Data protection impact assessment methods for the urban environment

Dalla Corte, Lorenzo; van Brakel, Rosamunde

Publication date:
2022

Document Version
Publisher's PDF, also known as Version of record

Link to publication in Tilburg University Research Portal

Citation for published version (APA):
Dalla Corte, L., & van Brakel, R. (2022). *Data protection impact assessment methods for the urban environment: A report for the Commissie Persoonsgegevens Amsterdam (CPA)*.

DATA PROTECTION IMPACT ASSESSMENT METHODS FOR THE URBAN ENVIRONMENT

A report for the Commissie Persoonsgegevens Amsterdam (CPA)

22.08.2022

Dr. Lorenzo Dalla Corte

Dr. Rosamunde van Brakel

Tilburg Institute for Law, Technology and Society (TILT)

TABLE OF CONTENTS

1. Introduction

Data Protection Impact Assessments (DPIAs) can be defined as the assessment of the impact on personal data protection of types of processing which, considering their nature, scope, context, and purposes, are likely to result in a high risk[1] to the rights and freedoms of natural persons.[2] DPIAs contribute to the General Data Protection Regulation (GDPR)'s objective of ensuring a high level of protection of the fundamental rights and freedoms of individuals (in particular their right to personal data protection) by functioning as both an *ex post* accountability measure, to be considered when demonstrating compliance with the GDPR,[3] and as an *ex ante* regulatory mechanism that compels data controllers to identify and address the risks that may derive from the processing operations they envisage, and the impact that those risks could have on natural persons.[4]

Yet, the performance and practice of DPIAs has raised several issues. The minimum requirements set for DPIAs by the GDPR are framed generally and broadly, which results in assessments that are often arbitrary and whose content and quality vary widely on a case-by-case basis – an issue that is not entirely mitigated, but sometimes even compounded, by the abundance of DPIA methodologies and templates available for controllers to choose from. Performing a DPIA is also not an easy task in itself: recognising risks in general, defining what is "a risk to a right"[5] in particular, and identifying the impact that such risks might have on natural persons, constitute significant conceptual hurdles. Likewise, some types of processing are inherently complex, and their assessment often requires a multidisciplinary approach or expertise by the assessor. Organisational issues, such as the inability to allocate adequate resources to the assessment, or the use of inadequate or inconsistent methodologies and templates, may also impact the performance of a DPIA, and thus its chances of achieving its goal as an accountability measure and as a regulatory mechanism. Finally, a problem already highlighted before the implementation of the GDPR is that DPIAs are often limited to just a compliance check. Beyond compliance checks with legal regulations, one must also consider more qualitative requirements that have to do with legality, legitimacy, participation and, especially, proportionality.[6]

Contemporary urbanities –smart cities– are a prime example of a context where the DPIA process can be particularly challenging, on account of the broad array of types of processing performed, the complexity intrinsic to many of them, and the varied range of rights and freedoms that can be

[1] "A "risk" is a scenario describing an event and its consequences, estimated in terms of severity and likelihood" – Article 29 Data Protection Working Party, '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' (2017) 6.

[2] GDPR, Art. 35. The Article 29 defines DPIAs as "A DPIA is 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" – Article 29 Data Protection Working Party, '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' (n 1) 4. See also Raphael Gellert, 'The Article 29 Working Party's Provisional Guidelines on Data Protection Impact Assessment' (2017) 3 European Data Protection Law Review (EDPL) 212.

[3] See GDPR, Recital 84: "The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation".

[4] Eleni Kosta, 'Article 35 Data Protection Impact Assessment' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): a commentary* (Oxford University Press 2020) 668.

[5] See Niels van Dijk, Raphaël Gellert and Kjetil Rommetveit, 'A Risk to a Right? Beyond Data Protection Risk Assessments' (2016) 32 Computer Law & Security Review 286; István Böröcz, 'Risk to the Right to the Protection of Personal Data: An Analysis Through the Lenses of Hermagoras' (2016) 2 European Data Protection Law Review 467. See also Raphaël Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34 Computer Law & Security Review 279; Raphaël Gellert, 'Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative' (2015) 5 International Data Privacy Law.

[6] Paul De Hert, 'A Human Rights Perspective on Privacy and Data Protection Impact Assessments' in Paul De Hert and David Wright (eds), *Privacy Impact Assessment* (Springer 2012) 38.

compressed by personal data processing in the urban environment.[7] The rampant digitalisation of modern cities, the ever-growing entwinement between code and space,[8] and the development of cyber-physical systems[9] and of the Internet of Things (IoT),[10] are also factors that are bound to increase the complexity of the DPIA process, and the resources it requires.[11] Complexity is further increased by the smart city's multi-actor environment, where diverging and dynamic interests of stakeholders[12] meet, and by the frequent repurposing and sharing of personal data, through increased connection, exchange, and continuous flows of information.[13]

The objective of this study is thus to provide a narrative inventory of existing DPIA methodologies, templates, and best practices currently available that might be used by the municipality of Amsterdam to improve its DPIA process and output. The report is structured as follows: after this brief introduction, section 2 discusses the methodology followed, and its limitations. Section 3 provides the background of DPIAs in the GDPR, and Section 4 reviews and discusses the state of the art of DPIA guidance documents, methodologies, and templates. In Section 5, the report outlines the best practices identified during the desk research, and in Section 6 it summarises the results of the empirical part. Section 7 deals with three questions raised by the Amsterdam Privacy Commission in light of the state of the art in DPIAs as it emerged from this research, namely the suitability of the DPIA template used by the City of Amsterdam, the prospect of pairing DPIAs and neighbouring kinds of assessments, and the possibility of developing sector-specific DPIA guidelines vis-à-vis generic, "all-purpose" ones. Finally, section 8 concludes the report.

2. Methodology and limitations

The methodology that has been used consisted of two phases. In the first phase we conducted desk research, document analysis vis-à-vis publicly available DPIA reports, and an extensive literature review including both academic publications (books, journal articles, working papers, policy briefs) and official policy documents. We queried major literature databases and search engines using search strings of increasing specificity[14] and, where necessary, in different languages. The second phase consisted of a survey, sent to data protection officers of municipalities in 13 countries,[15] and of a set of seven follow-up interviews with the same group of experts, which we used to triangulate our findings with the aim of ascertaining whether there were DPIA methodologies, templates, or best practices that did not result from our documental review.

[7] See e.g. Kelsey Finch and Omer Tene, 'Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town' (2013) 41 Fordham Urb. LJ 1581; Liesbet van Zoonen, 'Privacy Concerns in Smart Cities' (2016) 33 Government Information Quarterly; Lilian Edwards, 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective' (2016) 2 European Data Protection Law Review; Nora Ni Loideain, 'Cape Town as a Smart and Safe City: Implications for Governance and Data Privacy' (2017) 7 International Data Privacy Law 314.

[8] See Rob Kitchin and Martin Dodge, *Code/Space: Software and Everyday Life* (MIT Press 2011).

[9] See Laura DeNardis, *The Internet in Everything* (Yale University Press 2020).

[10] See e.g. Rolf H Weber, 'Internet of Things – New Security and Privacy Challenges' (2010) 26 Computer Law & Security Review 23; Marie-Helen Maras, 'Internet of Things: Security and Privacy Implications' (2015) 5 International Data Privacy Law 99; Rolf H Weber, 'Internet of Things: Privacy Issues Revisited' (2015) 31 Computer Law & Security Review 618.

[11] See e.g. Laurens Vandercruysse, Caroline Buts and Michaël Dooms, 'A Typology of Smart City Services: The Case of Data Protection Impact Assessment' (2020) 104 Cities 102731.

[12] Laurens Vandercruysse, Michaël Dooms and Caroline Buts, 'The DPIA: Clashing Stakeholder Interests in the Smart City?' in Dara Hallinan, Ronald Leenes and Paul De Hert (eds), *Data Protection and Privacy, Volume 14: Enforcing Rights in a Changing World* (Bloomsbury 2021).

[13] Athena Christofi, 'Smart Cities and Data Protection Framework in Context' (2020) SPECTRE Project, Deliverable 1.2.

[14] From general queries such as e.g. '("DPIA" OR "PIA" OR "privacy impact assessment" OR "data protection impact assessment") + ("method" OR "methodology" OR "template" OR "guidelines")' to more specific queries e.g. about PIA and DPIA standards.

[15] The Netherlands, Belgium, UK, Sweden, Finland, Czech Republic, Estonia, Spain, Italy, France, Austria, Germany and Slovenia.

This research is bound to incur in some limitations, both endogenous and exogenous in nature. The first one is linguistic: data controllers write DPIA (and PIA) reports in their own language, and sometimes so do the authorities and organisations publishing DPIA methods, guidelines, and templates.[16] Access restrictions (due e.g. to licensing costs, confidentiality, or institutional constraints) also limit the study's scope. Researching DPIAs is also limited by the fact that there is no general obligation to publish DPIA reports, which limits the material publicly available.

It is also, to some extent, muddled by the fact that the emergence of DPIAs in EU data protection law has been preceded and inspired by the PIA experience, and thus –despite the fact that some argue that PIAs and DPIAs should be different assessments–[17] DPIA methods, guidelines, and templates partly overlap with PIA ones. Indeed, while the PIA experience began outside the EU,[18] and has kept developing since the obligation to carry out a PIA was first proposed in the draft General Data Protection Regulation,[19] DPIAs are eminently grounded in EU data protection legislation, and heavily conditioned by its spirit and principles. There seems to be limited utility in analysing PIA frameworks that are specifically geared towards other jurisdictions, although this report still mentions some privacy risk assessment[20] methodologies that are jurisdictionally neutral, and can be used regardless of the applicable legal framework, and thus readily integrated with the DPIA process. PIAs are, by now, spread throughout the globe – there would be an abundance of extra-EU PIA guidance document, but hardly a point in using them (besides, perhaps, in particular cases, such as the ones involving data transfers to the third country where those guidance documents apply).[21]

Finally, DPIAs have been framed as a form of meta-regulation (see the section below),[22] a particular regulatory approach whose characteristics and consequences largely justify the fragmentation and varying quality of PIA and DPIA frameworks, methods, guidelines, and templates potentially available to municipal administrations, on the one hand, but also increases the complexity of the inquiry.

[16] Although many PIA and DPIA guidance documents are translated in English, which seems to be a good practice, as English has factually become the *lingua franca* of (multi-lingual) Europe.

[17] E.g. De Hert (n 6). This report, for both historical and logical reasons, albeit aware of the difference between the right to privacy and the one of personal data protection, refers to DPIA and PIA interchangeably, as most of the literature and documentation we examined does.

[18] See e.g. Roger Clarke, 'A History of Privacy Impact Assessments' (2004) <http://www.rogerclarke.com/DV/PIAHist.html>; Roger Clarke, 'Privacy Impact Assessment: Its Origins and Development' (2009) 25 Computer Law & Security Review 123; David Tancock, Siani Pearson and Andrew Charlesworth, 'The Emergence of Privacy Impact Assessments' (2010); D Tancock, S Pearson and A Charlesworth, 'Analysis of Privacy Impact Assessments within Major Jurisdictions', *2010 Eighth International Conference on Privacy, Security and Trust* (2010); R Bayley and others, 'Privacy Impact Assessments: International Study of Their Application and Effects' (UK Information Commissioner's Office 2007); Adam Warren and others, 'Privacy Impact Assessments: International Experience as a Basis for UK Guidance' (2008) 24 Computer Law & Security Review 233.

[19] For a brief analysis of the GDPR's legislative trajectory, see generally 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 & Security Review 130; Paul De Hert and Vagelis Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 Computer Law & Security Review 179.

[20] Risk assessment being a core component of the DPIA process, but not equivalent to it.

[21] By way of example, recent PIA guidelines were released by the privacy and data protection authorities of Mexico, Singapore, Canada, Australia, New Zealand, and (jointly) Argentina and Uruguay: see respectively Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales, 'Guía Para La Elaboración de Evaluaciones de Impacto a La Privacidad' (2020) <https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/guiaeip.pdf>; Personal Data Protection Commission, 'Guide to Data Protection Impact Assessments' (2021); Office of the Privacy Commissioner of Canada, 'Expectations: OPC's Guide to the Privacy Impact Assessment Process' (2020) <https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/> accessed 22 March 2022; Office of the Australian Information Commissioner, 'Guide to Undertaking Privacy Impact Assessments' (2020); Privacy Commissioner, 'Privacy Impact Assessment Toolkit' (2015) <https://www.privacy.org.nz/publications/guidance-resources/privacy-impact-assessment/> accessed 22 March 2022; Agencia de Acceso a la Información Pública de Argentina (AAIP) and Unidad Reguladora y de Control de Datos Personales (URCDP), 'Guía de Evaluación de Impacto En La Protección de Datos' (2020) <https://www.argentina.gob.ar/sites/default/files/guia_final.pdf>.

[22] Reuben Binns, 'Data Protection Impact Assessments: A Meta-Regulatory Approach' (2017) 7 International Data Privacy Law 22; Raphaël Gellert, *The Risk-Based Approach to Data Protection* (Oxford University Press 2020).

3. Data Protection Impact Assessments

According to Art. 35 of the GDPR, where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons,[23] an assessment of the impact of the envisaged processing operations on the protection of personal data –a DPIA– must take place. The execution of the DPIA must happen before the processing begins,[24] and is a responsibility of the controller, who must seek the advice of the Data Protection Officer(s) (DPO), when designated,[25] and the views of data subjects or their representatives, where appropriate and without prejudice to commercial or public interests or the security of the processing.[26] While DPIAs focus on assessing the impact of certain kinds of processing on the right to data protection,[27] the reference to "rights and freedoms"[28] in relation to the factors that give rise to the need to conduct a DPIA indicates that the obligation does not arise only when risks to data protection and privacy rights are envisioned, but also when other fundamental rights and freedoms are potentially threatened.[29]

DPIAs are particularly significant when new technologies are designed, deployed, or used, and whenever a type processing, by virtue of its nature, scope, context, or purposes, has a high chance to impact natural persons. The GDPR exemplifies the kinds of processing that warrant a DPIA by virtue of the risks they present:[30] the systematic and extensive evaluation of personal aspects relating to natural persons, based on automated processing, and on which decisions are based that produce significant effects concerning the natural person; processing on a large scale of sensitive data or of personal data relating to criminal convictions and offences; the systematic monitoring of publicly accessible areas on a large scale. The list *ex* Art. 35(3) GDPR is non-exhaustive, but a mere sample, and national data protection authorities (DPAs) have the mandate to establish lists of processing activities for which a DPA is mandatory.[31] DPIAs should thus be performed, for instance, in case of large-scale operations processing personal data at regional, national, or supranational level, when many data subjects could be affected, and when the processing is likely to result in a high risk. Such risk can be envisaged, for example, when the data processed is sensitive, where a new technology is used on a large scale, or where the type of processing renders it more difficult for data subjects to exercise their rights. A high risk is also assumed where personal data are processed for taking decisions regarding

[23] See GDPR, Recital 75: "The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects".

[24] Their proactive nature distinguishes them from other activities with a narrower scope, such as privacy audits, as they begin before the implementation of a technology or process, rather than after it: Binns (n 22) 24.

[25] GDPR, Art. 35(2).

[26] GDPR, Art. 35(9).

[27] "(A)n assessment of the impact of the envisaged processing operations on the protection of personal data".

[28] "(L)ikely to result in a high risk to the rights and freedoms of natural persons".

[29] Kosta (n 4).

[30] GDPR, Art. 35(3).

[31] GDPR, Art. 34(4). For the Netherlands, see the blacklist authored by the Autoriteit Persoonsgegevens and published in the Staatscourant Nr. 64418, 27 November 2019. EU Member State DPAs have submitted DPIA "blacklists" *ex* Art. 35(4) to the EDPB, which has in turn issued opinions aiming at establishing common criteria across the EU; those opinions can be found at https://edpb.europa.eu/our-work-tools/our-documents/topic/data-protection-impact-assessment-dpia_en, last accessed Jan. 2022.

(specific) natural persons, following any systematic and extensive evaluation (e.g. profiling) or the processing of sensitive data, biometric data, or data on criminal convictions and offences.[32]

There are however several circumstances where data controller can be exempted from the obligation of performing a DPIA.[33] National DPAs may establish a list of processing activities for which performing a DPIA is not necessary.[34] Moreover, a single DPIA may be used to address multiple similar processing operations that present similar high risks.[35] Finally, where the processing is based on a legal obligation to which the controller is subject[36] or on the performance of a task carried out in the public interest or in the exercise of the controller's official authority,[37] it has a legal basis (either in EU law or in the law of the Member State applicable to the controller) that regulates the specific processing operation(s) in question, and a DPIA has already been carried out in the context of the adoption of that legal basis, a DPIAs is not required unless Member States mandate otherwise.[38]

DPIAs are meant to evaluate the origin, nature, particularity, likelihood and severity of the risk to the rights and freedoms of natural persons.[39] Art. 35(7) GDPR lists the minimum substance that the DPIA must contain: a systematic description of the envisaged processing operations and the purposes of the processing,[40] an assessment of the necessity and proportionality of the processing operations in relation to the purposes, an assessment of the risks to the rights and freedoms of the data subjects involved, and the measures envisaged to address the risks,[41] taking into account the rights and legitimate interests of data subjects and other persons concerned. Compliance with approved codes of conduct is also considered when assessing the impact of the processing operations performed.[42]

The performance of a DPIA must take place *before* the processing – ideally, at the design stage. DPIAs should however be seen as a continuous process, rather than an individual exercise: DPIAs should be

[32] GDPR, Recital 91. The A29WP recommends considering nine criteria, noting that in most cases, a processing instance that meets two criteria requires a DPIA, and that 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. However, in some cases, a processing instance meeting only one criterion may require a DPIA. The criteria considered are: 1. Evaluation or scoring, including profiling and predicting; 2. Automated decision-making with legal or similar significant effect; 3. Systematic monitoring of data subjects; 4. Sensitive data or data of a highly personal nature; 5. Data processed on a large scale (by virtue of the number of data subjects concerned, the volume of data and/or the range of different data items being processed, the duration, or permanence, of the data processing activity, or the geographical extent of the processing activity); 6. Matching or combining 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. See Article 29 Data Protection Working Party, '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' (n 1) 8 ss.

[33] For instance, the processing of personal data should not be considered to be on a large scale if it concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In those cases, a data protection impact assessment should not be mandatory: GDPR, Recital 91.

[34] GDPR, Art. 35(5).

[35] GDPR, Art. 35(3). See also Recital 92: "There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity".

[36] GDPR, Art. 6(1)(c).

[37] GDPR, Art. 6(1)(e). See also Recital 93: "In the context of the adoption of the Member State law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question, Member States may deem it necessary to carry out such assessment prior to the processing activities".

[38] GDPR, Art. 35(10).

[39] GDPR, Recital 84. See also Recital 90.

[40] Including, where applicable, the legitimate interest pursued by the controller.

[41] Including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR. See also Recital 90.

