risk Lexicon.* [692] This approach will harmonise the terminology discrepancies around DPIA.

6.4.3 The Privacy Community and Researchers

- Efforts of the ISO at harmonising and updating the ISO standards concerning data protection risk management should be encouraged. However, **some relevant standards relating to privacy risk management need to be updated** as identified in Chapter Five, including ISO/IEC 29100:2011 and ISO 22307:2008.

- **Interdisciplinary research is recommended to the community of researchers in this area.** This is premised on the fact that risk assessment has an extra-legal origin and would require expertise from other disciplines such as risk management, data managers, software engineers, etc., to assist lawyers and data protection experts in the task of systematising the DPIA framework.

[692] Department of Homeland Security, 'Risk Steering Committee DHS Risk Lexicon' (September 2008) <https://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf> accessed 15 January 2020.

- **Further research is recommended to test and validate the methodology proposed in this study.** A comparative approach can be adopted to test it with similar methods from within and outside the EU jurisdiction with the view that lessons learned from this exercise will be used to update and refine this proposal in the future.

- **Research is also needed regarding the impact of *ex-ante* risk assessment, subsequent breach and liability imposed by the courts or supervisory authorities**. As well, a comparative approach should be adopted here to see the national and international developments in this area.

6.5 CONCLUDING REMARKS

The contribution of this dissertation is an attempt to develop a systematic and transparent framework for conducting a risk assessment during a DPIA as required by Article 35 of the GDPR. The framework proposed in this study adapts ISO 31000:2018 risk management processes to design a DPIA architecture, grounded by theoretical and conceptual methodology. The study has also shown how to operationalise risk assessment based on the requirements of Article 35 (7) (c) of the GDPR.

A major nucleus of the theoretical and conceptual framework of this dissertation is the description of what it entails to conduct a risk assessment and the conception of metrics that a risk assessor should consider while conducting this exercise to make an informed decision about the risks. By demonstrating the feasibility of a systematic and consistent approach to *ex-ante* risk assessment, this study has shown that a level of standardisation could be attained for implementing a DPIA across various data processing scenarios. This is arguably possible because the GDPR's requirements for *ex-ante* risk assessment are significantly sector-neutral. What is needed is concrete and harmonised guidelines to facilitate a smooth cross-sector application of DPIA.

A harmonised and systematic approach will bring a level of clarity in this respect, and the supervisory authorities would be able to weigh any assessment outcome.

Deviations that are not justifiable would easily be identified and questioned. One other advantage of adopting a systematic approach is that it makes it easier to translate guidelines into software for conducting a DPIA; arguably, therefore it was easy for the CNIL to transform its PIA template into open-source, downloadable software because of the systematic approach it adopted. Although the CIPL has briefly argued against harmonisation of DPIA risk assessment because it may stifle the flexibility needed to capture data protection risks, the approach suggested in this dissertation does not mean sacrificing the expertise of data controllers or risk assessors. Instead, as indicated in this study, a hybrid and systematic approach will even assist in channelling their thoughts and expertise in the right direction. This solution, however, requires future work aimed at validating the processes suggested in this study, which may reveal areas where flexibility may bring about the expected utility or optimal output and where it may not. As such, it should be possible to develop a template with defined and standardised parts, as well as subjective elements depending on the specific context of the application. This way, the one-size-fits-all pitfall feared by some critics would be avoided.

It is also worth emphasising that transparency is a tool upon which data protection is built, both as a principle and a way of showing accountability. It has also been used as an element of theorising data protection by De Hert and Gutwirth, though these authors did not develop the procedural aspect of this transparency theory that is relevant for *ex-ante* risk assessment. This study has shown how such procedural transparency can be applied within the context of DPIA, and argues that procedural transparency would increase the trust of the data subjects towards the data controller. Moreover, when correctly done, it would incorporate the views of the data subjects and other stakeholders as envisaged in the GDPR. This interaction allows them to "control" how their data is processed.

Finally, the output of this study differs from several prior studies on PIA/DPIA, as it focuses on the procedure and factors for completing the risk assessment phase of the DPIA. While many previous studies or guidelines have glossed over this issue, this study has sought to go beyond the surface to conceptualise what it means to assess risk in the context of data protection and has suggested a conceptual and theoretical basis for this. Given the importance of this subject matter to data controllers and processors, it is anticipated that this study will have

practical implications because it provides a step-by-step approach to conducting risk assessment under Article 35 of the GDPR. It will also be relevant to the data protection supervisory authorities because it suggests how they could approach future guidelines on the subject matter.

ANNEX I: TIMELINE OF THE INTRODUCTION OF IMPACT ASSESSMENT INTO EU DATA PROTECTION LAW

S/N	Timeline of events
1.	The UK's ICO funded a study: 'Privacy Impact Assessments: International Study of their Application and Effects', which report was published in October 2007.[1] Following the study's recommendations, the ICO published a PIA Handbook in 2007 (version 1.0, December 2007), which was revised in 2009 (version 2.0).[2] PIA was only mandatory for the UK public sector at this stage. The ICO also developed a PIA Code of Practice in 2014,[3] and following the GDPR adoption, has published a DPIA guidance from May 2018.[4]
2.	The RAND Corporation in a project that reviewed the DPD in 2009, which was sponsored by the UK's ICO, a PIA was considered among other tools for privacy protection.[5]
3.	The European Commission issued a recommendation on RFID in May 2009 calling on the Member States to ensure that industry, in collaboration with relevant civil society stakeholders, develops a framework for privacy and data protection impact assessments to be submitted for endorsement by the Article 29 Data Protection Working Party.[6]
4.	The November 2009 Madrid Resolution of the International Conference of Data Protection and Privacy Commissioners considered PIA as part of a proactive measure of protecting privacy which should be adopted by the states in their privacy legislation.[7]

[1] Linden Consulting Inc, 'Privacy Impact Assessment: International Study of their Application and Effects' (October, 2007) < http://www.rogerclarke.com/DV/ICO_2007_Study.pdf> accessed 16 May 2019.

[2] ICO, 'Privacy Impact Assessment Handbook' (Version 2.0, 2009).

[3] ICO, 'Conducting Privacy Impact Assessments Code of Practice' (February 2014).

[4] ICO, 'Data Protection Impact Assessments (DPIAs)' <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/> accessed 16 May 2019.

[5] Neil Robinson, Hans Graux, Maarten Botterman, and Lorenzo Valeri, 'Review of the European Data Protection Directive' (RAND 2009) 54 <http://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR710.pdf> accessed 16 May 2019.

[6] Commission, 'Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio- frequency identification' OJ L122/47.

[7] International Conference of Data Protection and Privacy Commissioners, 'International Standards on the Protection of Personal Data and Privacy - The Madrid Resolution' (5 November 2009) 22

5.	The European Commission considered the PIA as one of the measures to ensure compliance with data protection law such as in its January 2010 report on new privacy challenges;[8] in July 2010 speech by the European Commission's Vice-President called businesses and public authorities; [9] in the Commission's 2010 communication on a comprehensive approach on personal data protection in the European Union.[10]
6.	The Article 29 Working Party issued some opinions as mandated by the recommendations requiring the RFID and Smart meter DPIA. For the RFID impact assessment template in 2010,[11] and 2011[12] and for the Smart metering DPIA Template in April 2013,[13] and December 2013.[14]
7.	The French CNIL published a 'Methodology for privacy risk management - how to implement the Data Protection Act' in 2012, [15] which was updated in June 2015 in three documents— Privacy Impact Assessment (PIA): Methodology (how to carry out a PIA), Privacy Impact Assessment (PIA): Tools (templates and knowledge bases) and Privacy Impact Assessment (PIA): Good Practices (how to carry out a PIA).[16] A further update has been made to these documents following the GDPR in

<https://icdppc.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf> accessed 16 May 2019.

[8] Commission, 'Comparative Study on Different Approaches to New Privacy Challenges in Particular in the Light of Technological Developments' (Final Report, 20 January 2010).

[9] Viviane Reding, 'Towards a true Single Market of data protection' (Speech delivered on the Meeting of the Article 29 Working Party 'Review of the Data protection legal framework', Brussels, 14 July 2010, 3 <http://europa.eu/rapid/press-release_SPEECH-10-386_en.pdf> accessed 6 June 2019.

[10] Commission, 'Communication from the Commission to the European parliament, the council, the economic and social committee and the committee of the regions: A comprehensive approach on personal data protection in the European Union' COM (2010) 609 final, 12.

[11] WP29, 'Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications' (Adopted on 13 July 2010, WP 175).

[12] WP29, 'Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications (Adopted on 11 February 2011, WP 180).

[13] WP29, 'Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force (Adopted on 22 April 2013, WP 205).

[14] WP29, 'Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force (Adopted 4 December 2013, WP 209).

[15] CNIL, Methodology for privacy risk management - how to implement the Data Protection Act (June 2012) <http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf> accessed 12 May 2019.

[16] CNIL, PIA Methodology (how to carry out a PIA) <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf> accessed 12 May 2019.; PIA Tools (templates and knowledge bases); and PIA Good Practices (June 2015).

	February 2018 and now include four documents: PIA Methodology, Template, Knowledge bases and an example—Application to connected objects.[17] The CNIL has gone further to develop its privacy risk management tool into a software application, which it regularly updates.[18]
8.	The European Commission issued a recommendation on preparations for the roll-out of smart metering systems in 2012, calling on the Member States to ensure that a data protection impact assessment is carried out before deploying smart metering applications in order to ensure that national legislation implementing Directive 95/46/EC is respected.[19] The resulting DPIA template was published in 2014,[20] and updated in September 2018.[21]
9.	From January 2011 to October 2012, a Privacy Impact Assessment Framework for data protection and privacy rights (the PIAF project) was funded by the EU that aimed to encourage the EU and its Member States to adopt a progressive privacy impact assessment policy as a means of addressing needs and challenges related to privacy and the processing of personal data.[22]
10.	The European Commission included DPIA in the proposal for a General Data Protection Regulation[23] as well as the Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in 2012.[24]

[17] CNIL, 'CNIL publishes an update of its PIA Guides' (26 February 2018) <https://www.cnil.fr/en/cnil-publishes-update-its-pia-guides> accessed 12 May 2019.

[18] CNIL, 'The open source PIA software helps to carry out data protection impact assessment' (25 June 2019) <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment> accessed 7 July 2019.

[19] Commission, 'Commission Recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems' (2012/148/EU).

[20] Smart Grid Task Force, 'Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems' <https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf> accessed 12 May 2019.

[21] Smart Grid Task Force, 'Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems' (v.2 of 13 September 2018) <https://ec.europa.eu/energy/sites/ener/files/documents/dpia_for_publication_2018.pdf> accessed 27 August 2019.

[22] PIAF Legacy website < https://piafproject.wordpress.com/> accessed 9 July 2019.

[23] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM (2012) 11 final.