[42] GDPR, Art. 35(8).

subject to regular reviews.[43] Furthermore, where necessary, at least when there is a change of the risk envisaged, controllers must review their processing operations to assess if they are performed in accordance with the DPIA.[44]

3.1 Forerunners and neighbours

The introduction of Art. 35 in the GDPR did not happen in a vacuum: DPIAs have several antecedents and precursors both within and without the fields of privacy and personal data protection. The most notable antecedent is the Privacy Impact Assessment (PIA), a process aiming at assessing and mitigating the impact of privacy-invasive technologies and processes, and at managing compliance with privacy regulations. PIAs emerged between 1995–2005, driven both by growing public reaction against the increasingly privacy-invasive practices that arose during the second half of the 20th century and by the "natural development of rational management techniques".[45]

PIAs were, in turn, preceded by "technology assessments" (Tas), which were introduced by the Office of Technology Assessment (OTA) of the US Congress during the first half of the '70s,[46] and subsequently employed by European institution and Member States.[47] Tas encompass several different forms of policy analysis that aim at assessing the relationship between science and technology on one hand, and society on the other. Their purpose is to evaluate the probable detrimental effects of technological change, and to compare it with the possible benefits.[48]

Another antecedent can be found in the concept of Impact Statement (IS), most notably used in the field of environmental protection, which then evolved into the more substantial idea of Impact Assessment.[49] An Impact Assessment "is essentially a type of fact-finding and evaluation that precedes or accompanies research, or the production of artefacts and systems, according to specified criteria".[50] The performance of an impact assessment is often a requirement to be met in various kinds of institutional approval procedures; its aim is to estimate the likelihood and severity of potential harms associated with a project, and to show how those harms have been avoided or mitigated. Apart from PIAs, other types of Impact Assessment predate DPIAs: the Environmental Impact Assessment[51] is perhaps the most well-established Impact Assessment; the Social Impact Assessment[52] follows suit.

The momentum generated by the introduction of DPIAs in the GDPR, in conjunction to the experience deriving from other kinds of assessment (chiefly the PIA experience), has also given rise to novel kinds of evaluations that parallel DPIAs and often have a partly overlapping scope. A very close neighbour

[43] Article 29 Data Protection Working Party, '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' (n 1) 14. "In practice, this means that controllers must continuously assess the risks created by their processing activities in order to identify when a type of processing is 'likely to result in a high risk to the rights and freedoms of natural persons'" – Article 29 Data Protection Working Party, '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' (n 1) 6.

[44] GDPR, Art. 35(11). See also Recital 89.

[45] Clarke, 'Privacy Impact Assessment: Its Origins and Development' (n 18) 125.

[46] Clarke, 'Privacy Impact Assessment: Its Origins and Development' (n 18) 125.

[47] See e.g. Ruud Smits, Jos Leyten and Pim Den Hertog, 'Technology Assessment and Technology Policy in Europe: New Concepts, New Goals, New Infrastructures' (1995) 28 Policy sciences 271; Norman J Vig and Herbert Paschen, *Parliaments and Technology: The Development of Technology Assessment in Europe* (Suny Press 2000); Lars Klüver, Rasmus Øjvind Nielsen and Marie Louise Jørgensen, *Policy-Oriented Technology Assessment Across Europe* (Springer Nature 2015).

[48] Tancock, Pearson and Charlesworth, 'The Emergence of Privacy Impact Assessments' (n 18) 9.

[49] Tancock, Pearson and Charlesworth, 'The Emergence of Privacy Impact Assessments' (n 18) 9–10. See generally Dariusz Kloza and others, 'The Concept of Impact Assessment' in J Peter Burgess and Dariusz Kloza (eds), *Border Control and New Technologies* (Uitgeverij ASP).

[50] Charles D Raab, 'Information Privacy, Impact Assessment, and the Place of Ethics' (2020) 37 Computer Law & Security Review 6.

[51] See Directive 2014/52/EU of the European Parliament and of the Council of 16 April 2014 amending Directive 2011/92/EU on the assessment of the effects of certain public and private projects on the environment, 25.4.2014, OJ L 124/1.

[52] Ana Maria Esteves, Daniel Franks and Frank Vanclay, 'Social Impact Assessment: The State of the Art' (2012) 30 Impact Assessment and Project Appraisal 34.

to PIAs and DPIAs is thus the Surveillance Impact Assessment.[53] Artificial Intelligence (AI), Machine Learning (ML), and other forms of automated decision-making have led to Algorithmic Impact Assessments.[54] Rising ethical concerns relating to the design and deployment of new technologies resulted in the introduction of Ethical Impact Assessments,[55] and concerns over individual rights and freedoms gave rise to Human Rights Impact Assessments that specifically deal with new technologies and data processing.[56] Some proposals even attempt the merger between different kinds of impact assessment.[57]

3.2 Templates, methods, and methodologies

Since the beginning of the PIA experience, and even more so since the GDPR made DPIAs mandatory, a range of guides, methodologies, and templates have been published with the aim to assist data controllers and their organizations in performing PIAs and DPIAs. There is, however, considerable variation in the comprehensiveness and quality of the guides, methodologies, and templates available.[58] Given the broad description of and requirements for a DPIA resulting from Art. 35 of the GDPR, the process a data controller chooses to implement, the methods used to perform the assessment, and the supporting documents and tools, have a major effect on the value and usefulness of DPIAs on the ground.

National Data Protection Authorities (DPAs) have historically been at the forefront of the development of the concept of PIA, and consequently of DPIA, both individually and as assembled in the Article 29 Working Party (A29WP),[59] which produced its own DPIA guidelines.[60] The UK's Information Commissioner's Office (ICO), for instance, has been the first European DPA to develop a PIA guidance since well before the obligation to perform a DPIA was envisioned in EU law, using extra-European documents, methodologies, and templates in order to develop its own.[61] Likewise, the French *Commission nationale de l'informatique et des libertés* (CNIL) has published extensive PIA guidance,[62]

[53] David Wright and others, 'Sorting out Smart Surveillance' (2010) 26 Computer Law & Security Review 343; David Wright and Charles D Raab, 'Constructing a Surveillance Impact Assessment' (2012) 28 Computer Law & Security Review 613; David Wright, Michael Friedewald and Raphaël Gellert, 'Developing and Testing a Surveillance Impact Assessment Methodology' (2015) 5 International Data Privacy Law 40.

[54] Margot E Kaminski and Gianclaudio Malgieri, 'Algorithmic Impact Assessments under the GDPR: Producing Multi-Layered Explanations' [2020] International Data Privacy Law 19; Emanuel Moss and others, 'Assembling Accountability: Algorithmic Impact Assessment for the Public Interest' (2021). See also Janssen, who proposes a practical framework for human rights impact assessment in the context of automated decision-making (ADM), integrating it with DPIAs *ex* Art. 35 GDPR: Heleen L Janssen, 'An Approach for a Fundamental Rights Impact Assessment to Automated Decision-Making' (2020) 10 International Data Privacy Law 76.

[55] David Wright, 'A Framework for the Ethical Impact Assessment of Information Technology' (2011) 13 Ethics and Information Technology 199; David Wright and Emilio Mordini, 'Privacy and Ethical Impact Assessment' in Paul De Hert and David Wright (eds), *Privacy Impact Assessment* (Springer Netherlands 2012).

[56] Alessandro Mantelero and Maria Samantha Esposito, 'An Evidence-Based Methodology for Human Rights Impact Assessment (HRIA) in the Development of AI Data-Intensive Systems' (2021) 41 Computer Law & Security Review; Alessandro Mantelero, *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI* (Springer 2022).

[57] David Wright and others, 'Integrating Privacy Impact Assessment in Risk Management' (2014) 4 International Data Privacy Law 155; David Wright and Michael Friedewald, 'Integrating Privacy and Ethical Impact Assessments' (2013) 40 Science and Public Policy 755; Alessandro Mantelero, 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment' (2018) 34 Computer Law & Security Review 754.

[58] Roger Clarke, 'An Evaluation of Privacy Impact Assessment Guidance Documents' (2011) 1 International Data Privacy Law 111.

[59] And in the European Data Protection Board, since the GDPR repealed the DPD.

[60] Article 29 Data Protection Working Party, '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' (n 1).

[61] Bayley and others (n 18). See also Warren and others (n 18); David Wright, 'The State of the Art in Privacy Impact Assessment' (2012) 28 Computer Law & Security Review 54.

[62] The methodology of the CNIL comprises three guides: one setting out the PIA/DPIA methodology, a second containing PIA/DPIA templates, and a third providing a data protection knowledge bases: see CNIL, Privacy Impact Assessment (PIA) 1: Methodology, 2018; Privacy Impact Assessment (PIA) 2: Template, 2018; Privacy Impact Assessment (PIA) 3: Knowledge

updating it over the years to account for technological and social change, and developed its own software to chaperon data controllers through the execution of their DPIAs.[63] German DPAs, and the Conference of the Independent Data Protection Authorities of Germany (*Datenschutzkonferenz*), have also been providing PIA/DPIA guidance,[64] and so did e.g. the Spanish DPA (the *Agencia Española de Protección de Datos*, or AEPD)[65] and the Belgian DPA (the *Gegevensbeschermingsautoriteit*).[66] While the Dutch DPA *(*the *Autoriteit Persoongegevens*[67] did not publish its own methodology, and refers to the Dutch translation of the WP29 guidelines, a PIA model for the Netherlands was released by the Rijksoverheid.[68]

Research projects and academic organisations have also been quite active in producing new DPIA methodologies and templates,[69] and in evaluating existing ones.[70] For instance, the Flemish DPA has adopted a DPIA template that was developed by the d.pia.lab of the Vrije Universiteit Brussel.[71] Some professional organisations have been issuing their own methodologies and templates[72], and certain

Bases, 2018. Additionally, the CNIL published a document detailing the application of its methodology to IoT devices: see CNIL, Privacy Impact Assessment (PIA): application to connected objects. The CNIL methodology is available at https://www.cnil.fr/en/PIA-privacy-impact-assessment-en, last access Jan 2022.

[63] Commission Nationale de l'Informatique et des Libertés, 'The Open Source PIA Software Helps to Carry out Data Protection Impact Assessment' (2021) <cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment> accessed 15 July 2022.

[64] See The Standard Data Protection Model – A method for Data Protection advising and controlling on the basis of uniform protection goals, Version 2.0b, Adopted by the 99. Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder on the 17th of April 2020.

[65] The AEPD has been producing and updating guidance on PIA/DPIA and on risk management since at least 2014: see AEPD, Guía para la Evaluación de Impacto en la Protección de los Datos Personales, 2014; Guía práctica para las evaluaciones de Impacto en la Protección de los datos sujetas al RGPD, 2018; Guia prática de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD, 2018; Gestión del riesgo y evaluación de impacto en tratamientos de datos personales, 2021. The AEPD also provides models for DPIAs in both the public and the private sector: AEPD, Innovación y tecnología, available at https://www.aepd.es/es/areas-de-actuacion/innovacion-y-tecnologia, last access Jan 2022.

[66] Gegevensbeschermingsautoriteit, Aanbeveling nr. 01/2018 van 28 februari 2018, Aanbeveling uit eigen beweging met betrekking tot de gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging (CO-AR-2018-001).

[67] See Autoriteit Persoongegevens, Data protection impact assessment (DPIA), available at https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia, last access Jan 2022. Similarly, the Italian DPA (the *Garante per la Protezione dei Dati Personali,* GPDP) did not adopt its own guidelines, but rather points to the Italian versions of the A29WP opinion on DPIAs and of the CNIL DPIA tool.

[68] Rijksoverheid, Model gegevensbeschermingseffectbeoordeling rijksdienst (PIA), Versie 1.0, September 2017.

[69] E.g. David Wright and others, 'A Privacy Impact Assessment Framework for Data Protection and Privacy Rights' (2011) <https://piafproject.files.wordpress.com/2018/03/piaf_d1_21_sept2011revlogo.pdf>; Paul De Hert, Dariusz Kloza and David Wright, 'Recommendations for a Privacy Impact Assessment Framework for the European Union' (2012) <https://piafproject.files.wordpress.com/2018/03/piaf_d3_final.pdf>; Dariusz Kloza and others, 'Data Protection Impact Assessments in the European Union. Complementing the New Legal Framework towards a More Robust Protection of Individuals' (*d.pia.lab Policy Brief No. 1/2017*, 2017) <https://cris.vub.be/ws/portalfiles/portal/32009890/dpialab_pb2017_1_final.pdf>; Dariusz Kloza and others, 'Towards a Method for Data Protection Impact Assessment: Making Sense of GDPR Requirements' (*d. pia. lab Policy Brief No. 1/2019*, 2019) <https://cris.vub.be/ws/portalfiles/portal/48091346/dpialab_pb2019_1_final.pdf>; Dariusz Kloza and others, 'Data Protection Impact Assessment in the European Union: Developing a Template for a Report from the Assessment Process' (*d.pia.lab Policy Brief No. 1/2020*, 2020) <https://researchportal.vub.be/en/publications/data-protection-impact-assessment-in-the-european-union-developin>.

[70] E.g. Clarke, 'An Evaluation of Privacy Impact Assessment Guidance Documents' (n 58); Gellert, 'The Article 29 Working Party's Provisional Guidelines on Data Protection Impact Assessment' (n 2); David Wright, 'How Good Are PIA Reports – and Where Are They?' (2014) 25 European Business Law Review 407; David Wright, 'Making Privacy Impact Assessment More Effective' (2013) 29 The Information Society 307.

[71] Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens, 'Sjabloon VTC Voor GEB/DPIA' <https://overheid.vlaanderen.be/sjabloon-vtc-voor-geb/dpia> accessed 15 July 2022.

[72] E.g. NOREA, 'NOREA Handreiking Data Protection Impact Assessment' (2020); Rehab Alnemr and others, 'A Data Protection Impact Assessment Methodology for Cloud' in Bettina Berendt and others (eds), *Lecture Notes in Computer Science* (Springer 2015).

technological products and services have received specific, targeted[73] guidance. Standard-setting organisations have also been trying to formalise PIAs and DPIAs. The International Organization for Standardization (ISO) and the International Electrotechnical Commission[74], and so did the US National Institute of Standards and Technology (NIST). [75] The picture's complexity increases when considering a wider range of non-institutional actors active in the PIA and DPIA space for commercial (e.g. consultancies, software vendors) or non-commercial purposes (e.g. NGOs, civil society).

PIAs and DPIAs loom large in the transformation of contemporary municipalities into "smart" cities. The digitalisation of the urban environment leads to heightened privacy and data protection concerns, and PIAs and DPIAs are fundamental tools for demonstrating compliance with the law and for preventing or mitigating potential harms to data subjects. Some cities have thus developed their own PIA/DPIA methodologies and templates: the city of Helsinki, for instance, has published its own DPIA toolkit.[76] Organisations other than municipalities have also produced guidance targeted specifically at decision-makers in the urban environment.[77]

Contemporary municipalities hence have an ample selection of PIA and DPIA methodologies and templates to choose from. They can build on the minimum directions provided by Art. 35 of the GDPR, rely on the WP29's guidance, or on the guidance issued by the national DPA or by the DPA of another Member State. Decision-makers in the urban setting can also choose a methodology that is targeted to the specific domain or type of processing to be assessed, or develop their own set of methods and templates to account for the specific characteristics of the city in consideration. While the responsibility of executing a DPIA lies with the data controller assisted by the DPO(s), outsourcing DPIAs to an external DPO or to a consultancy is also a possibility. There is thus a copious assortment of methods and templates, each of which varies in content, quality, and depth; choosing which guidance documents and which methodology to rely on has, consequently, a major effect on the DPIA process and output.

3.3 PIA and DPIA as meta-regulation

The past decades[78] saw PIAs and DPIAs materialise in various jurisdictions, at first as a voluntary measure, and then as a mandatory obligation under the GDPR. DPIAs were thus born as a self-regulatory tool, but developed into a peculiar kind of compulsory requirement. This report adheres to the framing of PIAs and DPIAs as meta-regulation,[79] a technique where legislation is used to make

[73] See e.g. Smart Grid Task Force 2012-14 Expert Group 2: Regulatory Recommendations for Privacy Data Protection and Cyber-Security in the Smart Grid Environment, 'Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems' (2014). See also EDPS, 'Opinion of the European Data Protection Supervisor on the Commission Recommendation on Preparations for the Roll-out of Smart Metering Systems' (2012); Article 29 Data Protection 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).

[74] ISO/IEC 29134:2017, Information technology - Security techniques - Guidelines for privacy impact assessment, ISO/IEC JTC 1/SC 27. See also ISO 22307:2008, Financial services — Privacy impact assessment, ISO/TC 68/SC 9.

[75] Erika McCallister, Timothy Grance and Karen A Scarfone, 'Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) – Special Publication 800-122' (National Institute of Standards and Technology 2010).

[76] City of Helsinki, 'Data Protection Impact Assessment' (2019) <https://www.hel.fi/helsinki/en/administration/information/data-protection/data-protection-impact-assessment> accessed 22 March 2022.

[77] See e.g. Ben Green and others, 'Open Data Privacy: A Risk-Benefit, Process-Oriented Approach to Sharing and Protecting Municipal Data' (Berkman Klein Center for Internet and Society 2017).

[78] See generally Clarke, 'Privacy Impact Assessment: Its Origins and Development' (n 18); Warren and others (n 18); Tancock, Pearson and Charlesworth, 'The Emergence of Privacy Impact Assessments' (n 18); Tancock, Pearson and Charlesworth, 'Analysis of Privacy Impact Assessments within Major Jurisdictions' (n 18).

[79] Advanced by Binns (n 22). See also Gellert, *The Risk-Based Approach to Data Protection* (n 22). On the concept of meta-regulation, see Christine Parker, *The Open Corporation: Effective Self-Regulation and Democracy* (Cambridge University Press 2002). See also Sharon Gilad, 'It Runs in the Family: Meta-Regulation and Its Siblings' (2010) 4 Regulation & Governance 485; Cary Coglianese and Evan Mendelson, 'Meta-Regulation and Self-Regulation' in Robert Baldwin, Martin Cave and Martin Lodge (eds), *The Oxford Handbook of Regulation* (2010).

certain actors –in this case data controllers– responsible and accountable for their self-regulation processes and practices.

Meta-regulation is a regulatory strategy which does not prescribe specific measures or technologies, and that attempts to leverage corporations' existing management procedures, rather than necessarily creating new ones. This is bound to increase fragmentation and inhomogeneity in the environment of reference. Indeed, there are several DPIA frameworks, methods, guidelines, and templates for impact assessment, concerning many different domains of practice, and with dissimilar scope and quality.

While this lack of homogeneity and reliable granular guidance constitutes an obvious obstacle for data controllers, it has also been argued that the constant need for new frameworks, methods, guidelines, and templates is a function of the principle of receptiveness of impact assessments. Both the framework and the method are to be continuously improved if impact assessment is to serve its goals, to respond to societal change, and to give effect to new domains of practice.[80] The table below, adapted from Binns (2017),[81] maps the defining traits of meta-regulation to DPIAs in the GDPR.