[24] Commission, 'Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes

11.	In 2012, the first European textbook on PIA, which is a compendium of articles from various authors and edited by David Wright and Paul De Hert was published.[25]
12.	The Article 29 Working Party also published a statement on the risk-based approach in 2014 in which DPIA is mentioned.[26]
13.	The Spanish DPA published a guide on Impact Assessment in the Protection of Personal Data in 2014.[27] This guide has been updated in 2018.[28]
14.	The Centre for Information Policy Leadership (CIPL) hosted a series of multinational workshops from 2014 and published four white papers on risk management and its role in data protection.[29]
15.	The Conference of German Independent Data Protection Authorities of the Bund and the Länder (DSK) in November 2016 acknowledged a (English) Trial Version of 'The Standard Data Protection Model' that contains among other things an aspect of privacy risk analysis.[30] This document has been updated in 2018 (version 1.1, in German).[31] Even though this document strictly speaking is not focused on DPIA, but on

of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data' COM (2012) 10 final

[25] David Wright and Paul De Hert (eds), *Privacy Impact Assessment* (Springer, 2012).

[26] Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks', (2014) 14/EN, WP218.

[27] AEPD, GUÍA para una Evaluación de Impacto en la de Protección Datos Personales (2014) http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf

[28] AEPD, 'Guía práctica para las Evaluaciones de Impacto en la Protección de Datos Sujetas al RGPD' (2018) <https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf>.

[29] See CIPL, 'A Risk-based Approach to Privacy: Improving Effectiveness in Practice' (19 January 2014) 1 <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf>; CIPL, 'The Role of Risk Management in Data Protection' (2014), <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_2-the_role_of_risk_management_in_data_protection-c.pdf>; CIPL, 'Protecting Privacy in a World of Big Data – the Role of Risk Management', (discussion draft, February 2016), <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big _data_paper_2_the_role_of_risk_management_16_february_2016.pdf>; CIPL, 'Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR' (2016) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf> accessed 27 February 2019.

[30] 'The StandardData Protection Model A concept for inspection and consultation on the basis of unified protection goals' (V.1.0 – Trial version) <https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methodology_V1_EN1.pdf> accessed 10 July 2019.

[31] Das Standard-Datenschutzmodell Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele (April 2018) <https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V_1_1.pdf> accessed 9 July 2019.

	Privacy by design, it has been referenced by the WP29 concerning DPIA.[32] Later, the DSK published short papers on risk to the rights and freedoms of natural persons in April 2018,[33] and DPIA according to Article 35 GDPR in December 2018. [34]
16.	The Belgian Commissie voor de Bescherming van de Persoonlijke Levenssfeer (CBPL) published a draft recommendation on DPIA and Prior Consultation for public consultation in 2017 [35] and a final document in February 2018.[36]
17.	The Article 29 Working Party released a version of its Guidelines on Data Protection Impact Assessment in April 2017.[37] A revised version was later published in October 2017.[38]
18.	The Bayern Data Protection Authority (Germany) published a short guide on DPIA in June 2017.[39]
19.	The Irish Data Protection Commissioner (DPC) in 2017 explained the obligations under the GDPR, and a section was on DPIA.[40] There is currently a guide on DPIAs published in October 2019.[41]

[32] See WP29 Guidelines on DPIA. See also VALCRI, 'Data Protection Impact Assessments (DPIAs) in the law enforcement sector according to Directive (EU) 2016/680 – A comparative analysis of methodologies' <http://valcri.org/our-content/uploads/2018/06/VALCRI-DPIA-Guidelines-Methodological-Comparison.pdf> accessed 5 July 2019.

[33] DSK, 'Kurzpapier Nr. 18 Risiko für die Rechte und Freiheiten natürlicher Personen' (26 April 2018) <https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf> accessed 18 March 2019.

[34]DSK, 'Kurzpapier Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO' (17 December 2018) <https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf> accessed 18 March 2019.

[35] CBPL, 'Projet de recommandation d'initiative concernant l'analyse d'impact relative à la protection des données et la consultation préalable soumis à la consultation publique (CO-AR-2016-004) <https://www.privacycommission.be/sites/privacycommission/files/documents/CO-AR-2016-004_FR.pdf> accessed 8 July 2019.

[36] CBPL, 'Aanbeveling nr. 01/2018 van 28 februari 2018 met betrekking tot de gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging' CO-AR-2018-001 <https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/aanbeveling_01_2018.pdf> accessed 8 July 2019.

[37] WP29, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (Adopted on 4 April 2017, WP 248).

[38] WP29 'Guidelines on DPIA'.

[39] Bayerisches Landesamt für Datenschutzaufsicht, 'EU-Datenschutz-Grundverordnung (DS-GVO) Das BayLDA auf dem Weg zur Umsetzung der Verordnung (21 March 2017) <https://www.lda.bayern.de/media/baylda_ds-gvo_18_privacy_impact_assessment.pdf> accessed 8 July 2019.

[40] Data Protection Commission, 'Data Protection Impact Assessments' <http://gdprandyou.ie/data-protection-impact-assessments-dpia/> accessed 8 July 2019.

[41]Data Protection Commission, 'Guidance Note: Guide to Data Protection Impact Assessments (DPIAs)'

20.	The GDPR and the LEA Directive provisions requiring DPIA becomes enforceable on 25 May 2018.
21.	The European Data Protection Board, since January 2019, has been publishing opinions geared towards harmonising the 'Blacklist' of data processing that require a DPIA sent to it by Members States' supervisory authorities as well as the 'White' where DPIA is exempt.[42]
22.	The European Data Protection Supervisor in February 2018 published a guide on how to carry out a DPIA under the Regulation (EU) 2018/1725[43]
23.	Table 2 in the main document contains a fuller list of DPIA-related guidance documents for EU supervisory authorities. It complements this table.

(October 2019) <https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Guide%20to%20Data%20Protection%20Impact%20Assessments%20%28DPIAs%29_Oct19_0.pdf> accessed 24 December 2019.

[42] See the EDPB Opinions <https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en> accesses 12 February 2019.

[43] EDPS, 'Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments' (February 2018) <https://edps.europa.eu/sites/edp/files/publication/18-02-06_accountability_on_the_ground_part_1_en.pdf> accessed 11 January 2010.

ANNEX 2: PROVISIONS OF THE GDPR WHERE THE WORD 'RISK' IS MENTIONED

GDPR Provisions	Context
Recital 74	Responsibility and liability of the controller
Recital 75	Examples of harms resulting from data processing
Recital 76	Objective assessment/factors
Recital 77	Guidance on risk assessment
Recital 83	Security of Processing
Recital 84	Consultation with the supervisory authority
Recital 89	Introduces a risk-based approach
Recital 90	Minimum content of a DPIA
Recital 91	Examples of when to carry out a DPIA
Recital 92	Subject matter of DPIA
Recital 93	Assessment before adoption of Member States law
Recital 94	Risk mitigation and consultation of supervisory authority
Recital 95	Processor assistance to the controller
Article 24(1)	Accountability
Article 25(1)	Data protection by design and by default
Article 27(2)(a)	Appointment of rep.
Article 28(4); 32(1) and (2)	Data security
Article 30 (5)	Records of processing activities
Article 33	Data breach notification to the supervisory authority
Article 34(1)	Communication of data breach to the data subject

Article 35	DPIA
Article 36	Prior consultation
Article 39 (2)	DPO functions
Article 70(1)(h)	European Data Protection Board tasks

ANNEX 3: EXAMPLES OF SOFTWARE THAT AUTOMATE IMPACT ASSESSMENT

SN	Tool	Source
1.	Ave point	https://www.avepoint.com/privacy-impact-assessment/ https://www.avepoint.com/news/avepoint-launches-the-latest-release-of-the-avepoint-privacy-impact-assessment-system-with-newly-integrated-microsoft-gdpr-detailed-assessment-at-the-iapp-privacy-security-risk-conference-2017
2.	CNIL	https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment
3.	One Trust	https://www.onetrust.com/products/assessment-automation/
4.	Nymity ExpertPIA	https://www.nymity.com/solutions/expertpia/
5.	Granite	https://granitegrc.com/granite-privacy-impact-assessment/
6.	The CNRFID-CSL Privacy impact Assessment software	http://rfid-pia-en16571.eu/why-use-the-software/how-it-works/ http://rfid-pia-en16571.eu/why-use-the-software/
7.	Privaon Privacy Impact Assessment Tool	https://privaon.com/services/privacy-impact-assessment-tool/ http://privaon.com/wp-content/uploads/2014/10/What-is-a-Privacy-Impact-Assessment-PIA.pdf

BIBLIOGRAPHY

Books and Chapters in Edited Collections

Alnemr R et al., 'A Data Protection Impact Assessment Methodology for Cloud' in Bettina Berendt et al., (eds) *Privacy Technologies and Policy Third Annual Privacy Forum, APF 2015 Luxembourg,* Luxembourg, October 7–8, 2015 Revised Selected Papers (Springer 2016).

Alshamari M and Simpson A, 'Towards an Effective Privacy Impact and Risk Assessment Methodology: Risk Analysis' in Joaquin Garcia-Alfaro et al (eds) *Data Privacy Management, Cryptocurrencies and Blockchain Technology* (ESORICS 2018 International Workshops, DPM 2018 and CBT 2018, Barcelona, Spain, September 6-7, 2018, Proceedings).

Aquinas T, *Summa Theologica* (ST I-II, Q.94, A.II, 1947) <http://www.sacred-texts.com/chr/aquinas/summa/> accessed 11 July 2019.

Aristotle, *Politics: A Treaties on Government* (English version by the Project Gutenberg) <http://www.gutenberg.org/files/6762/6762-h/6762-h.htm> accessed 20 June 2016.

— —'Of Human Law' (ST I-II, Q.95, A.II, 1947) <http://www.sacred-texts.com/chr/aquinas/summa/sum233.htm> accessed 11 July 2019.

Australian Government Department of Health, *Environmental Health Risk Assessment Guidelines for Assessing Human Health Risks From Environmental Hazards*, (Department of Health 2012).

Australian Law Reform Commission, *Regulating Privacy* (2008) <http://www.alrc.gov.au/publications/4.%20Regulating%20Privacy/regulatory-theory> accessed 20 July 2016.

Beck U, *Risk Society: Towards a New Modernity* (Sage Publications 1986)

Bernstein P, *Against the Gods: The Remarkable Story of Risk* (John Wiley and Sons Inc 1996).

Bennett C, *Regulating Privacy Data Protection and Public Policy in Europe and the United States* (Cornell University Press 1992).

Bier C et al., 'Enhancing Privacy by Design from a Developer's Perspective' in Bart Preneel and Demosthenes Ikonomou (eds), *Privacy Technologies and Policy: First Annual Privacy Forum, APF 2012* (Springer Verlag 2014).

Bieker F et al., 'Data Protection Impact Assessment: A Hands-On Tour of the GDPR's Most Practical Tool' in Marit Hansen et al (eds) *Privacy and Identity Management. The Smart Revolution* (Springer 2018).

Bieker F et al., 'A Process for Data Protection Impact Assessment under the European General Data Protection Regulation' in S. Schiffner et al. (eds) APF 2016 LNCS 9857.

Blume P, 'Data Protection and Privacy – Basic Concepts in a Changing World' in Peter Wahlgren (ed), *Information and Communication Technology Legal Issues* (2010) 54 Scandinavian Studies in Law.

Bräutigam T, 'PIA: Cornerstone of Privacy Compliance in Nokia' in David Wright and Paul De Hart (ed) *Privacy Impact Assessment* (Springer 2012).

Brouwer E, *Digital Boarders and Real Rights: Effective Remedies for Third Country Nationals in the Schengen*

Information System (Martinus Nijhoff Publishers 2008)

Bora, 'Risk, Risk Society, Risk Behavior, and Social problems' in G. Ritzer (Ed.), *The Blackwell Encyclopedia of Sociology* (Vol. 8, Blackwell Publishing, 2007).

Cannataci J (ed), *The Individual and Privacy* (Vol. 1, Ashgate Publishing 2015).

Demetzou K, 'GDPR and the Concept of Risk: The Role of Risk, the Scope of Risk and the Technology Involved' in Eleni Kosta et al (eds) *Privacy and Identity Management Fairness, Accountability and Transparency in the Age of Big Data* (Springer 2019).

Douglas M, *Purity and danger: An analysis of the concepts of pollution and taboo* (Routledge 1966).

Dowding M, *Privacy Defending an Illusion* (Scarecrow Press 2011).

Duscha P, 'Audit, Continuous Audit, Monitoring and Revision' in Sowa/Duscha/Schreiber (Eds), *IT-Revision, IT-Audit und IT-Compliance – Neue Ansätze für die IT-Prüfung* (Springer 2015).

Feiler L, Forgó N and Weigl M, *The EU General Data Protection Regulation (GDPR): A Commentary* (Global Law and Business Ltd 2018).

Ferris M, 'The ISO PIA Standard for Financial Services' in David Wright and Paul de Hart (eds) *Privacy Impact Assessment* (Springer 2012).

FRA, *Handbook on European Non-discrimination Law* (FRA 2010).

— —*Handbook on European Data Protection Law* (Publication office of the EU 2014).

— —*Handbook on European Data Protection Law* (2018 edition, Publication office of EU).

Frey R, Mccormick S and Rosa E, 'The Sociology of Risk' in Clifton Bryant and Dennis Peck (ed) *21st Century Sociology: A Reference Handbook* (SAGE Publications 2006).

Freund J and Jones J, *Measuring and Managing Information Risk* (Butterworth-Heinemann 2015).

Fuller L, *The Morality of Law* (Yale University Press 1964).

Gormley A, Pollard S, Rocks S and Black E, *Guidelines for Environmental Risk Assessment and Management Green Leaves III* (Department for Environment, Food and Rural Affairs, UK, 2011).

Hansen M, 'Top 10 Mistakes in System Design from a Privacy Perspective and Privacy Protection Goals' in Jan Camenisch et al. (eds), *Privacy and Identity Management for Life* (Springer 2012).

Hansson O, 'Risk' in Edward Zalta (ed.) *The Stanford Encyclopedia of Philosophy* (Fall 2018 Edition) <https://plato.stanford.edu/archives/fall2018/entries/risk/> accessed 11 July 2019.

Hansson S, 'A Panorama of the Philosophy of Risk' in Sabine Roeser et al (eds.), *Handbook of Risk Theory* (Springer 2012).

Hart P, 'A human rights perspective on privacy and data protection impact assessment' in Wright D and Hert P (eds.) *Privacy Impact Assessment* (Springer Heidelberg 2012).

Heald D, 'Varieties of Transparency' in Christopher Hood and David Heald (eds), *Transparency: The Key to Better Governance?* (British Academy Scholarship, 2006).

Hert P and Gutwirth S, 'Privacy, data protection and law enforcement. Opacity of the individual and

transparency of power' in Erik Claes, Anthony Duff and Serge Gutwirth (eds), *Privacy and the Criminal Law* (Intersentia 2006).

Heun W, 'Risk Management by Government and the Constitution' in Gunnar Duttge, Sang Won Lee (Eds.), *The Law in the Information and Risk Society* (Universitätsverlag Göttingen 2011).

Hondius F, *Emerging Data Protection in Europe* (North-Holland publishing 1975)

Inness J, *Privacy, Intimacy and Isolation* (Oxford University Press 1992).

Killian W, 'Germany' in James Rule and Graham Greenleaf (ed), *Global Privacy Protection the First Generation* (Edward Elgar 2008).

Koops E, 'On Decision Transparency, or How to Enhance Data Protection after the Computational Turn' in Mireille Hildebrandt and Katja de Vries (Eds.), *Privacy, Due Process and the Computational Turn* (Routledge, 2013).

Kuner C, Bygrave L, and Docksey C, *The EU General Data Protection Regulation (GDPR) A Commentary* (Oxford University Press, expected September 2019).

Le Grand G and Barrau E, 'Prior Checking, a Forerunner to Privacy Impact Assessments' in David Wright and Paul De Hert (eds), *Privacy Impact Assessment* (Springer 2012).

Luhmann N, *Risk: A Sociological Theory* (De Gruyter 1993).

— —*Legitimation durch Verfahren* (Willy Fleckhaus und Rolf Staudt 1983).

Makulilo A (ed), *African Data Privacy Laws* (Springer International Publishing 2016).

Marcus A, 'Privacy in Eighteenth-century Aleppo: The Limits of Cultural Ideals' in Joseph Cannataci (ed), *The Individual and Privacy* (Vol 1 Ashgate Publishing 2015).

Makri E, Georgiopoulou Z, and Lambrinoudakis C, 'A Proposed Privacy Impact Assessment Method Using Metrics Based on Organizational Characteristics' in Sokratis Katsikas et al. (eds) *Computer Security*. CyberICPS 2019, SECPRE 2019, SPOSE 2019, ADIoT 2019 (Lecture Notes in Computer Science, vol 11980. Springer 2019).

Mill J, *Principles of Political Economy*, Book V, Chapter XI 2, <http://www.econlib.org/library/Mill/mlP73.html> accessed 23 June 2016.

Moore B, *Privacy Studies in Social and Cultural History* (M.E Sharpe Inc 1984).

Nash J, 'Law and Risk', in James Wright (Ed) *International Encyclopedia of the social and Behavioral Sciences* (2nd Ed, Vol. 13 2015).

National Research Council, *Risk Assessment in the Federal Government: Managing the Process* (The National Academies Press 1983).

Nissenbaum H, *Privacy in Context: Technology, Privacy and the Integrity of Social Life* (Stanford University Press 2010).

Nwankwo I, 'Information Privacy in Nigeria' in Alex Makulilo (ed), *African Data Privacy Laws* (Springer 2016):

Peterson M, *An Introduction to Decision Theory* (Cambridge University Press 2009).

Perri 6, *The future of privacy Volume 1 Private life and public policy* (Demos 1998).

Posner R, *The Economics of Justice* (Harvard University Press 1981).

Renn O, Schweizer P, Müller-Herold U and Stirling A, *Precautionary Risk Appraisal and Management An Orientation for meeting the Precautionary Principle in the European Union* (Europäischer Hochschulverlag 2009).

Rausand M, *Risk Assessment Theory, Methods, and Applications* (John Wiley and Sons 2011).

Rissi J and Sherman S, 'Cloud-Based IT Audit Process' in Ben Halpert (Ed), *Auditing Cloud Computing – A Security and Privacy Guide* (John Wiley & Sons 2011).

Rouvroy A and Poullet Y, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth, et al (ed) *Reinventing Data Protection?* (Springer 2009).

Röhl K and Machura S (eds), *Procedural Justice* (Routledge 2018).

Siebenkäs A and Stelzer D, 'Assessing Theories for Research on Personal Data Transparency' in Eleni Kosta et al. (eds), *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data* (Springer 2019).

Stauch M, 'Data Protection Law' in Paula Giliker (ed), *Research Handbook on EU Tort Law* (Edward Elgar Publishing 2017).

Steele K and Stefánsson O, 'Decision Theory' in Edward Zalta (ed.), *The Stanford Encyclopedia of Philosophy* (Winter 2016 Edition) <https://plato.stanford.edu/archives/win2016/entries/decision-theory/> accessed 16 July 2019.

Talabis M, Martin J and Wheeler E (eds), *Information Security Risk Assessment Toolkit* (Elsevier 2013).

Thoma F, 'How Siemens Assess Privacy Impacts' in David Wright and Paul De Hert (eds), *Privacy Impact Assessment* (Springer 2012).

Taylor R, 'No Privacy without Transparency' in Ronald Leenes et al (eds), *Data Protection and Privacy: The Age of Intelligent Machines* (Hart Publishing 2017).

Tzanou M, *The Fundamental Right to Data Protection* (Hart Publishing 2017).

van Est, Bart Walhout and Frans Brom, 'Risk and Technology Assessment' in Sabine Roeser et al. (eds.), *Handbook of Risk Theory* (Springer 2012).

von Grafenstein M, *The Principle of Purpose Limitation in Data Protection Laws: The Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation* (Nomos Verlagsgesellschaft mbH 2018).

von dem Bussche A and Stamm M, *Data Protection in Germany* (C.H Beck 2012).

Waters N, 'Privacy Impact Assessment – Great Potential Not Often Realised' in David Wright and Paul De Hert (eds), *Privacy Impact Assessment* (Springer 2012).

Wagner I and Boiten E, 'Privacy Risk Assessment: From Art to Science, by Metrics' in Joaquin Garcia-Alfaro et al (eds) *Data Privacy Management, Cryptocurrencies and Blockchain Technology* (ESORICS 2018 International Workshops, DPM 2018 and CBT 2018, Barcelona, Spain, September 6-7, 2018.

Whiteman M and Mattord H, *Principles of Information Security* (5th Edn, Boston, Cengage Learning 2012).

Wilhelmsen C and Ostrom L, *Risk Assessment: Tools, Techniques, and Their Applications* (1st Ed, Wiley 2012).

Wright D et al., 'Precaution and Privacy Impact Assessment as Modes Towards Risk Governance' in R Schomberg (ed) *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (EU 2011).

Wright D and De Hart P (ed), *Privacy Impact Assessment* (Springer 2012).

Zibuschka J, 'Analysis of Automation Potentials in Privacy Impact Assessment Processes' in Sokratis Katsikas et al. (eds), *Computer Security. CyberICPS 2019, SECPRE 2019, SPOSE 2019, ADIoT 2019* (Lecture Notes in Computer Science, vol 11980. Springer 2019).

Journal Articles

Allen A, 'Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm' (2000) Faculty Scholarship Paper 790.

Alsenoy B, 'Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation' (2016) 7 J Intell Prop Info Tech & Elec Com Law 271.

Anđelković L, 'The Elements of Proportionality as a Principle of Human Rights Limitations' (2017) 15:3 Law and Politics 235.

Barocas S and Levy K, 'Privacy Dependencies' (2019) Washington Law Review, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3447384> accessed 12 December 2019.

Barlow S et al. 'Transparency in Risk Assessment – Scientific Aspects Guidance of the Scientific Committee on Transparency in the Scientific Aspects of Risk Assessments carried out by EFSA. Part 2: General Principles' (2009) 1051 *The EFSA Journal* 1.

Banta N, 'Death and Privacy in the Digital Age' (2016) 94 N.C. L. Rev. 927.

Binns R, 'Data Protection Impact Assessments: A Meta-Regulatory Approach' (2017) 7 (1) International Data Privacy Law 22.