Constitutive feature of meta-regulation	**Manifestation in the GDPR regime**
Requires organizations to take responsibility for their self-regulation efforts	DPIAs require data controllers to assess and mitigate risks themselves (Article 35(1))
Requires organizations to undertake risk-assessment processes	A DPIA should encompass an evaluation of the risks to the rights and freedoms of individuals (Article 35(7c))
Requires organizations to identify risk-mitigation strategies	A DPIA should involve a description of 'the measures envisaged to address the risk' (Article 33(7d))
Does not prescribe specific measures or technologies	No particular measures are prescribed—the controller must identify measures by themselves
Holds organizations accountable for adhering to their own policies	Controllers expected to review compliance with the measures set out in their own DPIAs (Article 35(11))
Attempts to leverage corporations' existing management procedures	The GDPR attempts to embed DPIAs in management procedures partly through DPOs (Article 39(1c))
Ensures stakeholders can democratically engage in evaluating organizations' measures and policies	Controller must seek input from data subjects or their representatives when conducting a DPIA (Article 35(9))
Liability to sanctions is related to failure to undertake the process, rather than focusing on the outcome	Undertaking a DPIA, especially if it is referred to the supervisory authority for prior consultation, is likely to significantly reduce any penalties for subsequent infringement due to the circumstances outlined in (Article 83(2))

Table 1 DPIA as meta-regulation, adapted from Binns (2017)

4. The state of the art in DPIA guidance documents

This section provides a narrative mapping of the DPIA guidance documents that could be used by municipal authorities and that are currently available within the state of the art. One of the first issues that come up when constructing a narrative mapping of the DPIA processes and practices available is

[80] Kloza and others, 'Towards a Method for Data Protection Impact Assessment: Making Sense of GDPR Requirements' (n 69).

[81] Binns (n 22). See also Gellert, *The Risk-Based Approach to Data Protection* (n 22).

the lack of definitional clarity. This report thus defines as a DPIA **framework** the essential supporting structure or organisational arrangement for the DPIA, which outlines and describes the conditions and principles thereof. It defines a DPIA **method** as the specific procedure for approaching the assessment, which regulates the DPIA in practice and defines the steps to be undertaken to perform a DPIA.[82] DPIA methods are often supplemented by **guidelines** and **templates**, which further explain the DPIA process, assist with structuring it, and explain how to draft a **report** to document it.

4.1. EU institutions: A29WP/EDPB, EDPS, and ENISA

Unsurprisingly, one of the most referenced DPIA guidance document is the Article 29 Data Protection Working Party's 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk"'.[83] The A29WP Guidelines are not a fully-fledged framework or method: they rather are a clarification of the requirements *ex* Art. 35 GDPR with a view to developing common criteria on the methodology for carrying out a DPIA, but not a method on their own. The A29WP Guidelines explain the scope of a DPIA, the processing operations that are subject to a DPIA and the ones that are not, when to follow up with the national DPA in case of residual high risks, and (to some extent) how to carry out a DPIA by expounding its timing, who is responsible for its conduction, whether DPIAs must be published, and the (lack of an uniform) methodology to carry out a DPIA. The A29WP Guidelines, despite not providing a DPIA methodology *per se*, also contain a short list of the main existing EU DPIA frameworks (at the time of its writing) in their first annex, and, in their second annex, a (particularly useful) list of criteria to be used to determine whether a DPIA report or a DPIA methodology are acceptable in light of the requirements set by Art. 35 GDPR.

While specifically targeted at EU institutions, and although not related exclusively to DPIAs, but rather to the broader data protection compliance framework,[84] the EDPS' accountability toolkit[85] also provides a decent foundation for impact assessments. Part I of the Accountability Toolkit explains when carrying out a DPIA is mandatory and how to perform a threshold assessment to determine high risk,[86] and provides as an annex a checklist of criteria for assessing whether processing operations are likely to result in a high risk. Part II of the Accountability Toolkit clarifies the scope of DPIAs and the allocation of responsibilities;[87] most notably, it also defines how to carry out a DPIAs by explaining its basic requirements and how to choose an appropriate methodology, how to describe the processing and its necessity and proportionality, and how to assess and treat the risks it might engender. Part II of the Accountability Toolkit also expounds how to document the assessment and write its report, how to set up appropriate review cycles, whether the report is to be made public, and when to do a prior consultation. Its annexes further provide a catalogue of guiding questions per data protection principle, a template structure for a DPIA report, and references a few of the most developed DPIA methodologies publicly available at the time.

[82] Kloza and others, 'Towards a Method for Data Protection Impact Assessment: Making Sense of GDPR Requirements' (n 69).

[83] Article 29 Data Protection Working Party, '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' (n 1).

[84] The processing of personal data by EU institutions is not regulated by the GDPR, but by 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, 21.11.2018, OJ L 295/39.

[85] EDPS, 'Accountability on the Ground Part I: Records, Registers and When to Do Data Protection Impact Assessments' (2019); EDPS, 'Accountability on the Ground Part II: Data Protection Impact Assessments & Prior Consultation' (2019); EDPS, 'Accountability on the Ground: Guidance on Documenting Processing Operations for EU Institutions, Bodies and Agencies Summary' (2019).

[86] In those situations where the processing considered is not included in the EDPS list of kinds of processing for which DPIAs are mandatory, or in the list of kinds of processing for which they are not; see EDPS, 'Decision of the European Data Protection Supervisor of 16 July 2019 on DPIA Lists Issued Under Articles 39(4) And (5) of Regulation (EU) 2018/1725' (2019) <https://edps.europa.eu/data-protection/our-work/publications/guidelines/data-protection-impact-assessment-list_en>.

[87] Although geared towards EU institutions, it might provide a blueprint that can be adapted to other kinds of large organisations.

The European Union Agency for Cybersecurity (ENISA), despite not having published a DPIA framework or method in the strict sense, has also provided extensive guidance[88] on how to guarantee the security of processing operations, and (at least) one online risk assessment tool.[89] While ENISA's guidance and tool are focussed exclusively on the assessment of the security risks of personal data processing operations, and do not take into account several other parameters that go beyond security and that are required by Art. 35 GDPR, they could still be useful in the context of the risk assessment phase of the DPIA process.

4.2. National DPAs and other state bodies

Many European DPAs have been providing guidance on how to execute a DPIA. The UK's Information Commissioner Office (ICO) –although not an EU DPA anymore– has historically been at the forefront of the emergence of PIAs and DPIAs. The first ICO PIA guidelines were published in 2007[90] and constitute the first structured set of PIA guidelines issued by a European DPA. Following a public consultation, the ICO published a revised set of guidelines in 2014;[91] as the GDPR entered into force, the 2014 PIA code of practice was superseded in 2016 by GDPR-specific DPIA guidance that, at the time of writing, is still in place, albeit updated to reflect the consequences of Brexit. The guidance provided by the ICO is also complemented by a ready-made DPIA template.[92] While the ICO's DPIA guidance is meant to be generic and applicable to all kinds of data controller and processing operation, the ICO has also been active in providing sector-specific DPIA guidance in the context of its Children's Code,[93] and has also co-authored, with the Surveillance Camera Commissioner, DPIA guidance for carrying out impact assessments on surveillance camera systems specifically,[94] and a relative DPIA template.[95] The ICO's DPIA framework has been refined over the span of a decade and a half, is very granular and yet highly customisable, and has proven itself to be a very good resource for data controllers and DPOs both within the UK and outside of it.[96]

The French CNIL has also published (both in French and in English) an extensive PIA framework, updating its 2012 Measures for Privacy Risk Management[97] to match the GDPR DPIA requirement. The framework's basis now comprises a methodology,[98] a template,[99] and the knowledge base[100] necessary to perform a proper assessment; it is also complemented by guidelines specifying the

[88] ENISA, 'Handbook on Security of Personal Data Processing' (ENISA 2018); ENISA, 'Guidelines for SMEs on the Security of Personal Data Processing' (ENISA 2017). See also George Danezis and others, 'Privacy and Data Protection by Design - from Policy to Engineering' (European Union Agency for Network and Information Security 2014).

[89] ENISA, On-line tool for the security of personal data processing, available at https://www.enisa.europa.eu/risk-level-tool/risk, last access March 2022.

[90] ICO, 'Privacy Impact Assessment Handbook' (ICO 2007). The Handbook was then subject to a minor update in 2009: ICO, 'Privacy Impact Assessment Handbook v 2.0' (ICO 2009).

[91] ICO, 'Conducting Privacy Impact Assessments Code of Practice' (2014).

[92] ICO, 'Sample DPIA Template' (2018) <https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf> accessed 10 March 2022.

[93] ICO, 'Age Appropriate Design: A Code of Practice for Online Services' (2020) <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/>. The code of practice also annexes an adaptation of the general ICO template to the specificities of the sector considered (i.e. digital products and services aimed at children); for an example of a DPIA carried out using that template, see ICO, 'Sample Data Protection Impact Assessment: Connected Toy' (2020) <https://ico.org.uk/for-organisations/childrens-code-hub/sample-data-protection-impact-assessment-connected-toy/>.

[94] ICO and Surveillance Camera Commissioner, 'Data Protection Impact Assessments – Guidance for Carrying out a Data Protection Impact Assessment on Surveillance Camera Systems' (ICO; Surveillance Camera Commissioner 2020).

[95] ICO and Surveillance Camera Commissioner, 'DPIA Template' (2020) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/886883/SCC__ICO_DPIA_Template_V4_.docx> accessed 10 March 2022.

[96] As the UK exited the EU, time will tell whether that will still be the case in the (near) future.

[97] Commission Nationale de l'Informatique et des Libertés, 'Methodology for Privacy Risk Management' (CNIL 2012); Commission Nationale de l'Informatique et des Libertés, 'Measures for the Privacy Risk Treatment' (2012).

[98] Commission Nationale de l'Informatique et des Libertés, 'Privacy Impact Assessment (PIA) Methodology' (CNIL 2018).

[99] Commission Nationale de l'Informatique et des Libertés, 'Privacy Impact Assessment (PIA) Templates' (CNIL 2018).

[100] Commission Nationale de l'Informatique et des Libertés, 'Privacy Impact Assessment (PIA) Knowledge Bases' (CNIL 2018).

application of the DPIA method to connected objects,[101] and by a customisable open-source software tool.[102] The three main guides comprising the CNIL's DPIA framework set out the general DPIA method, provide a catalogue of facts and elements to be used for formalizing the DPIA analysis, and a catalogue of controls aimed both at complying with the legal requirements of the GDPR and at preventing or mitigating the risks and harms that might come from the processing. The CNIL's DPIA framework is horizontal –meaning that it is meant to be universal and applicable to all kinds of controllers and processing– and must thus be tailored to the kind of processing to be undertaken. Notably, the CNIL's DPIA framework implements the EBIOS[103] risk management method for DPIAs *ex* Art. 35 GDPR while satisfying the acceptability criteria of the A29WP guidelines[104] and being compatible with the most common risk management standards.[105]

Germany's Standard Data Protection Model (SDM),[106] originally published in German[107] and translated in English, might have been published later than the guidance provided by the ICO and the CNIL,[108] but still appears to be one of the most rigorous and referenced frameworks available. The SDM was developed and is maintained by the Technische und organisatorische Datenschutzfragen (AK Technik) working group of the Conference of the Independent Data Protection Authorities of the Federation and the Länder. It is not a DPIA methodology in the narrow sense of the term, but is rather meant to substantiate the abstract regulatory requirements of the GDPR into specific technical and organisational measures. Regardless, the Standard Data Protection Model is concerned with risk and impact assessment and mitigation, and should be seen in the same meta-regulatory context as e.g. the ICO or CNIL PIA and DPIA guidelines.

The SDM provides a tool to support the selection and evaluation of technical and organisational measures to ensure and demonstrate compliance with the GDPR; it systematises those measures, and supports their selection on the basis of specific data protection goals. The SDM, as opposed to other DPIA or PIA methods or frameworks examined in this report, is targeted specifically and exclusively towards compliance with EU data protection law norms and principles. It is by no means a mere template for a compliance check, however: the SDM represent a consistent and systematic attempt at translating the *spirit* of EU data protection law into concrete organisational and technical measures. In 2017, German supervisory authorities[109] tested the first version of the SDM on a fictitious use case, provided with some data protection critical properties for the simulation's purposes, and aimed to compare the simulation's result with a DPIA conducted according to a method based on the ISO DPIA

[101] Commission Nationale de l'Informatique et des Libertés, 'Privacy Impact Assessment (PIA) Application to Connected Objects' (CNIL 2018).

[102] Available at https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment

[103] EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) is a risk management methodology published by the French Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

[104] Article 29 Data Protection Working Party, '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' (n 1).

[105] On the integration between risk management methodologies and (D)PIAs, see Wright and others, 'Integrating Privacy Impact Assessment in Risk Management' (n 57); David Wright and others, 'Privacy Impact Assessment and Risk Management' (Office of the Information Commissioner 2013).

[106] Conference of the Independent Data Protection Authorities, 'The Standard Data Protection Model – A Method for Data Protection Advising and Controlling on the Basis of Uniform Protection Goals Version 2.0b' (2020).

[107] Conference of the Independent Data Protection Authorities, 'Das Standard Datenschutzmodell Eine Methode Zur Datenschutzberatung Und -Prüfung Auf Der Basis Einheitlicher Gewährleistungsziele' (2020).

[108] Version 1.0 was adopted by the 92^ Conference of the Independent Data Protection Authorities of the Bund and the Länder in Kühlungsborn on 9-10 November 2016: Conference of the Independent Data Protection Authorities, 'The Standard Data Protection Model: A Concept for Inspection and Consultation on the Basis of Unified Protection Goals' (2016). Version 1.0 was updated (by Version 1.1) in 2018, after the GDPR became applicable. Version 2.0b, the latest version at the time of writing, was adopted by the 99^ Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder on the 17th of April 2020: Conference of the Independent Data Protection Authorities, 'The Standard Data Protection Model – A Method for Data Protection Advising and Controlling on the Basis of Uniform Protection Goals Version 2.0b' (n 106).

[109] The Independent Centre for Data Protection Schleswig-Holstein (ULD) and the data protection supervisory authority of Mecklenburg-Western Pomerania.

standard[110] by the Bavarian State Office for Data Protection Supervision (BayLDA). A workshop was organised and both methods were presented. However, a comparison was not made since the participants did not agree on criteria for the comparison.[111]

The Spanish DPA, the EIPD, has also been quite active in the DPIA domain (and in providing high-quality data protection guidance more generally). Its guidance on Risk Management and Impact Assessment[112] updates and consolidates the preceding practical guidelines on Risk Analysis for the Processing of Personal Data and on Impact Assessments on Personal Data Protection.[113] The guide provides a unified view of risk management and DPIAs, and facilitates the integration of risk management and compliance with the GDPR with the data controller's management and governance processes. The EIPD further complements its guidance by providing a checklist[114] for determining the formal adequacy of a DPIA and for the submission of prior consultation,[115] DPIA templates for both the public and the private sectors,[116] and a set of tools for conducting risk analysis and data protection impact assessments (Gestiona EIPD),[117] to help compliance with GDPR for entities that carry out low risk processing activities (FACILITA GDPR),[118] and to help entrepreneurs and technology start-ups to comply with data protection regulations (FACILITA-EMPRENDE).[119] In addition to the AEPD –the national DPA– the regional Catalan Data Protection Authority (APDCat) also issued its own DPIA guidelines, both in Catalan[120] and in English,[121] providing data controllers also with a DPIA template and a matching software tool.[122] The Spanish National Cryptologic Centre (CCN) also developed a set of risk management tool, PILAR,[123] that it licenses to public administrations, and that, despite not being meant as a DPIA tool *per se*, can be used to assist data controller and DPOs with some steps of their DPIAs.

[110] ISO, 'ISO/IEC 29134:2017(En) Information Technology — Security Techniques — Guidelines for Privacy Impact Assessment' (2017).

[111] S Gonscherowski and others, 'Durchführung Einer Datenschutz-Folgenabschätzung Gem. Art. 35 DSGVO Auf Der Methodischen Grundlage Eines Standardisierten Prozessablaufes Mit Rückgriff Auf Das SDM Am Beispiel Eines "Pay as You Drive"-Verfahrens (V 0.10)' (2017) 62 <https://www.datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20171106-Planspiel-Datenschutz-Folgenabschaetzung.pdf>.

[112] AEPD, 'Risk Management and Impact Assessment in the Processing of Personal Data' (2021) <https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf>.

[113] AEPD, 'Guía Práctica Para Las Evaluaciones de Impacto En La Protección de Los Datos Sujetas Al RGPD' (AEPD 2018); AEPD, 'Guía Práctica de Análisis de Riesgos En Los Tratamientos de Datos Personales Sujetos Al RGPD' (AEPD 2018).

[114] AEPD, 'Checklist for Determining the Formal Adequacy of a DPIA and the Submission of Prior Consultation' <https://www.aepd.es/es/documento/checklist-dpia-submission-prior-consultation.docx> accessed 10 March 2022.

[115] GDPR, Art. 36.

[116] AEPD, 'Template For Data Protection Impact Assessment Report (DPIA) For Public Administrations' (2022) <https://www.aepd.es/es/documento/modelo-informe-EIPD-AAPP-en.rtf>; AEPD, 'Template For Data Protection Impact Assessment Report (DPIA) For Private Sector' (2022) <https://www.aepd.es/es/documento/modelo-informe-EIPD-sector-privado-en.rtf>.

[117] AEPD, 'Gestiona EIPD' <https://gestiona.aepd.es/> accessed 10 March 2022.

[118] AEPD, 'Facilita RGPD' <https://www.aepd.es/en/guides-and-tools/tools/facilita-rgpd> accessed 10 March 2022.

[119] AEPD, 'Facilita EMPRENDE' <https://www.aepd.es/en/guias-y-herramientas/tools/facilita-emprende> accessed 10 March 2022.

[120] APDCat, 'Guia Pràctica Avaluació d'impacte Relativa a La Protecció de Dades' (2017) <https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/Guia-Practica-avaluacio-impacte-proteccio-de-dades-2019.pdf>.

[121] APDCat, 'Guide Data Protection Impact Assessment' (2017) <https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/DPIA-Guide.pdf>.

[122] APDCat, 'Data Protection Impact Assessment Tool' <https://apdcat.gencat.cat/en/documentacio/programari/aipd-programari/> accessed 22 March 2022.

[123] CCN-CERT (Spanish Government National Cryptologic Center - Computer Security Incident Response Team), 'PILAR' (2022) <https://pilar.ccn-cert.cni.es/index.php/en/> accessed 15 July 2022.

The Irish Data Protection Commission –*An Coimisiún um Chosaint Sonraí*– (DPC) issued a DPIA guidance note[124] and a document listing the processing operations warranting a DPIA[125] in 2018, a few months after the GDPR became applicable, and more than two years after in entered into force. When compared with the other English-language DPIA and PIA frameworks examined above, it does not appear that the Irish DPC's guidelines add much to the state of the art. Other DPAs have issued PIA and DPIA guidelines that are either not particularly innovative or do not add much to this report with respect to the guidelines mentioned above, or are not translated into other languages (e.g. English).[126] The Czech Office for Personal Data Protection –the *Úřad pro ochranu osobních údajů*– thus issued DPIA guidelines in Czech,[127] the Polish DPA (*Urząd Ochrony Danych Osobowych*, or UODO) also published DPIA guidance in Polish,[128] and the Slovenian DPA issued its own DPIA guidelines in Slovenian.[129] At the time of writing, and to the authors' knowledge, the latest EU DPA to release DPIA guidelines (and a matching Excel tool) is the Finnish *Tietosuojavaltuutetun toimisto*, which interestingly worked towards making its DPIA guidance[130] compatible with both the processing operations falling under the GDPR and the ones falling under Directive 2016/680, which regulates 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. There are minor variations in the institutional background of the DPIA guidance published by some other DPAs: the Danish *Datatilsynet*, for instance, co-authored its DPIA guidelines with the Danish Ministry of Justice,[131] while the Office for Personal Data Protection of the Slovak Republic published its DPIA procedure through a decree,[132] and the Belgian DPA issued its own set of guidelines through a Recommendation.[133] Other EU DPAs provide cursory guidance about the DPIA process on their website,[134] or refer to (the translation of) other DPIA frameworks or guidelines, such as the CNIL's, or the A29WP's.[135]

National DPAs are not the only state body that has published PIA or DPIA guidelines. In the Netherlands, for instance, the Dutch DPA did not publish its own DPIA guidelines, but rather refers to the Dutch translation of the A29WP guidelines[136] and to a DPIA model and a template that were issued

[124] Data Protection Commission, *Guidance Note: Guide to Data Protection Impact Assessments (DPIAs)* (Data Protection Commission / An Coimisiún um Chosaint Sonraí 2018).

[125] Data Protection Commission, *List of Types of Data Processing Operations Which Require a Data Protection Impact Assessment* (Data Protection Commission / An Coimisiún um Chosaint Sonraí 2018).

[126] It would seem a best practice to translate national DPIA guidance in English, like e.g. the German, Spanish, and French DPA guidelines: English is factually a *lingua franca*, and both DPIA guidelines and reports benefit from their comparison with the available alternatives.

[127] Úřad pro ochranu osobních údajů, 'Metodika Obecného Posouzení Vlivu Na Ochranu Osobních Údajů' (2020).

[128] Urząd Ochrony Danych Osobowych, 'Jak Rozumieć Podejście Oparte Na Ryzyku?' (2018).

[129] Informacijski pooblaščenec, 'Ocene Učinkov Na Varstvo Podatkov Smernice Informacijskega Poobla Ščenca' (2017). An updated version has been released in 2019.

[130] Tietosuojavaltuutetun toimisto, 'Tietosuojan Vaikutustenarvioinnin Ohje' (2021).

[131] Datatilsynet and Justitsministereit, 'Konsekvensanalyse' (2018).

[132] Úradu na ochranu osobných údajov, 'Vyhláška – Úradu Na Ochranu Osobných Údajov Slovenskej Republiky z 29. Mája 2018 o Postupe Pri Posudzovaní Vplyvu Na Ochranu Osobných Údajov' (2018).

[133] Gegevensbeschermingsautoriteit, 'Aanbeveling Nr. 01/2018 van 28 Februari 2018 Aanbeveling Uit Eigen Beweging Met Betrekking Tot de Gegevensbeschermingseffectbeoordeling En Voorafgaande Raadpleging (CO-AR-2018-001)' (2018) <https://www.gegevensbeschermingsautoriteit.be/publications/aanbeveling-nr.-01-2018.pdf>. In Belgium, the Flemish Supervisory Commission for the processing of personal data also published its own DPIA template, developed on the basis of the output of the d.pia.lab (see below): Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens (n 71).

[134] E.g. IMY, 'Så Här Gör Man En Konsekvens-bedömning' (2021) <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/konsekvensbedomningar-och-forhandssamrad/sa-har-gor-man-en-konsekvensbedomning/> accessed 10 March 2022.

[135] See e.g. the Italian DPA, the GPDP, who points to the Italian translations of the A29WP guidelines and to an Italian version of the CNIL DPIA tool: Garante per la Protezione dei Dati Personali, 'Valutazione Di Impatto Sulla Protezione Dei Dati (DPIA)' <https://www.garanteprivacy.it/regolamentoue/DPIA>.

[136] Autoriteit Persoongegevens, 'Data Protection Impact Assessment (DPIA)' <https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia> accessed 10 March 2022.

in Dutch by the central government (*Rijksoverheid*).[137] Additionally, with regards to cities specifically, the IBD (the Information Security Service of Dutch municipalities) and the Association of Netherlands Municipalities (VNG) have developed various products to support municipalities in implementing and guaranteeing privacy, data protection, and information security, including a DPIA tool[138] known as Integrated Risk and Privacy Analysis (IRPA) and a set of related DPIA guidelines.[139] IRPA, which was developed and tested together with several municipalities, aims at facilitating the execution of many different kinds of assessment –including DPIAs– and the introduction of information security and data protection controls. The tool consists of a diverse combination of several assessments: a Data Privacy Impact Assessment (DPIA), including the pre-screening process, a tool for determining technical and organisational security measures and a basic security level (BBN), a baseline BBN test according to the Dutch BIO information security standard, a Risk Analysis, a "GAP(-O)" Analysis, and an ethical assessment through the integration of the Data Ethics Decision Aid (DEDA) tool.[140] IRPA –and the broader impact assessment framework developed by IBD– are notable, in particular, on account of how it foresees the default sharing of DPIA reports with all other members of the IBD community, by and through the tool itself.

The research underlying this report has also shown how some local government entities have issued their own DPIA templates, and in some cases their own guidelines, as e.g. the city of Helsinki did.[141] The Finnish capital published its own DPIA toolset,[142] designed specifically for Helsinki, both to facilitate the cooperation between the city and its service providers, and to foster data protection more generally by making the DPIA tools available to the public. It is worth noting how some other DPIA methodologies, guidelines, and templates created by local governments are not "forward-facing", meaning that they might not be published or publicly available, or that they are held in the data controller's intranet.[143] Some DPIA templates and guidelines, particularly at the local level, in other words, are just meant to be *used* by the controller (and its DPO), and there may be no reason to publish and document them; some other templates and guidelines, on the other hand, are meant to be used by a broader array of stakeholders, and are thus published, publicised, and documented.

4.3. Professional organisations and sector-specific frameworks

Besides the general DPIA guidance provided by Member State DPAs or by other state bodies, there are several examples of sector- or domain-specific DPIA frameworks that have been developed over the years, some of which predate the GDPR. At the EU level, an early example is the 2011 Privacy and Data Protection Impact Assessment Framework for RFID Applications,[144] the first PIA/DPIA framework endorsed by the Commission. The development of the RFID PIA framework was due to the impulse

[137] Rijksoverheid, 'Data Protection Impact Assessment' (2021) <https://www.kcbr.nl/beleid-en-regelgeving-ontwikkelen/integraal-afwegingskader-voor-beleid-en-regelgeving/verplichte-kwaliteitseisen/data-protection-impact-assessment> accessed 10 March 2022.

[138] VNG, 'IRPA-Tool' <https://www.informatiebeveiligingsdienst.nl/irpa-tool/> accessed 30 March 2022.

[139] Vereniging van Nederlandse Gemeenten / Informatiebeveiligingsdienst voor gemeenten (IBD), 'Handreiking Data Protection Impact Assessment (DPIA) Een Operationeel Kennisproduct Ter Ondersteuning van de Implementatie van de Baseline Informatiebeveiliging Overheid (BIO)' (2020) <https://www.informatiebeveiligingsdienst.nl/product/handreiking-dpia-bio/> accessed 30 March 2022.

[140] Utrecht Data School, 'Data Ethics Decision Aid (DEDA)' <https://dataschool.nl/en/deda/> accessed 30 March 2022.

[141] City of Helsinki (n 76).

[142] The toolset comprises a set of instructions for making a DPIA which guides data controllers from the initial assessment (a pre-screening) to the actual DPIA, providing them also with a risk analysis form and a data protection checklist.

[143] This is also coherent, *mutatis mutandis*, with the findings of a recent EDPS survey, where it was observed that many EU institutions do not publish their DPIAs on account of security concerns, confidentiality issues, and the lack of an explicit obligations in that sense, many other publish summaries of their DPIA, and a small number of EU institutions publish their DPIAs only on their intranet: EDPS, 'EDPS Survey on Data Protection Impact Assessments under Article 39 of the Regulation (Case 2020-0066)' (2020) 12–13.

[144] GS1, 'Privacy and Data Protection Impact Assessment Framework for RFID Applications' (2011). See also Sarah Spiekermann, 'The RFID PIA–Developed by Industry, Endorsed by Regulators' in Paul De Hert and David Wright (eds), *Privacy impact assessment* (Springer 2012). GS1 also developed a matching DPIA tool: GS1, 'GS1 EPC/RFID Privacy Impact Assessment Tool' <https://www.gs1.org/standards/rfid/pia> accessed 20 March 2022.

provided by the Commission's Recommendation on the implementation of privacy and data protection principles in RFID applications,[145] where the Commission tasked the RFID industry, in collaboration with relevant civil society stakeholders, with the development of a framework for privacy and data protection impact assessments. The RFID PIA framework was also subject, as mandated by the Commission's recommendation,[146] to the opinion of the A29WP, which –after raising a number of objections to an early draft–[147] eventually endorsed its final version.[148] The (relatively generic) RFID PIA framework also formed the basis for national specifications, such as the German Federal Office for Security in Information Technology (*Bundesamt für Sicherheit in der Informationstechnik*) Privacy Impact Assessment Guideline for RFID Applications.[149]

A second industry-specific PIA/DPIA guidance document endorsed by the Commission is the Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems.[150] In 2012, the European Commission issued Recommendation 2012/148/EU[151] on the preparation for the roll out of smart metering systems, where it endorsed the preparation and the adoption of a DPIA Template. A first version of the template was developed in 2013 by the Commission's Smart Grid Task Force (SGTF)[152] and submitted to the A29WP for its judgment. An initial A29WP opinion[153] raised a number of critical remarks: some of them were subsequently addressed by the SGTF in a second version of the Template, while some other criticalities seemed to remain.[154] The SGTF EG2 thus prepared a third version of the Template in 2014, which was eventually endorsed by the Commission.[155] The current version of the Template –the fourth one– has been extensively updated due to the adoption of the GDPR.[156]

Besides sector-specific EU DPIA guidance, professional and industrial associations have been publishing their own DPIA guidelines as well. While largely derivative in nature, (some of) those documents have the value of being tuned towards a specific industrial sector or professional domain, of which they might however also share the bias towards personal data protection. NOREA –the Dutch association of IT auditors– has been publishing its PIA guidance since 2013, updating it along the way and eventually rebranding it into DPIA guidelines as the GDPR entered into force.[157] Bitkom, a German

[145] Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radiofrequency identification (2009/387/EC), 16.5.2009, OJ L 122/47.

[146] Commission Recommendation 2009/387/EC, §4.

[147] Article 29 Data Protection Working Party, 'Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications WP 175' (2010); GS1, 'Industry Proposal–Privacy and Data Protection Impact Assessment Framework for RFID Applications' (2010) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp175_annex_en.pdf>.

[148] Article 29 Data Protection Working Party, 'Opinion 9/2011 on the Revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications WP 180' (2011); GS1, 'Privacy and Data Protection Impact Assessment Framework for RFID Applications' (n 144).

[149] Marie Caroline Oetzel and others, 'Privacy Impact Assessment Guideline for RFID Applications' (Julian Cantella ed, 2011) <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Langfassung.pdf?__blob=publicationFile&v=1>.

[150] SGTF EG2, 'Smart Grid Task Force 2012-14 Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment' (2018) <https://energy.ec.europa.eu/system/files/2018-09/dpia_for_publication_2018_0.pdf>.

[151] Commission Recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems (2012/148/EU), 13.3.2012, OJ L 73/9.

[152] Specifically, by Expert Group 2 (EG2).

[153] Article 29 Data Protection 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' (n 73).

[154] Article 29 Data Protection Working Party, '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 WP209' (2013).

[155] Commission Recommendation of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems (2014/724/EU), 18.10.2014, OJ L 300/63.

[156] SGTF EG2 (n 150).

[157] NOREA (n 72).

digital industry association, issued its own risk assessment and DPIA guide, both in German[158] and in English.[159] IAB Europe –an industrial association for digital marketing and advertising– released a set of DPIA guidelines targeted towards the online advertising ecosystem.[160]

Sector-specific PIA and DPIA frameworks have not been published only by private actors, but also by public organisations. Examples include, besides the sector-specific guidance by the UK ICO mentioned above,[161] the Guidance on Privacy Impact Assessment in health and social care issued by the Irish Health Information and Quality Authority (HIQA),[162] or the tool (and related methodology)[163] developed by the office of the DPO of the TICSALUT Foundation in collaboration with the Observatory of Bioethics and Law at the University of Barcelona,[164] which focuses on DPIA in the health sector, and is based on the framework created by the Catalan Authority for Data Protection.[165] Universities have also been developing interesting sector-specific PIA and DPIA guidance documents on their own: an example may be given by the University of Groningen, who developed a DPIA methodology specifically for human subject research.[166] Indeed, as the following section highlights, our review has shown that universities, research institutes, and publicly funded (or co-funded) research projects have had a notable influence on the development of PIA and DPIA in the EU.

4.4. Universities, research institutes, and research projects

From both a chronological[167] and a logical point of view, the work of academic institutes and other research endeavours –such as private research institutes, or EU-funded projects and consortia– has proven to be foundational for the development of PIAs and DPIAs in the EU. Several research projects have successfully entwined their output with official DPIA guidance issued by public authorities; others

[158] Bitkom, 'Risk Assessment & Datenschutz-Folgenabschätzung Leitfaden' (2017) <https://www.bitkom.org/Bitkom/Publikationen/Risk-Assessment-Datenschutz-Folgenabschaetzung.html>.

[159] Bitkom, 'Risk Assessment & Data Protection Impact Assessment Guide' (2017) <https://www.bitkom.org/Bitkom/Publikationen/Risk-Assessment-Data-Protection-Impact-Assessment.html>.

[160] IAB Europe Legal Committee, 'GDPR Data Protection Impact Assessments (DPIA) for Digital Advertising under GDPR' (2020) <https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf>. IAB UK also released a version of the same guidelines specifically for the UK: IAB UK, 'IAB UK Digital Advertising Guidance: Data Protection Impact Assessments under the GDPR' (2020) <https://www.iabuk.com/sites/default/files/public_files/IAB-UK Digital-advertising-guidance-Data-Protection-Impact-Assessments-under-the-GDPR.pdf>.

[161] ICO and Surveillance Camera Commissioner (n 95); ICO, 'Age Appropriate Design: A Code of Practice for Online Services' (n 93).

[162] Health Information and Quality Authority, 'Guidance on Privacy Impact Assessment in Health and Social Care Version 2.0' (2017) <https://www.hiqa.ie/sites/default/files/2017-10/Guidance-on-Privacy-Impact-Assessment-in-health-and-social-care.pdf>. A previous version predates the GDPR: Health Information and Quality Authority, 'Guidance on Privacy Impact Assessment in Health and Social Care' (2010) <https://www.hiqa.ie/sites/default/files/2017-03/HI_Privacy_Impact_Assessment.pdf>.

[163] Rather than a DPIA methodology in the sense used thus far, however, the document seems to rather resemble an users' manual for the tool.

[164] While the tool is available in English, Spanish, and Catalan, the methodology is, at the time of writing, available only in Catalan: TIC Salut Social, 'DPIA Tool' (2020) <https://ticsalutsocial.cat/dpd-salut/dpia-tool/> accessed 20 March 2022; TIC Salut Social and Observatori de Bioètica i Dret Universitat de Barcelona, 'Avaluació d'impacte Relativa a La Protecció de Dades (Aipd) En Salut – Metodologia d'aplicació' (2020) <https://ticsalutsocial.cat/wp-content/uploads/2021/07/aipd_formacio-metodologia.pdf> accessed 20 March 2022. For an account of the creation of the methodology, see Ricard Mas and others, 'Creació de La Metódólógia per a l'avaluació de l'impacte Relativa a La Prótecció de Dades En Salut (AIPD)' (*Universitat de Barcelona, Observatori de Bioètica i Dret – Càtedra UNESCO de Bioètica*, 2020) <https://ticsalutsocial.cat/wp-content/uploads/2021/07/aipd_creacio-metod_221220.pdf>.

[165] APDCat, 'Guia Pràctica Avaluació d'impacte Relativa a La Protecció de Dades' (n 120). In English, APDCat, 'Guide Data Protection Impact Assessment' (n 121).

[166] E Hoorn and C Montagner, 'Starting with a DPIA Methodology for Human Subject Research' (2018) <https://www.rug.nl/research/research-data-management/downloads/c2-dataprotection-dl/dpia_guidance_doc_v1_pub.pdf>.

[167] Academic studies conducted by universities and research institutes formed the basis for the PIA guidance of the ICO – Europe's earliest institutional DPIA guidelines: see e.g. Warren and others (n 18). They also arguably conditioned the development of Art. 35 GDPR.

have authored or customised PIA or DPIA methods in order to apply them to the specific domain covered by the research project of reference.

The PIAF[168] project, for instance, is one of the earliest and most cited research projects on PIAs (and thus DPIAs); although it published its deliverables before the publication GDPR, the PIAF project's guidance is of a high quality, and still timely. The experience of the PIAF project was later carried on to other academic endeavours, such as the d.pia.lab, which published valuable guidance on PIA, DPIA, and impact assessment practices in general.[169] The d.pia.lab's guidelines –its "policy briefs"– are, when compared to most of the other guidelines examined, particularly synthetic and to the point, without detriment to their general quality.

Fraunhofer, a German research organisation, also published practical DPIA guidance, both in English and in German.[170] The guide builds on previous work undertaken by the authors,[171] and moves from the German Standard Data Protection Model[172] developed by the German Conference of the Independent Data Protection Authorities. The Fraunhofer DPIA guide divides the process into five phases (Initiation, DPIA Preparation, DPIA Execution, DPIA Implementation, and Sustainability), each of which is further broken down through a set of elements (Objective, Input, Roles and responsibility, Implementation, and Output and results). The Fraunhofer DPIA guide is detailed and procedural, and puts a particularly heavy emphasis on documentation.[173]

Another rigorous framework that comes from an academic setting is the PIA methodology introduced by Spiekermann and Oetter,[174] which was adopted by the German Federal Office for Information Security (BSI) for their RFID PIA guidelines,[175] representing yet another entwinement between academic research and public governance. Following a research approach based on design science,

[168] Wright and others, 'A Privacy Impact Assessment Framework for Data Protection and Privacy Rights' (n 69). See also De Hert, Kloza and Wright (n 69); Gus Hosein and Simon Davies, 'Empirical Research of Contextual Factors Affecting the Introduction of Privacy Impact Assessment Frameworks in the Member States of the European Union' <https://piafproject.files.wordpress.com/2018/03/piaf_d2_final.pdf>.

[169] Kloza and others, 'Data Protection Impact Assessment in the European Union: Developing a Template for a Report from the Assessment Process' (n 69); Kloza and others, 'Towards a Method for Data Protection Impact Assessment: Making Sense of GDPR Requirements' (n 69); Kloza and others, 'Data Protection Impact Assessments in the European Union. Complementing the New Legal Framework towards a More Robust Protection of Individuals' (n 69).

[170] Nicholas Martin and others, *Die Datenschutz-Folgenabschätzung Nach Art. 35 DSGVO: Ein Handbuch Für Die Praxis* (Fraunhofer Verlag 2020); Nicholas Martin and others, *The Data Protection Impact Assessment According to Article 35 GDPR. A Practitioner's Manual.* (Fraunhofer Verlag 2020).

[171] Michael Friedewald and others, 'Die Datenschutzfolgenabschätzung – Ein Werkzeug Für Einen Besseren Datenschutz' (2016). See also Michael Friedewald and others, 'Data Protection Impact Assessments in Practice' in Sokratis Katsikas and others (eds), *ESORICS 2021 International Workshops* (Springer International Publishing 2022). Additionally, see Felix Bieker and others, 'A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation' in Stefan Schiffner and others (eds), *Privacy Technologies and Policy. APF 2016.* (Springer 2016).