Borocz I, 'Risk to the Right to the Protection of Personal Data: An Analysis through the Lenses of Hermagoras' (2016) 2:4 European Data Protection L Rev 467.

Butler D, 'A Tort of Invasion of Privacy in Australia?' [2005] MelbULawRw 11; (2005) 29(2) Melbourne University Law Review 339.

Bygrave L, 'Hardwiring Privacy' University of Oslo Faculty of Law Research Paper No. 2017-02.

— —'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements', (2017) 4:2 Oslo Law Review.

Calo M, 'The Boundaries of Privacy Harm' (2011) Indiana Law Journal 1132.

Clarke R, 'An Evaluation of Privacy Impact Assessment Guidance Documents' (2011) 1:2 International Data Privacy Law.

— —'Privacy Impact Assessment: Its Origins and Development', (2009) 25 CLSR 123.

Costa L, 'Privacy and the Precautionary Principle' (2012) 28 CLSR 14.

Craven J, 'Personhood: the Right to be Let Alone' (1976) Duke Law Journal 699.

Decker C, 'Goals-Based and Rules-Based Approaches to Regulation' (2018) BEIS Research Paper Number 8.

De Villiers M, 'Foreseeability Decoded' (2015) 16:1 Minnesota Journal of Law, Science & Technology, 355.

Diggelmann O and Cleis M, 'How the Right to Privacy Became a Human Right' (2014) 14:3 Human Rights Law Review 441.

Duncan N and Hutchinson T, 'Defining and Describing What We Do: Doctrinal Legal Research' (2102) 17 (1) Deakin Law Review 83.

EFSA 'Transparency in Risk Assessment Carried out by EFSA: Guidance Document on Procedural Aspects' (2006) 353 *The EFSA Journal* 1.

Fried C, 'Privacy' (1968) 77 Yale L.J. 475.

Gavison R, 'Privacy and the Limits of Law' (1980) 89:3 The Yale Law Journal 421.

Gellert R, 'Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative' (2015) 5 IDPL 1.

— —'Understanding the notion of risk in the General Data Protection Regulation' (2018) 34 Computer Law & Security Review 279, 283.

Gellert R and Kloza D, 'Can Privacy Impact Assessment Mitigate Civil Liability? A precautionary approach' 2012 Jusletter IT.

Gerstein R, 'Intimacy and Privacy' (1978) 89:1 Ethics 76.

Giddens A, 'Risk and Responsibility' (1990) 62 (1) The Modern Law Review.

Giliker P, 'A Common Law Tort of Privacy? The Challenges of Developing a Human Rights Tort' (2015) 27 SAcLJ, 761.

Godfrey P, 'Control of Risk. A Guide to the Systematic Management of Risk from Construction' (1996) Construction Industry Research and Information Association Special Publication 125.

Hamidovic H, 'An Introduction to the Privacy Impact Assessment Based on ISO 22307' (2010) 4 ISACA Journal 1.

Harbinja E, 'Post-mortem Privacy 2.0: Theory, Law, and technology' (2017) 31 International Review of Law, Computers & Technology 26.

Hert P and Papakonstantinou V, 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28 Computer Law and Security Review.

Hillson D and Hulett D, 'Assessing Risk Probability: Alternative Approaches' (PMI Global Congress Proceedings – Prague, 2004).

Hondius F, 'A Decade of International Data Protection' (1983) 30 (2) Netherlands International Law Review 103.

Hornung G and Schnabel C, 'Data Protection in Germany I: The Population Census Decision and the Right to Information Self-determination' (2009) 25 Computer Law & Security Report 84.

Hughes K, 'A Behavioural Understanding of Privacy and its Implications for Privacy Law' (2012) 75:5 The Modern Law Review 806.

Jones J, 'An Introduction to Factor Analysis of Information Risk (FAIR)' (2005) Risk Management Insight.

Kaplan S, 'The Words of Risk Analysis' (1997) 17(4) Risk Analysis 407

Kaplan S and Garrick B, 'On the Quantitative Definition of Risk' (1981) 1:1 Risk Analysis.

Kloza D et al., 'Data Protection Impact Assessment in the European Union: Complementing the New Legal Framework Towards a more Robust Protection of Individual' d.pia.lab Policy Brief No.1/2017.

Kloza D et al, 'Towards a Method for Data Protection Impact Assessment: Making Sense of GDPR Requirements' d.pia.lab Policy Brief 1 (2019) 3.

Konvitz M, 'Privacy and the Law: A Philosophical Prelude' (1996) 31 LCP 272.

Koops B et al, 'A typology of Privacy' (2017) 38 University of Pennsylvania Journal of International Law 483.

Kuner C, et al., 'Risk Management in Data Protection' (2015) 5 (2) International Data Privacy Law 96.

Licht J, Naurin D, Esaiasson P and Gilljam M, 'Does transparency generate legitimacy? An experimental study of procedure acceptance of open and closed-door decision-making' (QoG Working Paper Series 2011:8) 3.

Macenaite M, 'The "Riskification" of European Data Protection Law through a two-fold Shift' (2017) 8 European Journal of Risk Regulation.

Markesinis et al, 'Concerns and Ideas about the Developing English Law of Privacy (and How Knowledge of Foreign Law Might be of Help)' (2004) 52:1 The American Journal of Comparative Law 133.

Mendell J and Tanner W, 'Process Is More Important Than Product; Or Throw Out the Plan and Keep the Planner' (1975) 3:16 North American Society for Corporate Planning 3.

Michener G and Bersch K, 'Identifying Transparency' (2013) 18 Information Policy 233.

Mill A, 'A systematic Approach to Risk Management for Construction' (2001) 19 (5) Structural Survey 245.

Moore A, 'Defining Privacy' (2008) 39:3 Journal of Social Philosouphy 411.

Negley G, 'Philosophical Views on the Value of Privacy' (1966) 31 LCP 319.

Oetzel M and Spiekermann S, 'A Systematic Methodology for Privacy Impact Assessments – A Design Science Approach' (2013) 23 EJIS1.

Patterson D, 'Normativity and Objectivity in Law' (2001) 43 Wm. & Mary L. Rev. 325.

Posner R, 'Privacy, Secrecy, and Reputation' (1978) 28 BUFF L REV 1.

Prosser W, 'Privacy' (1960) 48, No. 3 CLR 383.

Quelle C, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach' (2018) 9 European Journal of Risk Regulation 502.

Raab C and Bennett C, 'The Distribution of Privacy Risks: Who Needs Protection?' (1998) 14 The Information Society 263.

Reed C, Kennedy E, and Silva S, 'Responsibility, Autonomy and Accountability: legal liability for machine learning' (2016) Queen Mary University of London, School of Law Legal Studies Research Paper No. 243/2016.

Rubenfeld J, 'The Right to Privacy' (1989) 102 Harv.L.Rev 737.

Sayers et al, 'Risk, Performance and Uncertainty in Flood and Coastal Defence – A Review' (R&D Technical Report FD2302/TR1, 2003).

Schwartz p, 'Internet Privacy and the State', (2000) 32 CONN. L. Rev. 815.

Solove D, 'A Taxonomy of Privacy' (2006) 154:3 University of Pennsylvania Law Review 447.

— —'The Myth of the Privacy Paradox' (2020) GW Legal Studies Research Paper No. 2020-10.

— —'Conceptualizing Privacy' (2002) 90 California Law Review 1088.

Solove D and Citron D, 'Risk and Anxiety A Theory of Data-Breach Harms' (2017) 96 Texas Law Review 737.

Som C, Hilty L and Köhler A, 'The Precautionary Principle as a Framework for a Sustainable Information Society' (2009) 85 JBE 493.

Spina A, 'A Regulatory Marriage de Figaro: Risk Regulation, Data Protection and Data Ethics (2017) 8 European Journal of Risk Regulation.

Stauch M, 'Risk and Remoteness of Damage in Negligence', (2001) 64 (2) MLR 191.

Suryateja P, 'Threats and Vulnerabilities of Cloud Computing: A Review' (2018) 6:3 International Journal of Computer Sciences and Engineering 297.

Tzanou M, 'Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a not so New Right', (201) 3:2 International Data Privacy Law.

US Department of Health, Education and Welfare, 'Records, Computers and the Rights of Citizens' (DHEW Publication No. (OS)73-94, 1973).

van der Sloot B, 'Where is the Harm in a Privacy Violation? Calculating the Damages Afforded in Privacy Cases by the European Court of Human Rights' (2017) 8 JIPITEC 322.

van Beers B, 'The Changing Nature of Law's Natural Person: The Impact of Emerging Technologies on the Legal Concept of the Person' (2017) 18:3 German Law Journal.

Warren S and Brandeis L, 'The Right to Privacy' (1890) IV Harvard Law Review 193.

Westin A, 'Privacy and Freedom' (1968) 25 Wash. & Lee L. Rev. 166.

Wright D and Raab C, 'Privacy Principles, Risks and Harms' (2014) 28 (3) IRLCT 277.

Wright D and Wadhwa K, 'Introducing a privacy impact assessment policy in the EU member states' (2013) 3 (1) International Data Privacy Law 13.

Yang T, 'The Emergence of the Environmental Impact Assessment Duty as a Global Legal Norm and General Principle of Law' (2019) 70 Hasting Law Journal 525.

Online Sources

Alberts C, 'Common Elements of Risk' (Technical Note CMU/SEI-2006-TN-014) <https://resources.sei.cmu.edu/asset_files/TechnicalNote/2006_004_001_14687.pdf> accessed 12 July 2019.

All Answers ltd, 'Breach of Duty Lecture' (Lawteacher.net, December 2019) <https://www.lawteacher.net/modules/tort-law/negligence/breach-of-duty/lecture.php?vref=1> accessed 15 December 2019.

AvePoint PIA, <https://www.avepoint.com/privacy-impact-assessment/> accessed 18 March 2019.

BBC, 'Facebook Staff "Flagged Cambridge Analytica Fears Earlier Than Thought"' (BBC News, 22 March 2019) <https://www.bbc.com/news/technology-47666909> accessed 21 June 2019.

Bitkom, 'Risk Assessment & Data Protection Impact Assessment Guide (Berlin 2017)

<https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2017/Leitfaden/170919-LF-Risk-Assessment-ENG-online-final.pdf> accessed 9 December 2019.

Bonn T, 'Europe's GDPR Outranks Beyonce on Google Search' (2018) <https://www.cnbc.com/2018/05/23/europes-gdpr-outranks-beyonce-on-google-search.html> accessed 4 July 2019.

Bolger P and Kelly J, 'Privacy by Design and by Default' <https://www.lexology.com/library/detail.aspx?g=72cdafaa-9644-453c-b72c-3d55dc5dc29d> accessed 1 August 2019;

Bhargava R, 'The Shifting Data Protection Paradigm: Proactive vs. Reactive' (25 July 2017) <https://devops.com/shifting-data-protection-paradigm-proactive-vs-reactive/> accessed 18 March 2019.

Blackstone W, 'Commentaries on the Laws of England (1765-1769)' <http://lonang.com/library/reference/blackstone-commentaries-law-england/bla-002/> accessed 23 January 2019

Brasseur K, 'Microsoft updates cloud contract privacy amid EDPS probe' *ComplianceWeek* (18 November 2019).