[172] Conference of the Independent Data Protection Authorities, 'The Standard Data Protection Model – A Method for Data Protection Advising and Controlling on the Basis of Uniform Protection Goals Version 2.0b' (n 106); Conference of the Independent Data Protection Authorities, 'Das Standard Datenschutzmodell Eine Methode Zur Datenschutzberatung Und -Prüfung Auf Der Basis Einheitlicher Gewährleistungsziele' (n 107).

[173] Amongst the documents it requires for carrying out a DPIA are: documentation about the processing operations, including the records of processing activities *ex* Art. 30(1) GDPR, documentation ensuring the lawfulness of processing *ex* Art. 6 GDPR, and preliminary considerations concerning the necessity and proportionality of the processing; documentation of the "positive" threshold assessment; a summary collection of information concerning the nature, scope, context and purposes of the processing and all other information relevant for the review; proposal of the DPIA team to carry out the execution phase and planning work- shops/deadlines; a DPIA report; documentation of the mitigation measures, test methodology and test records of the effectiveness of mitigation measures and of monitoring the risks; proof of compliance with the GDPR and approval of the processing.

[174] Marie Caroline Oetzel and Sarah Spiekermann, 'A Systematic Methodology for Privacy Impact Assessments: A Design Science Approach' (2014) 23 European Journal of Information Systems 126.

[175] Oetzel and others (n 149).

and on the basis of a BSI-authored risk assessment method,[176] the authors developed and tested a cyclical PIA methodology, comprised of seven steps[177] which cover the whole PIA/DPIA lifecycle.

Risk assessment and risk modelling are integral parts of the PIA/DPIA process. In this respect, it is worth highlighting both the PRIAM[178] and the LINDDUN[179] methodologies. PRIAM,[180] developed by researchers at INRIA, is not a full PIA or DPIA framework, but rather a rigorous and systematic privacy risk analysis (PRA) methodology – PRA being, as the authors claim, the core of a PIA. PRIAM's main claim is that PIA/DPIA frameworks do not define with sufficient precision how the analysis of privacy risks should be performed; PRIAM aims at filling the gap by providing a concrete, rigorous, and systematic PRA methodology that is customizable and compatible with existing PIA and DPIA frameworks. The methodology is made of two main phases: information gathering and risk assessment. In the information gathering phase, the categories and the attributes of seven core components (system, stakeholders, data, risk sources, feared events, harms and privacy weaknesses) are defined. After the information gathering phase ends, the risk assessment phase begins: there, the assessor formalises the relationship between privacy harms, feared events, and weaknesses by creating "harm trees", akin to attack trees in computer security,[181] leading to a well-defined and formalised risk assessment process.

LINDDUN,[182] developed since 2010 by researchers from KU Leuven, has a feebler connection with PIA and DPIA frameworks *stricto sensu*, rather being a privacy threat modelling[183] methodology. Nonetheless, it would provide an extremely solid supplement to any PIA/DPIA framework, albeit likely at the cost of some additional overhead. LINDDUN adapts the threat modelling practices that are commonplace in security processes to the specificity of privacy risks, and could provide additional rigour to the DPIA process – integrating it, rather than replacing it. LINDDUN consists of six steps: defining the data flows through a diagram (1), mapping the privacy threats to the diagram's elements (2), identifying threat scenarios (3), prioritising threats (4), eliciting mitigation strategies (5), and selecting the corresponding privacy-enhancing technologies (6). The first three steps are the core of LINDDUN, as they focus on the problem space and aim at identifying privacy threats – threat modelling, indeed. The three remaining steps are solution-oriented, as they mean to address the threats identified into strategies and technologies that can prevent the threats or mitigate their harm.[184] As privacy threat modelling can be a daunting task, particularly if the person doing the modelling does not have a technical background –LINDDUN is mostly thought for software developers

[176] Bundesamt für Sicherheit in der Informationstechnik (BSI), 'BSI-Standard 100-3: Risk Analysis Based on IT-Grundschutz' (2008).

[177] I.e. characterisation of the system, definition of the privacy targets, evaluation of the degree of protection demanded for each privacy target, identification of the threats for each privacy target, identification and recommendation of controls suited to protect against those threats, assessment and documentation of the residual risks, and documentation of the PIA process.

[178] Sourya Joyee De and Daniel Le Métayer, 'PRIAM: A Privacy Risk Analysis Methodology' (Giovanni Livraga and others eds, *INRIA Research Report*, 2016) 221 <https://hal.inria.fr/hal-01302541/file/RR-8876.pdf>.

[179] LINDDUN.org, 'LINDDUN - Home' (2020) <https://www.linddun.org/> accessed 20 March 2022.

[180] De and Le Métayer (n 178).

[181] The same approach is used by the LINDDUN methodology (see the following paragraph): see e.g. Kim Wuyts, Riccardo Scandariato and Wouter Joosen, 'LIND(D)UN Privacy Threat Tree Catalog' (2014) CW Reports 675.

[182] LINDDUN.org (n 179). See also e.g. Mina Deng and others, 'A Privacy Threat Analysis Framework: Supporting the Elicitation and Fulfillment of Privacy Requirements' (2011) 16 Requirements Engineering 3; Kim Wuyts, Riccardo Scandariato and Wouter Joosen, 'Empirical Evaluation of a Privacy-Focused Threat Modeling Methodology' (2014) 96 Journal of Systems and Software 122; Laurens Sion and others, 'Interaction-Based Privacy Threat Elicitation', *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (IEEE 2018).

[183] See Koen Yskout and others, 'Threat Modeling: From Infancy to Maturity', *2020 IEEE/ACM 42nd International Conference on Software Engineering: New Ideas and Emerging Results (ICSE-NIER)* (IEEE 2020).

[184] Kim Wuyts and Wouter Joosen, 'LINDDUN Privacy Threat Modeling: A Tutorial' (2015) CW Reports 685. See also Wuyts, Scandariato and Joosen (n 181).

and the likes– the LINDDUN team has also released LINDDUN Go,[185] a card-based introductory "lightweight" privacy threat modelling tool.

Research projects have also been very active in the PIA/DPIA space, although usually providing various kinds of DPIA-related guidance, rather than fully fledged "horizontal" DPIA methodologies and frameworks. The output of the SPECTRE project,[186] for instance, is particularly relevant for DPIAs in the (smart) urban environment, despite not being a DPIA framework or method *per se*.[187] EU-funded projects have indeed been particularly prolific in developing the concept of DPIA. Interesting research in the PIA and DPIA space has been undertaken, without pretence of exhaustivity, by the PARENT project,[188] which dealt with smart metering technologies, by the CyberSec4Europe project,[189] which attempted to consider and privacy and data protection standards and frameworks other than the GDPR, and by the HR-Recycler project,[190] in the context of industrial recycling of electronic waste. Other examples include, but are by no means limited to, deliverables e.g. from the PERSONA project,[191] about borderless crossing technologies, or the SynchroniCity project,[192] which dealt *inter alia* with DPIAs in the IoT, or the A4Cloud and tClouds project,[193] which dealt with DPIAs in cloud computing. Broadening the scope from PIAs and DPIAs to different –but related– kinds of impact assessment would lead to other insightful projects and to their output, e.g. the VIRT-EU project[194] and its privacy, ethics, and security impact assessment (PESIA), the PRESCIENT project,[195] which merged

[185] LINDDUN, 'LINDDUN GO' <https://www.linddun.org/go> accessed 20 March 2022. See also Kim Wuyts, Laurens Sion and Wouter Joosen, 'Linddun Go: A Lightweight Approach to Privacy Threat Modeling', *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (IEEE 2020).

[186] See e.g. Jonas Breuer, Rob Heyman and Jo Pierson, 'Mapping DPIA (Best) Practices in Smart Cities D 2.1' (*SPECTRE project*) <https://spectreproject.be/output/downloads-1/mapping-dpia-best-practices-in-smart-cities>; Laurens Vandercruysse, Caroline Buts and Michaël Dooms, 'Economic Costs of the DPIA D.3.1' (*SPECTRE project*, 2019) <https://spectreproject.be/output/downloads-1/deliverable-d3-1-economic-costs-of-the-dpia.pdf>; Laurens Vandercruysse, Caroline Buts and Michaël Dooms, 'A Typology of Smart City Services Based on DPIA-Costs D.3.2' (*SPECTRE project*, 2019); Laurens Vandercruysse, Caroline Buts and Michaël Dooms, 'Selecting a Data Protection Approach for Procurement of Smart City Services: Matching Policy Feasibility with Intrinsic Service Characteristics D.3.4' (*SPECTRE project*, 2019).

[187] Similarly, despite not being PIA/DPIA guidelines in the strict sense of the term (but rather with privacy and data protection by design, which are nonetheless intrinsically connected to PIAs and DPIAs), it might be worth mentioning the output of the PRIPARE project: see generally Nicolás Notario and others, 'PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology', *2015 IEEE Security and Privacy Workshops* (IEEE 2015).

[188] VUB-LSTS, 'D2.2 – Framework for Impact Assessment against RRI - ELSA Requirements' (*PARENT project*, 2016) <https://www.parent-project.eu/wp-content/uploads/D2.2_Framework-for-impact-assessment-against-ELSA-requirements.pdf>.

[189] Boštjan Kežmah and others, 'D3.6 Guidelines for GDPR Compliant User Experience' (*CyberSec4Europe project*, 2020) <https://cybersec4europe.eu/wp-content/uploads/2021/02/D3.6-Guidelines-for-GDPR-compliant-user-experience-Revision-2.0.pdf>.

[190] HR-Recycler project, 'D2.2 – HR-Recycler Impact Assessment Method' (2019) <https://www.hr-recycler.eu/wp-content/uploads/2020/02/D2.2.pdf>.

[191] Nikolaos Ioannidis and others, 'PERSONA Deliverable D3.2: PERSONA Assessment Method (Final Version)' (*PERSONA project*, 2021) <https://cris.vub.be/ws/portalfiles/portal/66227166/PERSONA_D3.2_v2.2_final_clean_PP_download_.pdf>.

[192] Lucio Scudiero and Sebastien Ziegler, 'SynchroniCity D1.4 Privacy by Design Methodology & PIA' (2017).

[193] Alexander Garaga and others, 'D:C-6.2 Prototype for the Data Protection Impact Assessment Tool' (*Cloud Accountability Project (A4Cloud)*, 2014) <http://cloudaccountability.eu/sites/default/files/D36.2 Prototype for the data protection impact assessment tool.pdf>. See also Alnemr and others (n 72); David Tancock, Siani Pearson and Andrew Charlesworth, 'A Privacy Impact Assessment Tool for Cloud Computing' in Siani Pearson and George Yee (eds), *Privacy and Security for Cloud Computing* (Springer London 2013). As for TClouds, see Ninja Marnau and others, 'D1.2.4 Cloud Computing – Data Protection Impact Assessment' (*TClouds project*, 2013) <https://tclouds.schunter.org/downloads/deliverables/TC-D1.2.4-Cloud-Computing-Privacy-Impact-Assessment-V1.1-Public.pdf>.

[194] Javier Ruiz and others, 'Deliverable 4.4 Final Report on PESIA' (*VIRT-EU project*, 2019) <https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c3b3de47&appId=PPGMS>.

[195] Michael Friedewald and others, 'Deliverable 4: Final Report — A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies' (*PRESCIENT project*, 2013) <https://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT_deliverable_4_final.pdf>.

privacy and ethical impact assessments, or the SAPIENT project,[196] which developed a surveillance impact assessment manual.

Besides risk assessments, other kinds of (impact) assessments have been developed as parallel or complementary to the DPIA process in an academic setting. An example is De Etische Data Assistent (DEDA),[197] a toolkit[198] developed by the Utrecht Data School of Utrecht University, in collaboration with the Municipality of Utrecht, that is meant to assist data analysts, project managers, and policymakers to identify ethical issues in projects, management, and policy that revolve around data processing. Another example is the Fundamental Rights and Algorithms Impact Assessment (FRAIA) manual, commissioned by the Dutch Ministry of the Interior and developed by Utrecht University to support organisations in making decisions about, and assessing the impact of, the development and deployment of algorithms.[199] Akin to what can be said vis-à-vis the frameworks and methods developed by public authorities,[200] the academic contribution to the development of PIAs, DPIAs, and neighbouring assessments is by no means limited to the European milieu. Although not a PIA nor a DPIA in the strict sense of the term, and while not geared towards EU data protection specifically, another valid example of a sectoral privacy risk assessment model coming from an academic environment is the Harvard Open Data Privacy guide.[201] Open Data Privacy is a remarkable risk/benefit analysis framework targeted at the 'smart city',[202] and specifically meant to help with balancing the potential benefits of open data initiatives with the privacy risks they might bring along.

4.5. Standards

Conceptualising the DPIA as a form of meta-regulation[203] explains the plethora of frameworks, methodologies, guidelines, and templates available to data controllers. The reduction of fragmentation and inhomogeneity, however, is one of the main functions of standards, and of the goals of standard-setting organisations. It is thus not surprising that a small number of PIA- and DPIA-related standards exist.

The ISO/IEC 29134:2017 standard – Guidelines for privacy impact assessment–[204] was published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as an attempt at standardising PIAs. The standard was created by Subcommittee SC 27 (IT Security techniques) of Technical Committee ISO/IEC JTC 1 (Information technology) specifies how the PIA process should be undertaken, and details the structure and content of a PIA report. ISO/IEC 29134:2017 is a horizontal framework: it aims at providing scalable guidance that can be

[196] David Wright and others, 'Surveillance Impact Assessment Manual' (*SAPIENT project*, 2014) <https://publica.fraunhofer.de/eprints/urn_nbn_de_0011-n-3161367.pdf>.

[197] Utrecht Data School, 'De Ethische Data Assistent (DEDA)' <https://dataschool.nl/deda/> accessed 15 July 2022. See also Aline Shakti Franzke, Iris Muis and Mirko Tobias Schäfer, 'Data Ethics Decision Aid (DEDA): A Dialogical Framework for Ethical Inquiry of AI and Data Projects in the Netherlands' [2021] Ethics and Information Technology 1. Another ongoing project by Utrecht Data School –BIAS– aims at developing an approach similar to DEDA but aimed at algorithms, rather than data: see Utrecht Data School, 'Beraadslagingsinstrument Voor Algoritmische Systemen (BIAS)' (2022).

[198] Consisting of a poster for brainstorming sessions, an interactive questionnaire, and a manual.

[199] Janneke Gerards and others, 'Impact Assessment Mensenrechten En Algoritmes' (*Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*, 2021) <https://www.uu.nl/sites/default/files/Rebo-IAMA.pdf>; Janneke Gerards and others, 'Fundamental Rights and Algorithms Impact Assessment (FRAIA)' (*Ministry of the Interior and Kingdom Relations*, 2022) <https://www.government.nl/documents/reports/2021/07/31/impact-assessment-fundamental-rights-and-algorithms>.

[200] While DPIAs are an EU-specific obligation, PIAs are well developed in other jurisdictions as well; indeed, non-EU PIA frameworks formed the basis for the UK ICO's PIA guidelines, the first of their kind in the European milieu. See e.g. Warren and others (n 18); Clarke, 'Privacy Impact Assessment: Its Origins and Development' (n 18); Tancock, Pearson and Charlesworth, 'The Emergence of Privacy Impact Assessments' (n 18).

[201] Green and others (n 77).

[202] Despite not being EU-focused, nor a (strictly speaking) a DPIA methodology, Open Data Privacy is particularly topical vis-à-vis this report's context – methods for assessing privacy and data protection risks and impacts in the "smart city" environment.

[203] See above.

[204] ISO/IEC 29134:2017 Information technology — Security techniques — Guidelines for privacy impact assessment.

applied to initiatives of all types and sizes of organizations, from companies and non-profits to government entities. ISO/IEC 29134:2017 is not specific to DPIAs under the GDPR, but is rather jurisdiction-neutral; regardless, it is one of the DPIA frameworks cited by the A29WP, and the granular knowledge base it provides can readily be integrated with the specificities of EU data protection law in general, and of DPIAs under the GDPR in particular.

Despite being the first horizontal, general PIA standard, ISO/IEC 29134:2017 was not the first attempt at standardising PIAs *tout court*. ISO 22307:2008,[205] prepared by Subcommittee SC 7 (Core banking) of Technical Committee ISO/TC 68 (Financial services), predates ISO/IEC 29134:2017 by almost a decade. ISO 22307:2008 recommends a standardized PIA process to identify and mitigate privacy risks in financial systems. It underlines that privacy and data protection legislation differs from jurisdiction to jurisdiction, and posits that the internationalization of PIAs is critical for global banking and cross-border financial transactions, referring to the 1980 OECD Guidelines on the protection of privacy and transborder flows of personal data as a normative basis for such internationalisation. While ISO 22307:2008 would *prima facie* seem to have a very limited relevance for DPIAs in the "smart city" environment, there has been (at least) one attempt at applying it exactly to that context.[206] Another standardised PIA framework predating ISO/IEC 29134:2017 is CEN 16571:2014.[207] Based on the Privacy and Data Protection Impact Assessment Framework for RFID Applications,[208] the standard aims at enabling a shared European method for undertaking a PIA in the RFID domain, and provides a standardized set of procedures for developing (RFID) PIA reports.

Although –at the time of writing– those are the only PIA or DPIA standards we could find, broadening the scope of the inquiry as to cover standards *adjacent* to the concept of PIA or DPIA would return a higher number of results. Thus, for instance, the ISO/IEC 2700-series, a set of standards containing best practices on information security management, could likely be integrated with PIA or DPIA processes, and so could e.g. ISO/IEC 29100:2011[209] and ISO 31000:2009.[210] The same could be said, *a fortiori*, when broadening the territorial scope of our research, which would lead to consider e.g. the US National Institute of Standards and Technology (NIST) privacy framework,[211] or its risk management one.[212]

4.6. Custom and bespoke templates

A narrative but systematic review of publicly available[213] PIA and DPIA reports has shown both a wide use of publicly available DPIA templates, such as the ICO's one, and a very substantial amount of

[205] ISO 22307:2008 Financial services — Privacy impact assessment. See also JM Ferris, 'The ISO PIA Standard for Financial Services' in David Wright and Paul De Hert (eds), *Privacy Impact Assessment* (Springer 2012).

[206] Yoichi Seto, 'Study on the Application of the Privacy Impact Assessment in Smart City' (2013) 98 Electronics and Communications in Japan 52.

[207] CEN 16571:2014 Information technology - RFID privacy impact assessment process: https://standards.iteh.ai/catalog/standards/cen/68b7d019-56b3-4405-a992-21a6092de18b/en-16571-2014

[208] GS1, 'Privacy and Data Protection Impact Assessment Framework for RFID Applications' (n 144). See also Spiekermann (n 144). GS1 also provides a free online RFID DPIA tool: GS1, 'GS1 EPC/RFID Privacy Impact Assessment Tool' (n 144).

[209] ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework.

[210] ISO 31000:2009 Risk management— Principles and guidelines.

[211] NIST, 'NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0' (2020) <https://doi.org/10.6028/NIST.CSWP.01162020>.

[212] See NIST, 'NIST Risk Management Framework' (2022) <https://csrc.nist.gov/Projects/risk-management/sp800-53-controls> accessed 22 March 2022. Using NIST risk management framework for DPIAs *ex* Art. 35 GDPR has already been suggested in Piotr Foitzik, 'Using NIST's Risk Management Framework to Conduct GDPR-Compliant DPIAs' (*IAPP - The Privacy Advisor*, 2019) <https://iapp.org/news/a/using-nists-risk-management-framework-to-conduct-gdpr-compliant-dpias/> accessed 22 March 2022.

[213] While the DPIA reports we collected and analysed were publicly available on the internet and indexed by search engines, we consider that the report's public availability might not always derive by the will to publish DPIA reports as a best practice, but also by lack of access controls or incorrect robots.txt settings.

custom and bespoke DPIA templates and reports[214] of varying depth and quality. The complexity and thoroughness of the assessment reports examined ranges from outstanding DPIAs[215] to arguably superficial DPIA reports that we see no need to reference. For the purposes of this report, our analysis has led to the following considerations.

First, it appears evident that DPIA templates, tools, and methods help data controllers perform a sound assessment, but they are not a "silver bullet" on their own. The same DPIA templates and guidelines can be used (and have been) used to produce DPIA reports of a starkly different quality. A second point, connected to the first, is that adequate expertise, independence, and resource allocation make or break DPIAs regardless of the documental support available. Indeed a third consideration is that not all projects and (foreseen) processing operations have the same complexity, significance, and potential to impact data subjects, nor their DPIAs (should) require the same amount of overhead and resources.[216]

This leads us to the fact that pursuing a "one size fits all" approach might not be the best course of action, particularly in a domain as complex and multifaceted as modern municipalities are. Cities – regardless of whether "smart" or not– operate, at different levels, across a multitude of different sectors, and engage with a plethora of diverse stakeholders for a very broad array of purposes. It stands to reason that the use of the same DPIA template across the whole municipality would boost consistency and homogeneity, and provide assessors with a vetted baseline that they can follow: DPIA templates are meant to "automatically" support best practices by identifying *ex ante* the 'right' questions to ask.[217] Yet, given the meta-regulatory nature of DPIAs and the vagueness of the requirements *ex* Art. 35 GDPR, adherence to those best practices is not a given, regardless of the quality of the DPIA templates used; hence, clearly defined and formulated acceptability and evaluation criteria might matter more than the adoption of one template or the other. Finally, as testified by the multitude of publicly (co)funded research projects undertaken over the years that attempted at building DPIA frameworks for specific technologies or practices, the specificities of the object of the assessment condition the assessment itself. In other words, an argument can be made against using the same model form to evaluate the data protection risks and impacts of e.g. both a municipal social housing programs and of the use of a particular cloud service provider by the local government.

Moreover, while the importance of PIA and DPIA guidelines, methods, and templates should not be understated, what seems to be most important is whether a DPIA process and the report that comes

[214] Coherently, an EDPS survey notes how "No less than 13 EUIs mention that they have developed specific internal DPIA templates forms, most including additional guidance to controllers […] Other EUIs went even further, developing a specific tool […] a DPIA checklist […] or establishing a specific internal methodology": EDPS, 'EDPS Survey on Data Protection Impact Assessments under Article 39 of the Regulation (Case 2020-0066)' (n 143) 11.

[215] See e.g. Sjoera Nas and Floor Terra, 'DPIA on Microsoft Teams, OneDrive Sharepoint and Azure AD (June 2021) Data Protection Impact Assessment on the Processing of Diagnostic Data' (*SLM Rijk and SURF*, 2022) <https://www.rijksoverheid.nl/documenten/publicaties/2022/02/21/public-dpia-teams-onedrive-sharepoint-and-azure-ad>. See also e.g. Rijksoverheid, 'Data Protection Impact Assessments DPIA's Office 365 ProPlus, Windows 10 Enterprise, Office 365 Online and Mobile Apps' (2019).

[216] See Vandercruysse, Buts and Dooms, 'Economic Costs of the DPIA D.3.1' (n 186); Vandercruysse, Buts and Dooms, 'A Typology of Smart City Services Based on DPIA-Costs D.3.2' (n 186); Vandercruysse, Buts and Dooms, 'Selecting a Data Protection Approach for Procurement of Smart City Services: Matching Policy Feasibility with Intrinsic Service Characteristics D.3.4' (n 186); Vandercruysse, Buts and Dooms, 'A Typology of Smart City Services: The Case of Data Protection Impact Assessment' (n 11).

[217] The value of DPIA templates, particularly when constituted by a checklist where each item is explained with sufficient detail, has already been underlined *inter alia* in an EDPS survey on DPIAs: "Those EUI using a checklist with full text instructions […] including guiding examples and counterexamples, fare best in procuring proof of the controller actually having considered why the processing operation at hand merits a DPIA. This is in particular the case, where the controller is forced to explicitly reason respective box-ticking" – EDPS, 'EDPS Survey on Data Protection Impact Assessments under Article 39 of the Regulation (Case 2020-0066)' (n 143) 9. The survey also highlighted the desire for a homogeneous DPIA framework across the whole EU institutional landscape, rather than within single institutions, and of shared templates, methods, and tools: EDPS, 'EDPS Survey on Data Protection Impact Assessments under Article 39 of the Regulation (Case 2020-0066)' (n 143) 21–22.

from it adhere to the best practices and acceptability criteria that have emerged over the years from the development of the PIA and DPIA experiences. It is indeed apparent how most well-developed PIA and DPIA frameworks and methods share the same core characteristics, and how most collections of best practices, yardsticks, and evaluation criteria developed since the advent of the PIA and the DPIA in the regulatory environment of reference contain the same main elements. Those characteristics and elements should be taken into account, from the outset, regardless of whether an organisation wants to carry out a DPIA, evaluate a DPIA report, choose an existing DPIA framework, or develop its own DPIA method. The following subsections list some of the best practices, yardsticks, and evaluation criteria that have been developed and used over the years to create and evaluate PIA and DPIA methods, guidelines, and reports.

5. Between methods and best practices

The meta-regulatory nature of PIAs in general and DPIAs *ex* Art. 35 GDPR in particular makes it so that it seems quite difficult, if not impossible, to adopt a "one-size-fits-all" approach, particularly when dealing with an environment as complex and multifaceted as the modern (smart) city, where the kinds of processing to be assessed are manifold and ever-growing. Some of the DPIA guidelines we analysed are engineered to be as generic and neutral as possible, and could be used as-is, adapted to the specific kind of processing to be assessed, or supplemented by additional guiding material in cases where the assessment is not straightforward. Other DPIA guidelines have been written with specific kinds of processing in mind, and trade off general applicability for a more targeted kind of guidance.

This research suggests that the decision of which DPIA framework and method to adopt or build should move from the best practices, evaluation criteria, and other kinds of yardsticks (collectively referred to as 'best practices' hereinafter) that have been developed by academia, policy, and practice since the beginning of the PIA/DPIA experience in Europe. The lists of best practices that resulted from our review have very strong similarities with each other: they vary in the level of detail, and in the importance that they give to certain elements of the DPIA process, but their gist is quite homogeneous. Conversely, most of the (higher quality) DPIA methods we examined adhere to the majority of the best practices identified by policy and academic literature. This section thus reports on some of the most referenced, comprehensive, and/or relevant collection of PIA- and DPIA-related best practices available in literature.

5.1 The A29WP Acceptability Criteria

The A29WP, in the development of its DPIA guidelines,[218] has chosen a fairly high-level approach, and does not specify which DPIA methodology should be followed, rather choosing to leave ample room for manoeuvre to data controllers, and to provide references to some of the most commonly used (and widely endorsed) DPIA methodologies. The second annex of the A29WP's DPIA guidelines, however, list the criteria for an acceptable DPIA that emerge from the analysis of the requirements set by Art. 35 GDPR. The table below, adapted from the A29WP's guidelines, reports on the criteria which data controllers can use to assess whether or not a DPIA, or a methodology to carry out a DPIA, complies with the minimum requirements set by the GDPR:

Requirement	Source
○ a systematic description of the processing is provided	Art. 35(7)(a)
○ nature, scope, context and purposes of the processing are taken into account	
○ personal data, recipients and period for which the personal data will be stored are recorded;	

[218] Article 29 Data Protection Working Party, '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' (n 1).

○ 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	Art. 35(8), Recital 90
○ necessity and proportionality are assessed	Art. 35(7)(b)
○ measures envisaged to comply with the Regulation are determined, taking into account:	Art. 35(7)(d), Recital 90
▪ measures contributing to the proportionality and the necessity of the processing on the basis of:	
▪ specified, explicit and legitimate purpose(s)	Art. 5(1)(b)
▪ lawfulness of processing (Article 6);	
▪ adequate, relevant and limited to what is necessary data	Art. 5(1I)
▪ limited storage duration	Art. 5(1)(e)
○ measures contributing to the rights of the data subjects:	
▪ information provided to the data subject	Art. 12, 13, 14
▪ right of access and to data portability	Art. 15, 20
▪ right to rectification and to erasure	Art. 16, 17, 19
▪ right to object and to restriction of processing	Art. 18, 19, 21
▪ relationships with processors	Art. 28
▪ safeguards surrounding international transfer(s)	Chapter V
▪ prior consultation	Art. 36
○ risks to the rights and freedoms of data subjects are managed	Art. 35(7)(c)
○ origin, nature, particularity and severity of the risks are appreciated or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:	cf. Recital 84
▪ 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	
▪ likelihood and severity are estimated	Recital 90
○ measures envisaged to treat those risks are determined	Art. 35(7)(d), Recital 90
○ interested parties are involved:	
○ the advice of the DPO is sought	Art. 35(2)
○ the views of data subjects or their representatives are sought, where appropriate	Art. 35(9)

Table 2: A29WP DPIA acceptability criteria, adapted from Article 29 Working Party (2017)

The A29WP's acceptability criteria should arguably be the starting point both to evaluate the quality and compliance of a DPIA report, and to choose, customise, or build a DPIA methodology, tool, or template. They are, however, very much based on compliance with the legal requirements of Art. 35 of the GDPR, and do not entirely reflect all the facets of an optimal DPIA method, nor all the content and traits of an ideal DPIA report. Other useful lists of best practices, evaluation criteria, and yardsticks that do not focus eminently on compliance have been produced both before and after the GDPR entered into force, and may be used as an effective complement to the A29WP's acceptability criteria.

5.2 Evaluating DPIA reports

The PIAF project published one of the earliest set of criteria indicating the effectiveness of a PIA report.[219] The core criteria used by the PIAF project provide a useful and synthetic list of the elements that should be present in a PIA report. According to the PIAF consortium, a PIA report should:

1. clarify whether the PIA was initiated early enough so that there was still to influence the outcome.
2. identify who conducted the PIA.
3. include a description of the project to be assessed, its purpose and any relevant contextual information.
4. map the information flows.
5. check the project's compliance against relevant legislation.
6. identify the risks to or impacts on privacy.
7. identify solutions or options for avoiding or mitigating the risks.
8. make recommendations.
9. be published on the organisation's website, in a redacted form if necessary.[220]
10. identify what consultation with which stakeholders was undertaken.

The PIAF project recognises that the list is quite concise, and recognised that other criteria could be included.[221] The PIAF consortium's further work refined the criteria outlined above and identified the following steps that an ideal PIA or DPIA process should follow, and that should be accounted for in the report it generates.[222] According to its "Step-by-step guide" to PIA, an optimized PIA process should contain the following key steps:

1. Determine whether a PIA is necessary (threshold analysis).
2. Identify the PIA team and set the team's terms of reference, resources, and time frame.
3. Prepare a PIA plan.
4. Agree on the budget for the PIA.
5. Describe the proposed project to be assessed.
6. Identify stakeholders.
7. Analyse the information flows and other privacy impacts.
8. Consult with stakeholders.
9. Check that the project complies with legislation.
10. Identify risks and possible solutions.
11. Formulate recommendations.
12. Prepare and publish the report, for example, on the organization' s website.
13. Implement the recommendations.
14. Third-party review and/or audit of the PIA.
15. Update the PIA if there are changes in the project.
16. Embed privacy awareness throughout the organization and ensure accountability.

While those criteria were formulated in a general fashion and written before the obligation to carry out a DPIA was introduced in (and specified by) the GDPR, they can still be used to complement the acceptability criteria set by the A29WP, thus providing a more nuanced evaluation framework for DPIA reports. Reports are, however, just the outcome of the (D)PIA process, which is bound to be as good as the framework and method it follows. The following section thus details how to evaluate PIA and DPIA guidance documents, and the frameworks and methods they outline.

[219] Wright and others, 'A Privacy Impact Assessment Framework for Data Protection and Privacy Rights' (n 69) 142. PIAF D3 is rather aimed at policymakers, and would have limited utility in the context of this report.

[220] Not publishing a PIA or DPIA report at all should be an exceptional decision, and adequately motivated.

[221] Wright and others, 'A Privacy Impact Assessment Framework for Data Protection and Privacy Rights' (n 69) 142.

[222] Wright, 'Making Privacy Impact Assessment More Effective' (n 70) 310.

5.3 Evaluating PIA methodologies

An early example of the evaluation of PIA guidance documents is given by Clarke,[223] who, drawing on the literature available at the time and on the author's (pioneering) work on the topic, submitted the following list of criteria and sub-criteria to be considered in the evaluation of the PIA guidelines available.[224] Clarke broadly identifies many major points about PIA and DPIA methodologies, but many of the items it lists are already covered by the text of Art. 35 (e.g. responsibility for the DPIA), or by EU data protection law more generally (e.g. the role of national DPAs).

1. **Status of the Guidance Document**: the guidelines, or rather the organisation adopting them, should clarify whether their adoption is recommended, encouraged, or purely voluntary.
2. **Discoverability of the Guidance Document**: the guidelines should be accessible, available, and actively publicised.
3. **Applicability of the Guidance Document**: the document should be clear about its scope, i.e. the kind and range of activities it applies to.
4. **Responsibility for the PIA**: Clarke argues that (D)PIA guidance "needs to make clear that the responsibility for the conduct of a PIA rests with organizations that sponsor, propose, or perform projects that have the potential to negatively impact privacy";[225] that is already taken care of by Art. 35 of the GDPR, but clarity on the organisational aspects of the DPIA process –beyond the allocation of responsibilities under the GDPR– is definitely beneficial.
5. **Timing of the PIA**: (D)PIAs are to be done before the processing begins, and the guidelines should make clear at (which) stage the DPIA process should start.
6. **Scope of the PIA**: Clarke argues that PIA guidelines should encompass broader dimensions of privacy than just "data privacy"; while the wording used does not reflect the distinction between the right to privacy and data protection as it emerged in EU law,[226] it does go along with the fact that Art. 35 of the GDPR requires an assessment of the impact of the processing on data subjects' rights and freedoms in general. The scope of the guidelines should also be clear vis-à-vis the importance of stakeholder engagement, and provide the reference points of the legislation to be considered.
7. **Stakeholder Engagement**: the documents should provide pointers for *meaningful* stakeholder engagement throughout the whole (D)PIA cycle, from the identification of the relevant stakeholders to the publication of the report.
8. **Orientation**: the guidelines should make clear that PIAs (and DPIAs) are to be thought of as processes, and not as products, and should be focused on finding solutions to the risks foreseen, rather than just on highlighting the problems anticipated.
9. **The PIA Process**: the guidance document considered should structure, detail, and formalise the steps and stages of the (D)PIA process, and delineate the content of an ideal DPIA report.
10. **The Role of the Oversight Agency**: DPIAs do not take place in a regulatory vacuum, and the national DPA is a key stakeholder in the DPIA process –from the publication of the inclusion and exclusion lists *ex* Art. 35(4) and 35(5) to the prior consultation to be carried out in case of residual risk.[227] DPIA guidelines should consider and clarify the DPA's role.

Clarke's criteria might be partly outdated if taken *verbatim* and from an EU perspective, as many of the criteria he submits have been internalised by policymakers and are embodied in Art. 35 GDPR or

[223] Clarke, 'An Evaluation of Privacy Impact Assessment Guidance Documents' (n 58).
[224] Clarke, 'An Evaluation of Privacy Impact Assessment Guidance Documents' (n 58) 113.
[225] Clarke, 'An Evaluation of Privacy Impact Assessment Guidance Documents' (n 58) 113, 114.
[226] On the distinction between privacy and data protection within the EU fundamental rights milieu, see e.g. Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer Law, Governance and Technology Series 2014); Orla Lynskey, 'Deconstructing Data Protection: The "Added-Value" of a Right to Data Protection in the EU Legal Order' (2014) 63 International and Comparative Law Quarterly 569; Aidan Forde, 'The Conceptual Relationship Between Privacy and Data Protection' (2016) 1 Cambridge L. Rev. 135.
[227] Art. 36 GDPR.

highlighted in the A29WP's guidelines and acceptability criteria, but are still a useful baseline, and is easily adaptable to DPIAs under EU law. Wright, still drawing on the experience of the PIAF project, also submitted a list of assessment criteria to be used to evaluate PIA guidance documents,[228] which can be taken into account when choosing, customising, or building a DPIA method. They are the following:

1. Does the PIA guide provide a privacy threshold assessment to determine whether a PIA is necessary?
2. Does it advocate undertaking a PIA for proposed legislation and/or policy as well as projects?
3. Is PIA regarded as a process?
4. Does the PIA guide target both companies as well as governments?
5. Does the PIA address all types of privacy (informational, bodily, territorial, locational, communications)?
6. Is PIA regarded as a form of risk management?
7. Does the PIA guide identify privacy risks?
8. Does the PIA guide contain a set of questions to uncover privacy risks?
9. Does the PIA guide identify possible strategies for mitigating those risks?
10. Does the guide explicitly say that PIA is more than a compliance check?
11. Does the PIA guide identify benefits of undertaking a PIA?
12. Does the PIA guide support consultation with external stakeholders?
13. Does the PIA guide provide a suggested structure for the PIA report?
14. Does the guide say that PIAs should be reviewed and updated throughout the life of a project?
15. Does the PIA guide encourage publication of the PIA report?
16. Does the PIA policy provide for third-party, independent review or audit of the completed PIA report?
17. Is PIA mandated by law, government policy, or must a PIA accompany budget submissions?
18. Do PIA reports have to be signed off by senior management (to foster accountability)?

Yet again, the specificity of DPIAs under EU data protection law and the target of this report renders a few of the criteria outlined by Wright (and by the PIAF project) either outdated, redundant, or somewhat irrelevant. However, the ones that still apply provide for a useful set of benchmarks to evaluate DPIA guidance documents and processes. More recently, Vemou and Karyda[229] derived, through a systematic analysis of the relevant literature, the following set of criteria used to evaluate available (D)PIA methods:

1. Is there a step to determine whether a PIA is necessary (threshold analysis)?
2. Is a specific legal framework used as a reference for defining privacy targets?
3. Does the process assess risks for the company (apart from ones for the individual)?
4. Is structured guidance (e.g. in the form of steps etc.) to assist in risk assessment provided?
5. Is any part of the process supported by automated tools?
6. Are organizational and technical measures to treat risks included/proposed?
7. Are directions for PIA conduction during Information Technology/Systems development included?
8. Is the entity responsible for organizing the PIA project specified?
9. Is guidance on setting up the PIA team provided?
10. Does it involve external stakeholders' consultation during risk assessment?
11. Is guidance on identifying external stakeholders provided?
12. Is the entity responsible for signing-off of the PIA report specified?

[228] Wright, 'Making Privacy Impact Assessment More Effective' (n 70) 308. Similar criteria are used in David Wright, Rachel Finn and Rowena Rodrigues, 'A Comparative Analysis of Privacy Impact Assessment in Six Countries' (2013) 9 Journal of Contemporary European Research.