Breach level index, <https://breachlevelindex.com/> accessed 30 October 2019.

Brooks S et al, 'An Introduction to Privacy Engineering and Risk Management in Federal Systems', NISTIR 8062 (2017) <https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf> accessed 9 July 2018

Brooks S and Nadeau E (eds), 'Privacy Risk Management for Federal Information Systems' (NISTIR 8062 (Draft, 2015) <http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf> accessed 18 March 2019.

Business Dictionary, 'Risk' <http://www.businessdictionary.com/definition/risk.html> access 12 July 2019.

Card D, 'The "Black box" Metaphor in Machine Learning' (*Towards Data Science,* 5 July 2017) <https://towardsdatascience.com/the-black-box-metaphor-in-machine-learning-4e57a3a1d2b0> accessed 26 December 2019.

Cambridge Dictionary, 'Transparency' <https://dictionary.cambridge.org/dictionary/english/transparency> accessed 17 December 2019.

Cavoukian A, 'Privacy by Design: The 7 Foundational Principles' <https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf> accessed 18 March 2019.

Chandler S, 'We're giving away more personal data than ever, despite growing risks' (*Venture Beat*, 24 February 2019) <https://venturebeat.com/2019/02/24/were-giving-away-more-personal-data-than-ever-despite-growing-risks/> accessed 28 June 2019:

CIPL, 'A Risk-based Approach to Privacy: Improving Effectiveness in Practice' (2014) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf> accessed 12 June 2019.

— —'The Role of Risk Management in Data Protection' (2014), <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_2-the_role_of_risk_management_in_data_protection-c.pdf> ——

— —'Protecting Privacy in a World of Big Data – the Role of Risk Management', (discussion draft, February 2016), <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_o

f_big _data_paper_2_the_role_of_risk_management_16_february_2016.pdf> accessed 12 June 2019.

— —'Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR' (2016) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf> accessed 27 February 2019.

Clarke R, 'What's Privacy' (Version of 7 August 2006) <http://www.rogerclarke.com/DV/Privacy.html> accessed 12 January 2018.

— —'Introduction to Dataveillance and Information Privacy, and Definitions of Terms' (Version dated 24 July 2016) <http://www.rogerclarke.com/DV/Intro.html> accessed 12 January 2018.

— —'Approaches to Impact Assessment' <http://www.rogerclarke.com/SOS/IA-1401.html> accessed 31 July 2019.

Committee on Foundations of Risk Analysis, 'SRA Glossary' (22 June 2015) <http://www.sra.org/sites/default/files/pdf/SRA-glossary-approved22june2015-x.pdf> accessed 14 July 2019.

Das Standard-Datenschutzmodell Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele (April 2018) <https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V_1_1.pdf> accessed 9 July 2019.

DLA Piper, 'DLA Piper GDPR Data Breach Survey 2020' (2020) <https://www.dlapiper.com/en/uk/insights/publications/2020/01/gdpr-data-breach-survey-2020/> accessed 20 February 2020.

DroneRulesPro, 'Data Protection Impact Assessment Template' <https://dronerules.eu/assets/files/DRPRO_Data_Protection_Impact_Assessment_EN.pdf>.

Dunkelberger D, 'Enterprise Risk Management [Part III]: 5 Examples of Positive Risk (17 July 2018) <https://www.ispartnersllc.com/blog/erm-5-examples-of-positive-risk/> accessed 28 August 2019.

Eagle N 'Who owns the data you generate online?' (*World Economic Forum,* 11 October 2014) <https://www.weforum.org/agenda/2014/10/digital-footprint-data-mining-internet/> accessed 25 June 2019.

EBIOS – Expression des Besoins et Identification des Objectifs de Sécurité (Expression of Needs and Identification of Security Objectives, <http://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/> accessed 23 January 2019.

EDPB, 'First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities' (2019) <https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf> accessed 4 July 2019.

ENISA, <https://www.enisa.europa.eu/> accessed 28 June 2019.

— —'Risk Management / Risk Assessment Standards' <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards> accessed 22 December 2019.

— —'Inventory of Risk Management / Risk Assessment Tools' <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools> accessed 22 December 2019.

— —'Risk Treatment' <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-process/risk-treatment> accessed 18 December 2019.

— —'Guidelines for SMEs on the Security of Personal Data Processing' (27 January 2017).

— —'Risk Assessment' <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-process/risk-assessment/risk-assessment> accessed 16 July 2019.

— —'Cloud Computing: Benefits, Risks and Recommendations for Information Security' (ENISA 2009).

— —'Cloud Security Guide for SMEs' (ENISA 2015).

ERMA, 'Top 4 Regulatory and Litigation Risks in 2018' (*ERMA,* 2018) <https://erm-academy.org/sites/default/files/Top%204%20Regulatory%20and%20Litigation%20Risks%20in%202018.png > accessed 20 February 2019.

EU Cloud CoC, 'About EU Cloud Code of Conduct' <https://eucoc.cloud/en/home.html> accessed 12 January 2020.

European Parliament, 'How Does Ex-ante Impact Assessment Work in the EU?' (February 2015) <http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/528809/EPRS_BRI(2015)528809_EN.pdf> accessed 30 July 2019.

— —'Report' <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BREPORT%2BA7-2013-0402%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN> accessed 18 March 2019.

Family Links Network, 'Code of Conduct for Data Protection Template for Data Protection Impact Assessment (DPIA)' <https://www.icrc.org/en/download/file/18149/dpia-template.pdf> accessed 9 December 2019.

Flaherty D, 'Privacy Impact Assessments: an essential tool for data protection' (A presentation to a plenary session on 'New Technologies, Security and Freedom', at the 22nd Annual Meeting of Privacy and Data Protection Officials held in Venice, September 27-30, 2000) <https://aspe.hhs.gov/legacy-page/privacy-impact-assessments-essential-tool-data-protection-142721> accessed 8 July 2019.

Freude A and Freude T, 'Echoes of History: Understanding German Data Protection' (*Bertelsmann Foundation*, 1 October 2016) <https://www.bfna.org/research/echos-of-history-understanding-german-data-protection/> accessed 12 May 2019.

Fisheries and Oceans Canada, 'Access to Information and Privacy (ATIP) Procedure Manual' (n.d) 52 <http://www.dfo-mpo.gc.ca/Library/277874.pdf> accessed 18 March 2019.

Granite <https://granitegrc.com/granite-privacy-impact-assessment/> access 29 November 2019.

Greenaway K et al., 'Privacy as a Risk Management Challenge for Corporate Practice' <https://www.ryerson.ca/content/dam/tedrogersschool/privacy/privacy_as_a_risk_management_challenge.pdf> accessed 18 December 2019.

Gabel D and Hickman T, 'Chapter 12: Impact Assessments, DPOs and Codes of Conduct – Unlocking the EU General Data Protection Regulation' (*White & Case,* 5 April 2019) <https://www.whitecase.com/publications/article/chapter-12-impact-assessments-dpos-and-codes-conduct-unlocking-eu-general-data> accessed 31 August 2019.

Gjerdrum D, 'A Brief History of ISO 31000 – and Why It Matters' (*Risk and Insurance,* February 9, 2016) <http://riskandinsurance.com/a-brief-history-of-iso-31000-and-why-it-matters/> accessed 12 June 2019.

Hauser J, 'The Evolution of the Concept of Privacy' (EDRi, 25 March 2015) <https://edri.org/evolution-concept-privacy/> accessed 23 June 2016.

Himma K, 'Natural Law' (IEP) <http://www.iep.utm.edu/natlaw/> accessed 13 June 2019.

HIIG, 'Warum Privacy ≠ Datenschutz ist (und wie sie sich überschneiden)' (4 May 2016) <https://www.hiig.de/warum-privacy-%E2%89%A0-datenschutz-ist-und-wie-sie-sich-ueberschneiden/> accessed 12 November 2019.

IAIA, 'What is Impact Assessment' (IAIA, October 2009) <http://www.iaia.org/uploads/pdf/What_is_IA_web.pdf> accessed 29 July 2019.

IGI Global, 'What is Information Society' <https://www.igi-global.com/dictionary/library-science-and-technology-in-a-changing-world/14504> accessed 20 February 2020.

International Conference of Data Protection and Privacy Commissioners, 'Resolution on Privacy by Design' (27-29 October 2010) 2 <https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf> accessed 31 July 2019.

InvestorWords, 'Systematic Approach' <http://www.investorwords.com/19342/systematic_approach.html#ixzz5oEC7p62q> accessed 7 July 2019

ISO <https://www.iso.org/about-us.html> accessed 14 July 2019.

iPHR manual <https://www.iphr.care/apps/procedures/static/Tutorial.pdf> accessed 20 December 2019.

Jones J, 'What about "Positive Risk"? – Part' (30 November 2019) <https://www.fairinstitute.org/blog/what-about-positive-risk-part-1> accessed 28 August 2019.

Jóri A, 'Data Protection Law - An Introduction' <http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.Privacy> accessed 31 July 2019.

Jstor, 'Natural Law' (Jstor) <https://www.jstor.org/topic/natural-law/?refreqid=excelsior%3A9a2f84b2ca3603c2e62e1d04b0873b8a> accessed 28 August 2019.

Koot M, 'Mandatory Privacy Impact Assessments for Dutch Government IT Projects' (*Infosec Island*, 24 October 2013) <http://www.infosecisland.com/blogview/23441-Mandatory-Privacy-Impact-Assessments-for-Dutch-Government-IT-Projects-.html> accessed 7 July 2019.

Lasser R, 'Engineering Method' <https://sites.tufts.edu/eeseniordesignhandbook/2013/engineering-method/> accessed 30 October 2019.

Lee N, Resnick P and Barton G, 'Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms' (Brookings, 22 May 2019) <https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/> access 12 December 2019.

Linden Consulting Inc, 'Privacy Impact Assessment: International Study of their Application and Effects' (October, 2007) <http://www.rogerclarke.com/DV/ICO_2007_Study.pdf> accessed 16 May 2019.

LINDDUN Privacy Threat Modeling Privacy Knowledge (table) <https://7e71aeba-b883-4889-aee9-a3064f8be401.filesusr.com/ugd/cc602e_46135199dc0d49308e76f30a1a657cf7.pdf> accessed 18 December 2019.

LINDDUN Privacy Threat Modeling <https://distrinet.cs.kuleuven.be/software/linddun/linddun.php> accessed 9 December 2019.

Lippman D, 'Microsoft to update Office Pro Plus after Dutch ministry questions privacy' *Politico* (2 February 2019) <https://www.politico.eu/article/microsoft-to-update-office-pro-plus-after-dutch-ministry-questions-privacy/> access 12 January 2020.

Lomas N, 'Facebook Staff Raised Concerns About Cambridge Analytica in September 2015, Per Court Filing' (Techcrunch, 22 March 2019)

Maastricht University, 'Data Protection Officer (DPO) Certification 2019' <https://www.maastrichtuniversity.nl/events/data-protection-officer-dpo-certification-2019> accessed 21 December 2019.

Magee J, 'St. Thomas Aquinas on the Natural Law' (*Acquinasonline,* last updated 5 February 2015) <http://www.aquinasonline.com/Topics/natlaw.html> accessed 17 September 2019.

Multistakeholder Expert Group, 'Contribution from the Multistakeholder Expert Group to the Stock-Taking Exercise of June 2019 on One Year of GDPR Application' (Report, 13 June 2019) <https://ec.europa.eu/commission/sites/beta-political/files/report_from_multistakeholder_expert_group_on_gdpr_application.pdf> accessed 17 September 2019.

National Cancer Institute, 'Cell Phones and the Cancer Risk' <https://www.cancer.gov/about-cancer/causes-prevention/risk/radiation/cell-phones-fact-sheet> accessed 11 July 2019.

Ng, 'A Guide on the Data Lifecycle: Identifying Where Your Data is Vulnerable' (21 August 2018) <https://www.varonis.com/blog/a-guide-on-the-data-lifecycle-identifying-where-your-data-is-vulnerable/> accessed 16 May 2019.

NCSC, 'Risk Management Guidance' <https://www.ncsc.gov.uk/guidance/summary-risk-methods-and-frameworks> accessed 9 July 2019.

NIST, 'Managing Information Security Risk' (NIST Special Publication 800-39, 2011) <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf> accessed 28 June 2019.

— —'Guide for Conducting Risk Assessments' (NIST Special Publication 800-30 Revision 1, 2012) <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf> accessed 28 June 2019.

NIST Computer Security Resource Centre Glossary <https://csrc.nist.gov/glossary/term/vulnerability> accessed 20 September 202.1

Nwankwo I, 'The "Whitelist" and its Value during a Data Protection Impact Assessment' (*DPOBlog*, (25 October 2019) <https://dpoblog.eu/the-whitelist-and-its-value-during-a-data-protection-impact-assessment> accessed 3 December 2019.

Nymity ExpertPIA <https://www.nymity.com/solutions/expertpia/> access 29 November 2019.

OAIC, 'Privacy Impact Assessment Guide' (Revised May 2010) <http://www.icb.org.au/out/?dlid=38156>;

— —'Guide to Undertaking Privacy Impact Assessment' (2014) <https://www.oaic.gov.au/resources/agencies-and-organispations/guides/guide-to-undertaking-privacy-impact-assessments.pdf> accessed 9 July 2018.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980 <https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> accessed 13 May 2019.

O'Mara M, 'The End of Privacy Began in the 1960s' (*New York Times,* 5 December 2018) <https://www.nytimes.com/2018/12/05/opinion/google-facebook-privacy.html> accessed 19 January 2019.

One Trust <https://www.onetrust.com/products/assessment-automation/> accessed 19 January 2019.

Oxford Dictionary 'Netizen' <https://en.oxforddictionaries.com/definition/netizen> accessed 24 February 2017.

Oxford Learner's Dictionaries, 'Terminology' <https://www.oxfordlearnersdictionaries.com/definition/english/terminology?q=terminology> accessed 25 December 2019

PCI Security Standards Council <https://www.pcisecuritystandards.org/> accessed 28 August 2019.

PCI Security Standards Council, Information Supplement. PCI DSS Risk Assessment Guidelines (November 2012) <https://www.pcisecuritystandards.org/documents/PCI_DSS_Risk_Assmt_Guidelines_v1.pdf> accessed 29 August 2019.

PIAF Legacy website <https://piafproject.wordpress.com/> accessed 9 July 2019.

PIAF Deliverable D1: A Privacy Impact Assessment Framework for Data Protection and Privacy Rights (2011) <http://www.piafproject.eu/ref/PIAF_D1_21_Sept_2011.pdf> accessed 23 May 2019.

Privaon Privacy Impact Assessment Tool <https://privaon.com/services/privacy-impact-assessment-tool/> access 29 November 2019.

Pavon, 'PIA Privacy Impact Assessment' (*Pavon,* Whitepaper 15.4.16) <http://privaon.com/wp-content/uploads/2014/10/What-is-a-Privacy-Impact-Assessment-PIA.pdf> accessed 14 December 2019.

PWC, 'General Data Protection Regulation' (2017) <https://www.pwc.com.cy/en/publications/assets/general-data-protection-regulation-why-how-when-january-2017.pdf> accessed 2 September 2019.

Reding V, 'Towards a true Single Market of data protection' (Speech delivered on the Meeting of the Article 29 Working Party 'Review of the Data protection legal framework', Brussels, 14 July 2010, 3 <http://europa.eu/rapid/press-release_SPEECH-10-386_en.pdf> accessed 6 June 2019.

Riffat M, 'Privacy Audit—Methodology and Related Considerations' <https://www.isaca.org/Journal/archives/2014/Volume-1/Pages/Privacy-Audit-Methodology-and-Related-Considerations.aspx> accessed 31 July 2019.

Riskope, 'Glossary of Risk-related Technical Terms' <https://www.riskope.com/wp-content/uploads/2017/08/Glossary-of-risk-related-technical-terms.pdf> accessed 25 December 2019.

Ross, R et. al, 'Developing Cyber Resilient Systems: A Systems Security Engineering Approach', NIST Special Publication 800-160 Volume 2 (NIST 2019) 1 <https://doi.org/10.6028/NIST.SP.800-160v2> accessed 20 September 2021.

Robinson N, Graux H, Botterman M and Valeri L, 'Review of the European Data Protection Directive' (Rand 2009) 2 <http://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR710.pdf> accessed 3 September 2019.

Schwartz P, 'Risk and High Risk: Walking the GDPR Tightrope' (IAPP, 29 March 2016) <https://iapp.org/news/a/risk-and-high-risk-walking-the-gdpr-tightrope/https://iapp.org/news/a/risk-and-

high-risk-walking-the-gdpr-tightrope/> accessed 25 July 2016.

Schmidt C, 'Austria: EUR 800.– in GDPR Compensation for Unlawful Processing of Political Affiliation Data (Hint: It's not Schrems ... yet!)' <https://www.linkedin.com/pulse/austria-eur-800-gdpr-compensation-unlawful-processing-christopher/> accessed 11 November 2019.

Schlehahn E, Marquenie T and Kindt E, 'Data Protection Impact Assessments (DPIAs) in the Law Enforcement Sector According to Directive (EU) 2016/680 – A Comparative Analysis of Methodologies' (*VALCRI* White Paper WP-2017-12) <http://valcri.org/our-content/uploads/2018/06/VALCRI-DPIA-Guidelines-Methodological-Comparison.pdf> accessed 14 December 2019.

Solove D, 'Privacy and Data Security Violations: What's the Harm? <https://teachprivacy.com/privacy-data-security-violations-whats-harm/> accessed 26 August 2019.

Segall L, "Pastor outed on Ashley Madison commits suicide" CNN Business (sept 8 2015) https://money.cnn.com/2015/09/08/technology/ashley-madison-suicide/.

Spacey J, 'What is Legal Risk' (*Simplicable,* 24 August 2015) <https://simplicable.com/new/legal-risk> 16 November 2019.

Treasury Board, 'Directive on Privacy Impact Assessment' (2010) <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308&section=html> accessed 9 July 2018.

The Free Dictionary, 'Foreseeability' <https://legal-dictionary.thefreedictionary.com/Foreseeability> accessed 15 December 2019.

The Law Dictionary, 'What is Systematic Approach' <https://thelawdictionary.org/systematic-approach/> accessed 7 July 2019.

The CNRFID-CSL Privacy impact Assessment software <http://rfid-pia-en16571.eu/why-use-the-software/how-it-works/>_access 29 November 2019.

Tikriti A, 'Foreseeability and Proximate Cause in a Personal Injury Case' (*AllLaw* n.d) <https://www.alllaw.com/articles/nolo/personal-injury/foreseeability-proximate-cause.html> accessed 12 October 2019.

UK National Cyber Security Centre, 'Guidance Summary of Risk Methods and Frameworks' (23 September 2016) <https://webarchive.nationalarchives.gov.uk/20170307014628/> accessed 9 July 2019.

UNEP, 'Guidelines for conducting Integrated Environmental Assessments' (2011) <https://wedocs.unep.org/bitstream/handle/20.500.11822/16775/IEA_Guidelines_Living_Document_v2.pdf?sequence=1&isAllowed=y> accessed 29 June 2019.

United States Consumer Product Safety Commission, 'Carbon-Monoxide-Questions-and-Answers' <https://www.cpsc.gov/Safety-Education/Safety-Education-Centers/Carbon-Monoxide-Information-Center/Carbon-Monoxide-Questions-and-Answers> accessed 14 May 2019.

VALCRI, 'Data Protection Impact Assessments (DPIAs) in the law enforcement sector according to Directive (EU) 2016/680 – A comparative analysis of methodologies' <http://valcri.org/our-content/uploads/2018/06/VALCRI-DPIA-Guidelines-Methodological-Comparison.pdf> accessed 5 July 2019.

Standards

ISO/Guide 73:2009(en) Risk management — Vocabulary (2009).

ISO 22307: 2008 Financial Services – Privacy Impact Assessment (2008).

ISO/IEC 27000 family of Information Security Management Standards.

ISO/IEC 27005:2011 on information security risk management (2011).

ISO/IEC 27005 Information technology – Security Techniques – Information Security Risk Management (3rd edition, 2018).

ISO/IEC 29100:2011 Information technology -- Security Techniques -- Privacy Framework (2011).

ISO 29134:2017: Guidelines for PIA (2017).

ISO 31000 Risk Management – Principles and Guidelines (First edition 2009).

ISO 31000:2018 Risk Management — Guidelines (2018).

ISO /TR 31004: 2013 - Technical Report (2013).

ISO/IEC 31010:2009 - Risk Management - Risk Assessment Techniques (2009).

Other Sources

AEPD, 'GUÍA para una Evaluación de Impacto en la de Protección Datos Personales' (2014) http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf.

— —'Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD' (2018) ('AEDP Guide on DPIA').

— —'Guia Práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD' (2018) ('Practical Guide on Risk Analysis').

— —'Indicative List of the Types of Data Processing that Do Not Require A Data Protection Impact Assessment Under Art 35.5 GDPR' <https://www.aepd.es/media/guias/ListaDPIA-35-5-Ingles.pdf> accessed 30 January 2020.

Australian Law of Negligence Review Panel, 'Review of the Law of Negligence: Final Report' (October 2002)101-119, <https://treasury.gov.au/review/review-of-the-law-of-negligence> accessed 15 December 2019.

Bayerisches Landesamt für Datenschutzaufsicht, 'Musterbeispiel „Insight AG – Kfz-Telematik-Versicherungstarif" Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO in Anlehnung an die ISO/IEC 29134' (DSFA-Bericht zum Fallbeispiel des Workshops 19.07.2017) <https://www.lda.bayern.de/media/03_dsfa_fallbeispiel_bayIda_iso29134.pdf> accessed 30 January 2020.

— —'EU-Datenschutz-Grundverordnung (DS-GVO) Das BayLDA auf dem Weg zur Umsetzung der Verordnung (21 March 2017) <https://www.lda.bayern.de/media/baylda_ds-gvo_18_privacy_impact_assessment.pdf> accessed 8 July 2019.