[229] Konstantina Vemou and Maria Karyda, 'Evaluating Privacy Impact Assessment Methods: Guidelines and Best Practice' (2019) 28 Information & Computer Security; Konstantina Vemou and Maria Karyda, 'An Evaluation Framework for Privacy Impact Assessment Methods', *MCIS 2018 Proceedings* (2018).

13. Is an external evaluation/audit of the PIA report required?
14. Is publication of the PIA report to inform external stakeholders provisioned?
15. Is the owner of residual risks specified?
16. Are periodical reviews provisioned? Are revision thresholds defined?
17. Is a PIA report template proposed? Which are its contents?

To a varying level of detail, all the literature examined lists roughly the same requirements when enucleating and enumerating the *desiderata* of PIA and DPIA methods and guidelines. Moreover, although the PIA/DPIA process and the report it generates are not identical concepts, and should be kept conceptually distinct, the criteria that have been proposed to evaluate a PIA or DPIA report can be easily adapted to the evaluation of a PIA or DPIA process, and *vice versa*.

5.4 PIA Evaluation and Grading System (PEGS)

To date, this report found that the most comprehensive and granular set of benchmarks according to which to evaluate PIA (and DPIA) methods and reports is the "PIA Evaluation and Grading System" (PEGS) proposed by Wadhwa and Rodrigues.[230] PEGS is meant to improve the PIA process through the provision of means of evaluating and grading PIA reports, methods, and templates; it also provides a common basis for their comparison, facilitating their selection by data controllers. PEGS is meant to be adaptable, to respond to the plasticity of the (D)PIA process, and is based on a checklist approach combined with the possibility to specify the assessor's answer through a ''scope for improvement'' blank field. The table below reproduces Wadhwa and Rodrigues's PEGS.[231]

Evaluation criteria	Specification
1. Clarification of early initiation	Was the PIA initiated early enough to influence project design?
	Does the PIA report state whether the PIA was initiated early?
	Does the PIA report outline how the PIA influenced project design?
2. Identification of who conducted PIA	Does the PIA report identify who conducted the PIA and their expertise/experience in PIA conduct?
	Does the PIA report identify when the PIA was conducted?
	Does the PIA report identify its target audience (i.e. for whom it was prepared)?
	Does the PIA report provide contact details for further information in relation to the PIA?
	Does the PIA outline/document the PIA process? Does the PIA report outline what guidance it followed?
	Does the PIA report state who approves it? Does the PIA outline a post-implementation review/audit process?
3. Project description, purpose and relevant contextual information	Does the report sufficiently describe the project being assessed and provide relevant contextual information (such as business rationale, project scope, or relevant social, economic or technological considerations)?
	Does the report describe the purpose and objectives of the project?

[230] Kush Wadhwa and Rowena Rodrigues, 'Evaluating Privacy Impact Assessments' (2013) 26 Innovation: The European Journal of Social Science Research 161.
[231] Wadhwa and Rodrigues (n 230) 170.

4. Information flow mapping	Does the PIA map the information flows? (i.e. how information is to be collected, used, stored, secured and distributed and to whom and how long the data is to be retained)
5. Legislative compliance checks	Has all law relevant to the project been surveyed and the project checked for compliance?
6. Identification of privacy risks and impacts	Does the PIA assess risks to data privacy?
	Does the PIA assess and indicate the level of risks to privacy of the person?
	Does the PIA assess and indicate the level of risks to personal behaviour?
	Does the PIA assess and indicate the level of risks to personal communications?
	Does the PIA caution project managers and assessors that the risks listed in the PIA guide are not exhaustive?
	Does the PIA report make provisions to address issues arising out of future changes to the project?
	Does the PIA analyze the public acceptability of the scheme and its applications?
7. Identification of solutions/options for risk avoidance, mitigation	Does the PIA identify means/solutions for risk avoidance?
	Does the PIA identify means/solutions for risk mitigation?
8. Recommendations	Does the PIA make recommendations?
	Are the recommendations accompanied by timeframes for implementation?
	Have the recommendations been implemented/incorporated in project design?
9. Publication	Has the PIA report/executive summary/edited version been published?
	If the PIA report is not published, has an explanation to that effect been made public?
10. Identification of stakeholder consultation	Have stakeholders been consulted as part of the PIA process? Was the consultation adequate (representative of relevant interests)?
	Did stakeholders have the chance to provide information and comment?
	Does the PIA report document the stakeholder involvement and engagement process?
	Does the PIA incorporate stakeholder engagement throughout the project life cycle?

Table 3: PIA Evaluation and Grading System (PEGS), adapted from Wadhwa and Rodrigues (2013)

5.4.1 A note on DPIA tools evaluation yardsticks

In developing PEGS, Wadhwa and Rodrigues's paper[232] moves from the evaluation of a small number of PIA software tools. This report notes how the offer of (D)PIA software has increased considerably over the past years, particularly in the business space. Although commercial software is out of the scope of this report, it seems opportune to highlight the yardsticks the authors used to carry out a rough assessment of the DPIA software they considered, which are the following:

[232] Wadhwa and Rodrigues (n 230).

1. **Operational usability**: Is the tool itself simple and intuitive to use with a minimum need for training?
2. **Contextual usability**: Are the questions asked/examined when using the tool easy to understand?
3. **Applicability**: Is the tool equally applicable to a broad range of applications and technologies?
4. **Thoroughness**: Are the questions examined in using the tool sufficiently detailed in scope?
5. **Accessibility**: Is the tool easy to find on the Internet? Is it costly?
6. **Privacy focus**: Is the tool focused only on privacy-related issues, or is it a subset of a larger evaluation process?

Notably, the authors consider the fact that a tool might be focused exclusively on privacy (and data protection) an evaluation criterion to be considered – the only criterion amongst the ones they list that implies a preliminary axiological judgment. On the one hand, focussing on privacy and data protection avoids the dilution of (D)PIAs and their conflation with other neighbouring but different kinds of assessment. On the other hand, the wording of Art. 35 of the GDPR explicitly mandates the consideration of all the rights and freedoms of the data subject, not only privacy and data protection, and there is a strong case to be made for the integration of (D)PIAs within the controller's already existing operating procedures (e.g. risk management processes). This report submits that there is no approach that is right by default, and that the decision on whether to consider DPIAs in isolation or to integrate them with other risk assessment processes depends on the needs and characteristics of the controller and its organisation.

5.5 DPIA best practices for cities

With regard to DPIA best practices for (smart) cities specifically, we highlight the SPECTRE project's deliverable D2.1, "Mapping DPIA (Best) Practices in Smart Cities".[233] On the basis of a systematic literature review, and with a view to finding which DPIA approaches are most applicable for fostering data protection in cities, the SPECTRE project provided a short list of recommendations specifically tuned towards personal data protection in the municipal context. The table below reproduces the best practices identified by the SPECTRE project.

Theme	Best practice
Smart City (projects)	Training, awareness, literacy and knowledge are most decisive for data protection. These are not only preconditions for a good (D)PIA. They will also prevent issues before they occur or become acknowledged through a (D)PIA.
	Transparency, good communication with stakeholders and effective engagement strategies are key to successful data protection in smart city projects. Although this requires efforts, it is paid-off by higher acceptance and trust of citizens, or by not wasting money when realising that a project is not necessary.
	Data protection and privacy policies are required also for smart cities. They must be consistent, accessible and understandable.
	Communication about privacy and data protection can be more creative than just privacy notices in public space (just-in-time push notifications, illustrations, visualizations...)
	Interdisciplinary networks of stakeholders (e.g. a privacy committee) can be a great and inclusive way of fostering collaborative data protection in the smart city.
	A privacy angle can be more applicable than data protection for the complex context of the smart city as it is more comprehensive. This is certainly the case from the legal point

[233] Breuer, Heyman and Pierson (n 186).

	of view. Data protection, as put forward by the GDPR, can be seen as a means to achieve privacy.
Data Protection Experts	Standardisations are required regarding processes, guidelines and best practices. This will help to make it understandable for different stakeholders, for example for engineers to design by privacy, for administrators of cities to implement DPIAs and reap the benefits.
	This will help different stakeholders to collaborate, because not all speak the same "language".
	The guidelines and lists (on processing operations) provided by DPAs should be enriched through ways to include multi-criteria risk-analysis. This could also consider ethical and social consequences of data processing where possible, but in a standardised and understandable way for different actors.
	Find ways to include perceptions of risk in such multi-criteria risk-analysis.
Assessors	Do not regard the GDPR and DPIAs as a problem for your organisation, but as a way of discovering inefficiencies and shortcomings that is beneficial to the organisation.
	DPIAs can be instrumentalised as means of generating trust and establishing accountability.
	A (D)PIA must be clearly defined in terms of its purposes and its objectives. In that way, they are concrete and specific, not like conflated conceptualisations of the methodology. This can also help to overcome the tensions between the timing of (D)PIAs put forward by many and technological development (or innovation).
	Purposes and objectives of a (D)PIA must be realistic, considering budget and time constraints that apply in the real world.
	Define what risks your organisation is assessing, and why. Be transparent about it.
	Choose and adapt the approach (whether DPIA or something else) to your specific context. Lists of questions are arguably more conductive than checklists to satisfy all the requirements attached to a DPIA.
	Participation in defining risks together with different stakeholders can add highly valuable input. But it is also challenging to conciliate heterogeneous interests, emotions etc.
	Participation is not only about including the public; participation can be external and internal. Organisation-internal participation is arguably most important.
	When turning to participation, be sure what you want to reach with it and how. Carefully consider which groups to include, which stakeholders and interests to address. An engagement and communication strategy are necessary.
	Participation can seem as a whitewashing exercise rather than earnest efforts to include different opinions if not done properly. The costs and efforts can be too high.

Table 4: Smart City DPIA best practices, adapted from SPECTRE D2.2.

Unsurprisingly, given the multiplicity and variety of areas in which cities and the local government is active, the best practices that the SPECTRE project identified with respect to (smart) cities specifically are extremely resemblant, if not identical, to the best practices an assessor would (or should) follow with respect to DPIAs and, to a large extent, to impact assessments in general.

5.6 Impact Assessment best practices into DPIA best practices

At a higher level of abstraction, we hold that the best practices applicable to impact assessments in general are applicable to DPIA in particular, *a fortiori* given the lower degree of maturity of DPIAs as compared to other (older and more established) kinds of impact assessment. In this respect, a synthetic but comprehensive list of best practices to be followed when carrying out an impact assessment (and thus not just a DPIA) have been submitted by the Vrije Universiteit Brussel's d.pia.lab.[234]

Building on a comparative analysis of impact assessments in multiple areas (e.g. environmental impact assessments, social impact assessments), the authors listed the best practices for a generic impact assessment. They did so specifically to evaluate the DPIA requirements *ex* Art. 35 of the GDPR, rather than to adapt those best practices to the DPIA process; regardless, the list is still applicable to DPIAs as-is. Below are the impact assessment best practices identified in the d.pia.lab's Policy Brief No. 1/2017,[235] condensed and adapted to DPIAs and to data protection terminology for conciseness and lexical consistency:

1. A DPIA is a systematic process, undertaken in accordance with an appropriate method, and conducted in a timely manner. It starts early in the lifecycle of a personal data processing operation, ideally at the design stage, and necessarily before the processing begins. It continues throughout the processing's lifecycle and is revisited when needed: DPIAs are "living instruments".
2. DPIAs analyse the projected consequences of personal data processing against the rights and freedoms of the data subjects involved, both at the individual and at the collective level.
3. There is no 'silver bullet' for carrying out DPIAs. What matters is the choice of an appropriate framework and method(s) allowing for the best possible understanding and management of the negative externalities of the envisaged data processing operation.
4. The DPIA process must not only identify, describe, and analyse the possible negative externalities of the personal data processing operation under assessment, but also recommend how to prevent or mitigate them.
5. DPIAs should be understood as "best efforts obligations", to be carried out to the best of the controller's and the DPO's abilities, depending upon the state-of-the-art and to the resources available.[236]
6. The DPIA process requires the controller (and the DPO) to have sufficient knowledge and know-how at their disposal.
7. The DPIA must be documented transparently and in writing; it must be, ideally, publicly available and easily accessible, without prejudice to legitimate secrecy.
8. The DPIA process must be deliberative. External stakeholders must be identified and sought, and their input must be taken into due consideration.
9. The data controller, eventually with the assistance of the DPO, is accountable for the DPIA, and able to demonstrate that the process undertaken is sound.
10. The independence of the assessor must be ensured, both in terms of autonomy and of resources at their disposal.
11. The DPIA process must be structured, sufficiently simple, and not disproportionately burdensome.
12. The DPIA process is (necessarily) adaptive to the characteristics of the personal data processing operation(s) under assessment and of the data controller's organisation: one size does not fit all.

[234] Kloza and others, 'Data Protection Impact Assessments in the European Union. Complementing the New Legal Framework towards a More Robust Protection of Individuals' (n 69).

[235] Kloza and others, 'Data Protection Impact Assessments in the European Union. Complementing the New Legal Framework towards a More Robust Protection of Individuals' (n 69) 2–3.

[236] On the topic, see Vandercruysse, Buts and Dooms, 'Economic Costs of the DPIA D.3.1' (n 186); Vandercruysse, Buts and Dooms, 'A Typology of Smart City Services: The Case of Data Protection Impact Assessment' (n 11).

13. The DPIA process must be inclusive: as many stakeholders, perspectives, societal concerns as possible should be considered by the assessor. It is based upon both expert knowledge and the layperson's opinion, elicited by encouraging public participation.
14. DPIAs are receptive and evolutive; methods and the processes must be regularly developed and adapted.
15. DPIAs require a supportive environment, both in terms of executive support and of cooperation among internal stakeholders.

It should be noted that the best practices above, adapted from the d.pia.lab's Policy Brief No. 1/2017 to be GDPR-specific, go well beyond the minimum requirements set by Art. 35 of the GDPR, and should be read as set of recommendations complementing Art. 35 of the GDPR, and operationalising its requirements. The best practices listed by the d.pia.lab's Policy Brief No. 1/2017 constitute,[237] with respects to DPIAs as mandated by the GDPR, arguably the most coherent and well-developed set of recommendations reviewed by this report, and achieve a remarkable balance between detail and simplicity.

6. DPIAs in practice: user analysis

This section presents the second phase of the research, the user analysis. This phase had two goals: 1) to provide additional empirical data to complement the results of the desk research of the first phase of the research and 2) to obtain a better insight in DPOs' experiences with DPIAs, including challenges and best practices, how the DPIA process looks like on the ground, and how available guidelines, methodologies, and templates are being used by the respondents.

After providing more information about the methodology followed, this section addresses the analysis of the survey and interviews, with reference to the templates and tools used, the risk categories considered, and the experiences in conducting DPIAs for (smart) video surveillance, followed by discussion of the challenges and best practices that came up in the interviews.

6.1 Methodology

To triangulate the findings of the doctrinal and documental desk research undertaken, this study also relied on a survey and on a set of follow-up interviews. The goal of the survey was to acquire information from municipalities in the Netherlands and Europe about the templates, models and methodologies used to conduct their DPIAs. The survey was made with the help of Microsoft Forms and consisted out of five open questions (see below) asking about the types of DPIA templates/methodologies used by the respondents. The survey included a description of the research project and a data protection notice. The survey was sent out to 72 official email addresses of data protection officers (DPOs) of municipalities in 13 countries, which were selected amongst the ones available online. The goal was to provide a representative sample of European countries.[238] A reminder was sent two weeks after the initial invitation. In total 14 respondents answered the survey.[239] Ten respondents indicated they were DPOs, one respondent assistant DPO, one respondent compliance manager and one respondent Secretary of the Delegate Committee for Data Protection in the Ministry of Health; a last respondent did not fill in their role. Based on the information provided in question one, representatives of the following seven countries filled in the questionnaire: UK, The Netherlands, Slovenia, Spain, Italy, Germany, and Belgium.

[237] The same can be said for the other two "policy briefs" issued by the d.pia.lab at the time of writing, Policy Brief No. 1/2019 (which lays out the basis for a method for DPIAs under the GDPR) and Policy Brief No. 1/2020 (which outlines a DPIA template).

[238] The Netherlands, Belgium, France, Spain, Italy, Slovenia, Czech Republic, Estonia, Finland, Sweden, Germany, Austria, UK.

[239] Yet, one DPO responded to the email with the survey request indicating that they had no time to fill it in, and another respondent of the survey answered "no" to all questions.

#	Question
1	What is your role in the organisation, what is your disciplinary background, and in which city are you based?
2	Do you use a DPIA methodology, model, or template? • Which one? Please explain
3	Are you using a pre-existing model/template or did you make your own?
4	Do you use software tools to execute a DPIA? • Which tool? Please explain
5	Are the same DPIA methodologies, models, and template used consistently across your organisation?

Table 5: survey questions

The goal of the interviews was to conduct a user analysis and obtain a better insight about how DPIAs are carried out in practice, about the DPIA process in general, and about the DPOs' experiences and best practices. A first tranche of requests was sent to DPO email addresses in the Netherlands, Spain and Germany; a second tranche of invitations was sent to official DPO email addresses from other countries as well. In total invitations were sent to 18 email addresses of municipalities in eight countries,[240] and reminders were sent after 10 days. Five DPOs, one assistant-DPO and a strategic legal expert from four countries responded positively.[241] The interview protocol consisted of nine (sets of) questions, which were drafted based on a discussion with the Amsterdam Privacy Commission. The intention was to conduct semi-structured interviews leaving sufficient room for follow-up questions. Depending on the person, the interviews lasted between 45 minutes and 1 hour and 30 minutes. The questions are reported in the table below.

#	Question
1	Could you state your name, title, and affiliation, and city that you are based?
2	Could you tell a bit about your role in the organization?
3	Do you use a DPIA methodology, model, or template? • Which one? Please explain • Are you using a pre-existing model/template, or did you make your own? • Is it possible to consult the one you use?
4	What does the DPIA process look like in your municipality and what are your main positive and negative experiences conducting them? • Where do you see room for improvement?

[240] The Netherlands, Belgium, France, Spain, Slovenia, Germany, Austria, UK.

[241] The Netherlands, Belgium, Spain, and Germany. One email address provided an error and there was one automatic response stating the email address was only to be used for data access requests. One of the DPOs from Germany who did respond indicated they did not have sufficient knowledge of English to be able to answer questions in an interview. It was suggested to translate the interview questions to German and asked if they could fill it in on paper. The answers were not received in time for the report. Interviews were conducted in English and Dutch in June 2022.

	• Do you involve stakeholders and/or citizens in the DPIA process?
5	What risk factors/categories are taken up in the assessment? • Do you take into account risk factors in relation to other fundamental rights such as non-discrimination and bias, freedom of speech etcetera? • If yes, in what way has this been taken into account in the DPIA? • Have you considered adjusting the DPIA methodology you have been using, adding extra categories/factors? • Have you heard of algorithmic impact assessments and human rights impact assessments, and do you think these can complement the DPIA process?
6	Could you explain in detail in the context of smart video surveillance the process of conducting a DPIA and if there are specific risk factors/categories that are assessed?
7	Which do you consider good or best practices in the way you conduct DPIAs and the way the DPIA is designed?
8	Do you have examples of good or best practices from other cities or DPOs?
9	Do you think that an (automated) DPIA software tool would make the DPIA process more efficient?