BSI, 'Technical Guidelines RFID as Templates for the PIA-Framework' <bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03126/TG_RFID_Templates_for_PIA_Framework_pdf.pdf?__blob=publicationFile&v=1> accessed 12 January 2020.

CBPL, 'Projet de recommandation d'initiative concernant l'analyse d'impact relative à la protection des données et la consultation préalable soumis à la consultation publique (CO-AR-2016-004) <https://www.privacycommission.be/sites/privacycommission/files/documents/CO-AR-2016-004_FR.pdf> accessed 8 July 2019.

— —'Aanbeveling nr. 01/2018 van 28 februari 2018 met betrekking tot de

gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging' CO-AR-2018-001 <https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/aanbeveling_01_2018.pdf> accessed 8 July 2019.

CNIL PIA Methodology (last updated in February 2018).

— —'Privacy Impact Assessment (PIA) Knowledge Bases' (February 2018) <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf> accessed 27 February 2019.

— —'Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données n'est pas requise' <https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-non-requise.pdf> accessed 30 January 2020.

— —'Methodology for privacy risk management - how to implement the Data Protection Act' (June 2012) <http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf> accessed 12 May 2019

— —'The PIA Software 2.0 Available and Growth of the PIA Ecosystem' (06 December 2018) <https://www.cnil.fr/en/pia-software-20-available-and-growth-pia-ecosystem> accessed 14 December 2019.

— —'The Open Source PIA Software Helps to Carry Out Data Protection Impact Assessment' (25 June 2019) <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment> accessed 14 December 2019.

— —'PIA Measures for the Privacy Risk Treatment Good Practice' June 2015.

— —'PIA Tools (templates and knowledge bases)' June 2015.

— —'Guide Du Correspondant Informatique Et Libertes' (2011 edition) <https://www.cnil.fr/sites/default/files/typo/document/CNIL_Guide_correspondants.pdf> accessed 21 December 2019.

— —PIA Methodology (how to carry out a PIA) (2015) <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf> accessed 12 May 2019.

CNPD, 'Guide De Préparation Au Nouveau Règlement Général Sur La Protection Des Données' <https://cnpd.public.lu/fr/dossiers-thematiques/Reglement-general-sur-la-protection-des-donnees/responsabilite-accrue-des-responsables-du-traitement/guide-preparation-rgpd.html> accessed 18 March 2019.

Council of Europe, 'Guide on Article 8 of the European Convention on Human Rights – Right to respect for private and family life' (Last updated 31 August 2019) <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf > accessed 20 February 2020.

Datatilsynet, 'Vurdering av personvernkonsekvenser (DPIA)' <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/?id=10361> accessed 2 January 2020.

— —'Varsel om vedtak om overtredelsesgabyr Rælingen kommune' (19/01478-6/KBK, 26 February 2020).

Department of Homeland Security, 'Risk Steering Committee DHS Risk Lexicon' (September 2008) <https://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf> accessed 15 January 2020.

Data Protection Commission, 'Guidance Note: Guide to Data Protection Impact Assessments (DPIAs)' (October 2019) <https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Guide%20to%20Data%20Protection%20Impact%20Assessments%20%28DPIAs%29_Oct19_0.pdf> accessed 24 December 2019.

— —'Data Protection Impact Assessments' <http://gdprandyou.ie/data-protection-impact-assessments-dpia/> accessed 8 July 2019.

— —'List of Types of Data Processing Operations which require a Data Protection Impact Assessment' <https://dataprotection.ie/sites/default/files/uploads/2018-11/Data-Protection-Impact-Assessment.pdf> accessed 12 January 2018.

DigitalEurope, 'DigitalEurope Comments on the Risk-based Approach' (28 August 2013) <https://teknologiateollisuus.fi/sites/default/files/file_attachments/elinkeinopolitiikka_digitalisaatio_tietosuoja_digitaleurope_risk_based_approach.pdf> accessed 12 December 2019.

DSK, 'Kurzpapier Nr. 18 Risiko für die Rechte und Freiheiten natürlicher Personen' (26 April 2018) <https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf> accessed 18 March 2019.

— —, 'Kurzpapier Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO' (17 December 2018) <https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf> accessed 12 December 2019.

EDPB, 'Opinions' <https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en> accessed 24 December 2019.

— —'Opinion 11/2018 on the draft list of the competent supervisory authority of Ireland regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)' (adopted 25 September 2018) <https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion_2018_art._64_ie_sas_dpia_list_en.pdf> accessed 12 December 2019.

— —'Opinion 11/2019 on the draft list of the competent supervisory authority of the Czech Republic regarding the processing operations exempt from the requirement of a data protection impact assessment (Article 35(5) GDPR)' (*EDBP* 12 July 2019) <https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-112019-draft-list-competent-supervisory_en> accessed 30 January 2020.

— —'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (Adopted on 13 November 2019)

— —'Press release: Third Plenary session: EU-Japan draft adequacy decision, DPIA lists, territorial scope and e-evidence' 26 September 2019 <https://edpb.europa.eu/news/news/2018/press-release-third-plenary-session-eu-japan-draft-adequacy-decision-dpia-lists_en> accessed 6 March 2019.

English translation of Decisions of the Federal Constitutional Court (Entscheidungen des Bundesverfassungsgerichts – BVerfGE 65) by German Konrad-Adenauer-Stiftung (Hanover 2013) <https://freiheitsfoo.de/files/2013/10/Census-Act.pdf> accessed 15 June 2019

European Commission, 'Proposal for an ePrivacy Regulation' <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation> accessed 23 November 2019.

— —'Data Protection Impact Assessment for Smart Grid and Smart Metering Environment' <https://ec.europa.eu/energy/topics/markets-and-consumers/smart-grids-and-meters/smart-grids-task-force/data-protection-impact-assessment-smart-grid-and-smart-metering-environment_en> accessed 12 January 2020.

— —'A comprehensive approach on personal data protection in the European Union' COM (2010) 609 final.

— —‘Comparative Study on Different Approaches to New Privacy Challenges in Particular in the Light of Technological Developments’ (Final Report, 20 January 2010).

EDPS, ‘Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation’ (February 2018).

— —‘Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments’ (February 2018) <https://edps.europa.eu/sites/edp/files/publication/18-02-06_accountability_on_the_ground_part_1_en.pdf> accessed 11 January 2010.

— —‘Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit’ (11 April 2017).

— —‘Necessity and Proportionality’ <https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en> accessed 4 August 2019.

— —‘EDPS investigation into IT contracts: stronger cooperation to better protect rights of all individuals’ <https://edps.europa.eu/press-publications/press-news/press-releases/2019/edps-investigation-it-contracts-stronger_en> accessed 4 December 2019.

— —‘EDPS Opinion on Privacy in the Digital Age: "Privacy by Design" as A Key Tool to Ensure Citizens' Trust in ICTs’, <https://edps.europa.eu/press-publications/press-news/press-releases/2010/edps-opinion-privacy-digital-age-privacy-design_en> accessed 4 December 2019.

— —‘Opinion 5/2018 Preliminary Opinion on Privacy by Design’ (31 May 2018).

— —‘EDPS Survey on Data Protection Impact Assessments under Article 39 of the Regulation (case 2020-0066)’, <https://edps.europa.eu/sites/default/files/publication/20-07-06_edps_dpias_survey_en.pdf> accessed 12 September 2021

Finnish Office of the Data Protection Ombudsman, ‘Risk assessment and data protection planning’ <https://tietosuoja.fi/en/risk-assessment-and-data-protection-planning> accessed 2 January 2020.

GDPRhub, ‘Datatilsynet - 19/01478-6’ (GDPRhub, last updated 11 March 2020) <https://gdprhub.eu/index.php?title=Datatilsynet_-_19/01478-6> accessed 28 March 2020.

— —‘CE - N° 434376’ (GDPRhub, last updated 17 January 2020) <https://gdprhub.eu/index.php?title=CE_-_N%C2%B0_434376> accessed 28 March 2020.

— —‘Rb. Den Haag - C/09/550982/HA ZA 18/388’ <https://gdprhub.eu/index.php?title=Rb._Den_Haag_-_C/09/550982/HA_ZA_18/388> accessed 28 March 2020.

ICO, PIA Handbook in 2007 (version 1.0, December 2007), which was revised in 2009 ‘Privacy Impact Assessment Handbook’ (Version 2.0, 2009).

— —‘Conducting Privacy Impact Assessment Code of Practice’ (Version 1.0, 2014).

— —‘Sample DPIA Template’ <https://ico.org.uk/media/2553993/dpia-template.docx> accessed 23 March 2019.

— —‘Guide to the General Data Protection Regulation - Data Protection Impact Assessment’ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/> accessed 16 December 2019.

— —‘How do we a DPIA?’ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/> accessed 12 December 2019.

— —‘Data Protection Act 1998 Monetary Penalty Notice Dated 14 January 2013’.

— —‘Security’ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/> accessed 12 December 2019.

— —‘What’s new under the GDPR?’ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-s-new-under-the-gdpr/#whatsnew1> accessed 31 July 2019.

— —‘ICO Data Protection Audit Manual’ (Version 1, June 2001) <https://www.cmpe.boun.edu.tr/~ozturan/etm555/dataaudit/html/download/pdf/audit_all.pdf> accessed 12 December 2019.

IAPP Certification <https://iapp.org/certify/cippe-cipm/> accessed 25 December 2019.

IDPC, ‘DPIA Template’ <https://idpc.org.mt/en/Documents/Guidelines%20on%20DPIA%20template.pdf> accessed 25 December 2019.

Irish Computer Society, ‘European Certified Data Protection Officer Programme’ <https://www.ics.ie/training/european-certified-data-protection-officer-programme-1> accessed 25 December 2019.

Joyee De and Le Métayer M, ‘PRIAM: A Privacy Risk Analysis Methodology (Research Report n° 8876 — version 1.0 2016).

Korff D and Georges M, ‘The DPO Handbook: Guidance for Data Protection Officers in the Public and Quasi-Public Sectors on How to Ensure Compliance with the European Union General Data Protection Regulation’ (As approved by the Commission, July 2019)184 <https://www.garanteprivacy.it/documents/10160/0/T4DATA-The+DPO+Handbook.pdf> accessed 2 January 2020.

Maldoff G, ‘The Risk-Based Approach in the GDPR: Interpretation and Implications’ (IAPP, March 2016).

Ministerie van Justitie en Veiligheid, ‘DPIA Windows 10 Enterprise v.1809 and preview v. 1903’ (Version 1.5, 11 June 2019).

Ministry of Justice and Security Strategic Vendor Management Microsoft (SLM Rijk), ‘DPIA Office 365 ProPlus version 1905 (June 2019) Data protection impact assessment on the processing of diagnostic data’ (Version 1, 22 July 2019).

Office of the Commissioner for Data Protection Cyprus, ‘Data Protection Impact Assessment’ <http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page2c_en/page2c_en?opendocument#> accessed 13 December 2019.

Office of the Data Protection Ombudsman (Finland), ‘Carrying out an Impact Assessment’ <https://tietosuoja.fi/en/carrying-out-an-impact-assessment> accessed 13 December 2019.

ONF, ‘Threat Analysis for the SDN Architecture’ (Version 1.0, July 2016) <https://www.opennetworking.org/wp-content/uploads/2014/10/Threat_Analysis_for_the_SDN_Architecture.pdf> accessed 21 December 2019.

Privacy Company, ‘DPIA Diagnostic Data in Microsoft Office Proplus’ (5 November 2018).

Penfrat J, 'Microsoft Office 365 banned from German schools over privacy concerns' *Edri* (17 July 2019).

Pompon R, 'IT Security Risk Control Management: An Audit Preparation Plan' (Apress, 2016).

RRC, *IOSH Managing Safely (*3rd ed, Autumn 2018) Module 4.

Rijksoverheid, 'Data protection impact assessments DPIA's Office 365 ProPlus, Windows 10 Enterprise, Office 365 online and mobile apps' <https://www.rijksoverheid.nl/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise> access 8 January 2020.

SDM, 'The Standard Data Protection Model. A concept for inspection and consultation on the basis of unified protection goals' (V.1.0 – Trial version November 2016) <https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V1.0.pdf> access 8 January 2020.

Smart Grid Task Force, 'Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems' (v.2 of 13 September 2018) <https://ec.europa.eu/energy/sites/ener/files/documents/dpia_for_publication_2018.pdf> accessed 27 August 2019.

Smart Grid Task Force, 'Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems' (2014) <https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf> accessed 12 May 2019.

Sun T, 'CYBER 503x Cybersecurity Risk Management Unit 5: Security Metrics' (Lecture Notes September 2021).

Tancock D, Pearson S, and Charlesworth A, 'The Emergence of Privacy Impact Assessments' HP Laboratories HPL-2010-63 <http://www.hpl.hp.com/techreports/2010/HPL-2010-63.pdf> accessed 12 August 2015.

WP29, 'Statement on the Role of a Risk-based Approach in Data Protection Legal Frameworks' (WP 218, 30 May 2014).

— —'Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications' [WP 175].

— —'Guidelines on the Application and Setting of Administrative Fines for the Purpose of the Regulation 2016/679' (adopted 3 October 2017) WP 253.

— —'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "likely to Result in a High risk" for the Purposes of Regulation 2016/679' (Adopted on 4 October 2017).

— —'Guidelines on Personal Data Breach Notification under Regulation 2016/679' (adopted 6 February 2018) WP250rev.01.

— —'The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal' (adopted 1 December 2009, WP 168).

— —'Guidelines on Transparency under Regulation 2016/679' (Adopted on 11 April 2018).

— —'Opinion 03/2013 on Purpose Limitation' (adopted 2 April 2013) WP 203 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> accessed 12 December 2019

— —‘Guidelines on Data Protection Officers (‘DPOs’)’ (Adopted on 13 December 2016) WP 243 <http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf> accessed 31 August 2019.

— —‘Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems (‘DPIA Template’) prepared by Expert Group 2 of the Commission’s Smart Grid Task Force’ (2013) 00678/13/EN WP205

— —‘Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications (Adopted on 11 February 2011, WP 180).

Vrije Universiteit Brussel’s Laboratory for Data Protection and Privacy Impact Assessments (d.pia.lab) <http://www.dpialab.org/> accessed 13 January 2020.

Weiss M and Archick K, ‘U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield’ (Congressional Research Services 2016).

RESUME

Iheanyi Samuel Nwankwo

iheanyi.nwankwo@gmail.com

WORK EXPERIENCE

01/2012 – Current – Hannover

RESEARCH ASSOCIATE – LEIBNIZ UNIVERSITÄT

*Research and execution of EU-funded projects for the Institute for Legal Informatics, Faculty of Law, Leibniz Universität Hannover, including:

- **OPTIMIS** (focusing on cloud computing)
- **p-Medicine** and **CHIC** (focusing on medical research and ethics)
- **CARISMAND** (focusing on disaster management)
- **SPEAR** and **SDN-microSENSE** (focusing on information security in smart energy grids)
- **MAPPING** (focusing on internet governance)
- **EVIDENCE** (focusing legal aspects of evidence)
- **CITYCOP** (focusing on community policing)
- **iBorderCTRL** (focusing border control and management).

*Part-time teaching for LL.B class

- **Introduction to European IT Law**

04/2010 – 08/2010 – Lagos

LEGAL PRACTICE – C.E. NDULUE AND ASSOCIATES

03/2009 – 08/2010 – Lagos

LEGAL/ADMINISTRATIVE OFFICER – CVL TECHNOLOGY LIMITED

03/2001 – 03/2002 – Aba, Nigeria

WAREHOUSE CLARK – UNILEVER NIGERIA PLC

EDUCATION AND TRAINING

2013 – 2021

PHD – Leibniz Universität Hannover

2010 – 2011

MASTER OF LAWS (IP AND IT LAW) – Lebniz Universität Hannover

2007 – 2008

BARRISTER AT LAW (BL) – Nigerian Law School

2002 – 2007

BACHELOR OF LAWS (LL.B) – University of Nigeria, Nsukka

PUBLICATIONS

Book Chapters

- Nwankwo, I. "The "Whitelist" and its VAlue during a Data Protection Impact Assessment" in Kahler, T (ed.) Turning Point in Data Protection Law (Nomos, 2020)
- Nwankwo, I., Wendt, K., & Mifsud Bonnici, J. "Addressing Cultural Rights in Disaster Management: A Checklist for Disaster Managers" in G. Bartolini, D. Cubie, M. Hesselman & J. Peel (eds.), Yearbook of International Disaster Law (Volume 1, Brill, 2018).
- Al-Sharieh, S., Forgó, N., Mifsud Bonnici, J., Nwankwo, I. & Wendt, K. "Securing the Person and Protecting the Data: The Requirement and Implementation of Privacy by Design in Law Enforcement ICT Systems" in J. P. Mifsud Bonnici & J. Cannataci (eds.) Changing Communities, Changing Policing (Neuen Wissenschaftlichen Verlag, 2018).
- Nwankwo, I. "Information Privacy in Nigeria" in Alex Makulilo (ed), African Data Privacy Laws (Springer 2016).

Journals and conferences

- Hänold, S., Forgó, N., Kobeissi, D., and Nwankwo, I. "Legal Perspectives on Post-mortem Use of Biomaterial and Data for Research: A Focus on the German Situation", 24(3) (2017) European Journal of Health Law [https://doi.org/10.1163/15718093-12341415].
- Nwankwo, I. "Missing Links in the Proposed EU Data Protection Regulation and Cloud Computing Scenarios: A Brief Overview" 5 (2014) JIPITEC 32 [http://www.jipitec.eu/issues/jipitec-5-1-2014/3905/jipitec_5_1_nwanko.pdf].
- Weiler1, G., Schröder, C., Schera1, F., Dobkowicz, M., Kiefer, S., Karsten, R. H., Hänold, S., Nwankwo, I., Forgó, I., Stanulla, M., Eckert, C., and Graf, N. "p-BioSPRE - an information and communication technology framework for transnational biomaterial sharing and access", 2014 ecancer 8 401 [DOI: 10.3332/ecancer.2014.401].
- Jefferys, B., Nwankwo, I., Neri, E., Chang, D., Shamardin, L., Hänold, S., Graf, N., Forgó N., and Coveney, P. "Navigating Legal Constraints in Clinical Data Warehousing: A Case Study in Personalized Medicine", 2013 Interface Focus 3: 20120088 [http://dx.doi.org/10.1098/rsfs.2012.0088].
- Kirkham, T., Armstrong, D., Djemame, K., Corrales, M., Kiran, M., Nwankwo, I., Jiang, M., Forgó, N. "Assuring Data Privacy in Cloud Transformations", TRUSTCOM, 2012, [doi:10.1109/TrustCom.2012.97].
- Nwankwo, I., Hänold, S., and Forgó, N. "Legal and Ethical Issues in Integrating and Sharing Databases for Translational Medical Research within the EU", BIBE, 2012, 13th IEEE International Conference on BioInformatics and BioEngineering 428 – 433 [10.1109/BIBE.2012.6399764].
- Djemame, K., Barnitzke, B., Corrales, M., Kiran, M., Jiang, M., Armstrong, D. Forgó, N., and Nwankwo, I. "Legal Issues in Clouds: Towards a Risk Inventory", Philos Trans A Math Phys Eng Sci. 2012 Dec 10;371(1983):20120075 [doi: 10.1098/rsta.2012.0075].
- Nwankwo, I. "Proposed WIPO Treaty for Improved Access for Blind, Visually Impaired, and Other Reading Disabled Persons and Its Compatibility with TRIPS Three-Step Test and EU Copyright Law" 2 (2011) JIPITEC 203 [http://www.jipitec.eu/issues/jipitec-2-3-2011/3175/nwankwo.pdf].
- Nwankwo, I. "Informed Consent of a Patient and the Dilemma of the Medical Practitioner" The Barrister, Journal of Law Students Association, University of Nigeria, 2006.

Theses

- Nwankwo, I. "Towards a Transparent and Systematic Approach to Conducting Risk Assessment under Article 35 of the GDPR" (PhD Thesis 2021).
- Nwankwo, I. "Measures Against Attacks on Information Systems: An Analysis of the European and African Unions' Legal Frameworks" (LL.M Thesis, 2011).
- Nwankwo, I. "International Law and the Renewed Global War on International Terrorism: September 11, 2001 Terrorist Attacks in Perspective" (LL.B Thesis, 2007).

Lectures and Presentations

- Nwankwo, I. "European IT Law: A Focus on European Data Protection, Information Security, and IP Law", Series of lectures presented to LL.B class (Summer Semesters 2018, 2019; 2020; 2021), Leibniz Universität Hannover.
- Nwankwo, I. "Conducting a DPIA under the GDPR", INSITU Summer School, Leibniz Universität Hannover, 2019.
- Nwankwo, I. "Managing personal data risks & conducting a DPIA under the GDPR", INSITU Summer School, Leibniz Universität Hannover, 2017.

- Nwankwo, I. "Electrifying the Fence: Finding the Interface between IT and IP Law", IP Workshop, Faculty of Law, University of Nigeria, Enugu Campus, 26 Nov. 2015.
- Nwankwo, I. "Privacy and Health Information Technology: Reflecting Legal Requirements in Technical Solutions", The Erasmus Observatory on Health Law Summer School on Health Law and Ethics, Rotterdam, the Netherlands, 7 July 2015.
- Nwankwo, I. "Legal and Ethical Aspects of In Silico-based Medicine", 6th International Advanced Research Workshop on In Silico Oncology and Cancer Investigation – the CHIC Project Workshop, Athens, Greece, 3-4 Nov. 2014.
- Nwankwo, I. & Neri, E. "Providing a Network of Trust in Processing Health Data for Research", 23RD EICAR Annual Conference, Frankfurt Germany, 17-18 Nov. 2014.
- Nwankwo, I. "Legal Aspects of Information Security", INSITU Summer School, Leibniz Universität Hannover, 2014.
- Nwankwo, I. "The Proposed Data Protection Regulation and International Data Transfer in Cloud Transformations: A Kaleidoscopic View", 6th International Conference on Computers, Privacy and Data Protection, Brussels, 23-25 January 2013.
- Nwankwo, I. "Internet Governance in Africa", EUROSSIG Summer School Meissen, 4-10 August 2013.