Table 6: Interview questions

6.2 Results

This section discusses the results of the survey and of the interviews. To a large extent, the experts interviewed confirmed the insights of the academic and policy literature reviewed and of the analysis of the DPIA reports examined during this research. The discussion also highlighted some complementary considerations vis-à-vis DPIAs on the ground, including a number of challenges and best practices.

6.2.1 Templates and tools used

The experts that responded to the interviews and to the survey indicated that, while carrying out a DPIA, they rely on a wide and varied gamut of guidelines, tools, and templates. Some mentioned documents[242] and tools[243] issued by public authorities, some others referred to guidelines from private organisations,[244] and a number of experts also indicated that they use (or plan to use) commercial products and/or services offered by private companies to carry out DPIAs within their municipality.

Nine respondents of the survey indicated that they use their own DPIA template, developed entirely in-house or based upon a pre-existing template, models or guidelines. Two respondents of the survey indicated using a mix of a pre-existing template and their own. Ten respondents of the survey indicated they do not use a particular software tool to carry out the DPIA, while four indicated that they do. Two interviewees indicated using existing templates and four interviewees used official

[242] I.e. ICO, 'Guide to the General Data Protection Regulation (GDPR)' (2021) <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf>; ICO, 'Sample DPIA Template' (n 92); Rijksoverheid (n 137); AEPD, 'Template For Data Protection Impact Assessment Report (DPIA) For Public Administrations' (n 116); Informacijski pooblaščenec (n 129); Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens (n 71).

[243] Commission Nationale de l'Informatique et des Libertés, 'The Open Source PIA Software Helps to Carry out Data Protection Impact Assessment' (n 63); CCN-CERT (Spanish Government National Cryptologic Center - Computer Security Incident Response Team) (n 123).

[244] I.e. NOREA (n 72).

templates that were adjusted to their needs. Two interviewees indicated using two templates depending on what kind of project. Different formats are used for the templates: there are templates in Word, in Excel, in online forms.

One of the experts interviewed underlined, in particular, that a template that is designed as a check-box exercise did not really seem to work in their organisation. According to this expert by rephrasing and reformatting the assessment from a check box exercise, making it more detailed and 'scientific' and leaving more room to go into detail about specific issues makes sure that the privacy officers deal with all aspects.

6.2.2 Risk categories

Question four of the interview protocol asked about the risk categories or profiles considered in the templates and guidelines used by the interviewees and their organisations, and whether they amended them or built their own risk catalogue. As stated above, four interviewees indicated using an adjusted template, and two used unmodified official templates. Only one of the experts interviewed indicated that they are using a template that is divided into a general section and a more specific section based on the sector that is being looked at (e.g. cameras, health data…), and customize the template on the basis of the risks to the rights that might be interfered with the most by the kind of processing assessed. All the other experts interviewed used a standard template for all sectors or projects. One of the interviewees remarked that the template of the Flemish DPA[245] was very good for the legal data protection categories but was not considered sufficient when it comes to information security categories, and the CNIL output was much better in that respect.

Most interviewees indicated that no risk categories were specifically included in the DPIA guidelines/templates to address specific human rights other than data protection, bias, or algorithms. Most of the respondents did indicate that even though the DPIA guidelines/templates did not identify those specific risk profiles/categories, when relevant they were regardless considered when carrying out the DPIA. In response to the question of adding more risk categories or profiles to do with fundamental rights or bias an interviewee explains that the nature of data processing often does not require them to go that far: *"The risks are not that broad or that far-reaching; they are really related to the specific data processing and they are more likely to be related to the information security aspects or at a time when there are questions about the lawfulness of the data processing, certain categories of personal data about which you might have doubts as to whether they are lawful, and following on from that the issue of proportionality, you have to see the risks in that, so they are often practical in nature. You also see that departments get no further than this kind of practical risk approach."*

There was some support from the experts for adding categories from human rights and algorithmic impact assessments or doing separate impact assessments in addition to the DPIA, however, there were some doubts about the feasibility of the time this would take. One expert commented that they would welcome separate algorithmic and human rights impact assessments in parallel with the DPIA,[246] if there were sufficient resources to conduct them. There is no consensus amongst the experts about if and how algorithmic and human rights impact assessments should be implemented. Some experts indicated that these should be separate assessments, while others argue that all these assessments should be integrated into one document. According to one expert in response to this issue: "*a lot of applications contain some form of an algorithm and that is going to play an increasingly important role so I would certainly not see it in isolation from each other.*"

[245] Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens (n 71).

[246] E.g. Ruiz and others (n 194); Utrecht Data School, 'De Ethische Data Assistent (DEDA)' (n 197); Gerards and others, 'Impact Assessment Mensenrechten En Algoritmes' (n 199); Mantelero and Esposito (n 56).

Most of the experts interviewed indicated that the DPIA guidelines and templates in use in their municipalities do not foresee specific risk categories relating to video surveillance,[247] and claimed that the municipalities they worked for did not use "smart" video surveillance systems. However, exceptionally, one interviewee indicated that their municipality uses a template with a separate section addressing risk factors/categories specifically concerning video surveillance. The interviewee indicated that the reason for this is that a lot of cameras are in use in the municipality, and gave the example of two specific risks occurring with CCTV cameras in particular. The first is a cultural risk, as the cameras have already been in use for 30 years, and there is a culture amongst the older employees that they can do anything they like with the cameras, such as zooming in on people. A second CCTV-related risk mentioned seemingly pertains to either purpose/function creep or to issues in complying with the purpose limitation[248] principle: according to the interviewee, in contrast to the use of images for security purposes, the use of camera images for other purposes, such as e.g. train traffic control, is hardly regulated, and it is often not straightforward to justify or explain why they are being used and the information they process.

Other municipalities do not use specific risk categories or profiles in the context of (smart) video surveillance. One expert indicated that cameras are seen as a solution for everything and are being pushed by the central government whereby the DPO is asked to only focus on narrow GDPR compliance without room for ethical questions. In contrast, other experts indicated that city councils were very concerned and critical about new smart video surveillance developments.

6.2.3 Challenges to DPIAs on the ground

The challenges identified during the interviews essentially reflect the best practices recognised during the doctrinal and documental research above. The ones mentioned the most pertain, on the one hand, to the quality of the DPIA guidelines and templates available, and on the other hand to organisational issues broader than the DPIA process itself.

Resistance, political pressure, and procurement issues

Most experts indicate that there is a significant resistance towards conducting DPIAs, and to the GDPR in general. It is often considered a burden, and people do not understand why it is important. According to one expert: "*People are reluctant towards the GDPR, it is considered a burden, a documentation procedure that does not provide added value… and even though we advised to carry it out, sometimes the DPIA is not conducted, is done half-heartedly or drags on for a long time."*

Two interviewees indicated that there is a significant pressure from the central government to implement certain technologies which has an impact on the DPIA process. Projects in cities are often politically motivated: cities are seen as test cases and there is a big push for digitization from the government, with the result that ethical and data protection issues are seen as obstacles for innovation. This has an impact on the way DPIAs are conducted and projects assessed.

Two experts indicated that the public procurement process and laws make it difficult to choose the provider who is the strongest in terms of data protection and human rights. One expert indicated that this is because of the strong anti-corruption law in the country. "*It is so strong that it does not give us the tools to choose the best contractor in terms of human rights in terms of sustainability. And this is difficult. It's quite difficult to play with. You know, I'm very forced to choose the provider … that is the cheapest one … and sometimes the cheapest is not the strongest in terms of rights defending.*"

Expertise, legal jargon, and customisation

[247] Conversely, as mentioned above, the UK ICO, jointly with the Surveillance Camera Commissioner, issued DPIA guidelines and templates specifically for CCTV surveillance: ICO and Surveillance Camera Commissioner (n 94); ICO and Surveillance Camera Commissioner (n 95).

[248] GDPR, Art. 5(1)(b).

Half of the experts indicated that there is a lack of expertise amongst municipal privacy officers and project leaders and in one municipality this has led to the assistant DPO having to conduct the DPIAs themselves. According to her *"Because there is so much resistance from some people, also from the general population against the GDPR (...) therefore there is also resistance to learn more about it. Because we have made e-learnings, we have made a whole website about GDPR where I then send those project leaders and people who are working on it, yes but do they follow it, I doubt it."* Other experts indicated that the expertise is improving but on the other hand that it is not always easy to find enough staff with the necessary expertise as there is so much work in this area available.

Several experts indicated that the official templates are difficult to use by the people conducting the DPIAs. For instance, an interviewee from the Netherlands submitted that the CNIL software tool was considered too challenging to use by project leaders on account of both the legal jargon used and of the way it was translated to Dutch. Other official government templates were considered to be too difficult, elaborate, and time-intensive to use, and this was the main reason to adjust them. Templates have been adjusted by rephrasing the questions and language and making the assessments significantly shorter, but also for instance by leaving more space to go more in depth about certain risks. According to one interviewee, "*we notice that filling in DPIAs is difficult and project people only very rarely do this themselves. Because we also notice that it is difficult for them, for most people the language use, the GDPR jargon is Chinese, so the process is done together with them. Often this takes several meetings*". The interviewee went on to say that another obstacle is that sometimes the CNIL tool has bugs, and it takes time to learn how to use it, which are all factors that obstacle its adoption. *"If it would be in a Word format or Excel in an easy-to-click format that would already help but there is no budget to develop our own tool."* That is of course not an issue that is limited to the CNIL tool: another expert indicated, for instance, that the NOREA DPIA guidelines[249] were also seen as too time intensive and too complicated for most people to use.

6.2.4 Further DPIA best practices

Many of the best practices identified during the qualitative stage of the research also echo the points of reference listed in the academic and policy literature reviewed in the preceding sections. The experts interviewed submitted, in particular, that either the following approaches have led to positive results, or that they saw their pursuit as a worthy objective.

Increasing awareness, motivation, and accessibility

One of the categories of best practices mentioned by several experts is raising awareness amongst the people conducting and signing off on the DPIAs (project leaders, chief security officers) about the importance of the DPIA process, and making sure people see the DPIA and DPOs themselves as part of the solution to certain privacy and data protection issues meant to improve the quality and efficiency of the projects assessed, rather than as an obstacle to their development. One expert indicated that creating a positive culture for dealing with mistakes, and learning from errors through training and awareness-raising sessions are seen as the best way to increase expertise and motivation. All interviewees indicate that they have invested in e-learning and training sessions both to raise awareness and increase expertise, and to get people to embrace data protection, stimulating intrinsic motivation and spontaneous compliance.

Several experts also indicated that the accessibility of the DPIA methodology or template is very important for the effectiveness of the DPIA process. Official templates are often seen as too time-intensive, too complicated and with too much legal jargon. Therefore, to remove the threshold for people to conduct the DPIAs the templates need to be "*readable by the specialist departments that do not deal with privacy issues on a daily basis*." One expert says that he observed that a DPIA template

[249] NOREA (n 72).

he adapted and simplified was becoming commonplace within the organization, and saw it as a success.

Pre-assessment and other kinds of parallel impact assessments

Most of the interviewees indicated that a pre-assessment is carried out to decide if conducting a DPIA is necessary, and see this as a good practice. In three municipalities the pre-assessment is a short checklist assessment based on the criteria proposed in the guidelines provided by the Article 29 Data Protection Working Party.[250]

Most of the experts also indicate that they saw as appropriate adding an ethical assessment to the DPIA process. An inspiration for these ethical assessments has been the *Data Ethics Decision Aid* (DEDA) which was developed by Utrecht Data School in collaboration with the city of Utrecht.[251] Several issues that are taken up in an algorithmic impact assessment such as bias are also taken up in the DEDA. In some municipalities the ethical assessment is used as a pre-assessment in others it is conducted in tandem with the DPIA. One expert indicated that they had significantly shortened the DEDA. In another municipality an adjusted version of the DEDA has been developed which is also inspired by values identified by the Rathenau Institute.[252] In general, the original version of the DEDA is considered to be too elaborate, too linear and the process was considered too time intensive. According to the DPO "*We have a number of strict principles that we want to articulate in a few pages on the basis of the Rathenau value model, so we can have a sharp discussion with each other whereby the values are fully investigated*." The idea is that, if possible, citizens are involved to strengthen the process even further. Although there is not a lot of motivation to conduct ethical assessments in practice they are being carried out as the advice given by the DPO is binding, and projects will not move forward without the approval of the DPO.

One of the experts indicated support for pairing DPIAs and other kinds of value-laden impact assessments (e.g. algorithmic impact assessments or human rights impact assessment) earlier on in the process, "*at the beginning of the project phase, at the moment when people are thinking about how they want to realise a goal*." This was confirmed by other experts as well. Other interviewees highlighted the fact that it would be better to incorporate the ethical assessment at the same time as the DPIA because, for instance, "*when investigating the value of privacy, reference is often made to the DPIA, but if the DPIA has not yet been carried out, then you can examine all the values and obtain a positive outcome of the assessment, but if you then carry out the DPIA, it may turn out that the legal basis is lacking, in which case the party is cancelled*." In other words, it is not efficient to do the whole ethical assessment if it is unclear if there is a legal basis for processing personal data. Another expert raised the same issue but suggested that the assessment of the legal basis for processing personal data is usually taken up in the pre-assessment to avoid this issue anyhow.

One expert indicated that, apart from a DPIA, they conduct two more impact assessments in tandem: a sustainability and human rights impact assessment, and a business impact assessment. According to the expert "*we have a triple risk analysing. First of all regarding sustainability and human rights. …, this is one part. We also have what we call a compliance risk analysis, which takes care of all kinds of regulations regarding what kind of rights may be in risk mean in terms of the action we take. Not only data protection, also equality rights or you know many other kind of rights and we also have a third kind of risk analysis which is more focused on let's say business processes. Sometimes some activities put in risk our own processes, okay, so we have to balance how to keep the rights of people in all times,*

[250] Article 29 Data Protection Working Party, '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' (n 1).

[251] Utrecht Data School, 'De Ethische Data Assistent (DEDA)' (n 197); Franzke, Muis and Schäfer (n 197).

[252] The values identified by Rathenau Institute are privacy, autonomy, security, human dignity, social justice, power relations, and supervision of the technology: Linda Kool and others, 'Opwaarderen - Borgen van Publieke Waarden in de Digitale Samenleving' (*Rathenau Instituut*, 2017) <https://www.rathenau.nl/sites/default/files/2018-02/Opwaarderen_FINAL.pdf>. The municipality added health as an extra value to this list.

compliance, sustainability, quality, data protections without putting in risk some parts of procedures that we need to give our service." In the context of the sustainability impact assessment process the municipal organization established a sustainability committee including civil society organisations. In addition to the committee surveys are sent out every six months to stakeholders to obtain their views about new projects. This model could also be an inspiration for the DPIA process.

Multidisciplinary approach, stakeholder involvement, and software tools

All experts indicated that discussing the DPIA with the project leaders, other privacy officers, with experts in other disciplines, and with other stakeholders is an essential part of the DPIA process, and a general best practice. Several experts went further by indicating that, setting up a multidisciplinary team – as opposed to just relying on multidisciplinary input – is often necessary to carry out the DPIA for some projects, on account of the diverse expertise required.

One municipality that was interviewed established an ethics commission following a discussion in the city council about the use of algorithms by the government, which got a lot of media attention. The composition of the commission reflects society and "*so not lawyers, we don't want them there at all, but citizens with an affinity with privacy law and especially the ethical aspects that play a role in it*. *(…) The committee can give solicited or unsolicited advice so, for example, our DPO can send a DPIA to the ethics committee to see if they find something of it."* Another expert indicated that would welcome a small ethics committee with citizens and ethics experts who would ask questions such as, for instance, 'what do we want to accomplish as a city?', 'does this fit into the goals of a city?'. However, she did wonder if yet another step in the process would be feasible.

Most of the experts interviewed viewed positively the idea of using software tools to support the DPIA process, particularly with respect to accessible "end-to-end" management software that could support the administrative part of the DPIA process, making it more efficient. One expert indicated that these tools could help smaller municipalities with limited resources to improve their data protection compliance capacity, which is currently very limited. There however seemed to be some scepticism about the possibility for such tools to help with the *content* of the assessment, rather than with the *process*. As one of the interviewees stated in response to having a DPIA software tool, for instance: "*if an algorithm does it for you, a lot of information leaks away into the organisation because then you no longer have people thinking for themselves because the algorithm says it can do it. Is the algorithm really good enough? Does it take into account all the aspects? You come across things that we just come across spontaneously in a conversation, sometimes during the conversation you come across things like, hey wait a minute, here comes an aspect, we haven't thought of that yet, how does that work exactly?"* In other words, the unwritten knowledge, 'unexpected factors', serendipitous discussions, and stakeholder engagement that can come up during the DPIA process might get lost with software solutions that reduce human involvement.

Both DPIA methods and reports should be 'living documents'

All experts indicated that regularly updating the DPIA of a given process and its report is seen as a best practice. However, not all experts indicated that a procedure was in place to do this in their organisation. Two experts indicated that the DPIA would be reassessed whenever there is a change in the personal data processing considered, and one municipality had a procedure in place whereby a reassessment is expected every three years. Although the experts indicated that it is a best practice to regularly update the assessment, and despite it being a legal requirement under the GDPR, an expert argued that in practice the assessments are often seen as something one-off, often end up in a drawer, and are not regularly reassessed.

In contrast with the other experts interviewed, one interviewee claimed that the municipality where they worked was significantly more active in updating its DPIA reports, and saw them as living documents that needs to be adjusted regularly. The interviewee explained that they "*have a procedure which says that minimum once per year, they have to make a risk analysis. This is the* *minimum but the reality is that I actualize these every three or four months. You know we see we have a lot of information: terabytes of images in our system and … with all those problems regarding cybersecurity where cameras are a main objective of hackers, we would like to get in control, to get control for them. We are always trying to protect them in a very stronger and stronger way. So we have a procedure, but we are keeping it even more often that what it says*."

Two interviewees also indicated that they regularly update the DPIA guidelines/template that they use whenever new risks and issues that they had not thought of before arise. When asked about whether new risk factors or categories have been added to the DPIA template/methodology used in her organisation, one interviewee indicated that "*They are simply adjusted as we go along. If we run into sudden things, if It is not quite as clear as it is being read now, then the text will simply be adjusted again.* (…) *Actually, you are constantly in a PDCA*[253] *cycle.*" It is not only the DPIA report –the output of the DPIA process– that needs to be regularly updated, at least where there is a change in the personal data processing, but also the DPIA method itself.

7. Additional considerations on the state of the art in DPIAs

The dialogues through which the research team elicited the questions and concerns of the Amsterdam Privacy Commission highlighted three main sets of inquiries with respect to the state of the art in DPIAs. The first one relates to whether the DPIA template used by the municipality of Amsterdam, which has been translated and enclosed in this report's annexes, matches the best practices identified by the literature reviewed. The second set of inquiries pertains to the advantages and disadvantages of pairing DPIAs with other kinds of assessments (e.g. algorithmic impact assessments, human rights impact assessments, and the likes) that may have a similar scope and a neighbouring subject matter, but that do not necessarily answer to all the requirements set by Art. 35 of the GDPR. The third cluster of considerations relates to the trade-offs between developing particular DPIA methods and templates for specific kinds of personal data processing as opposed to having a single general DPIA template to be used for all processing instances. This section addresses those three groups of queries.

7.1 The municipality of Amsterdam's standard DPIA template

In light of the documental research and of the best practices identified above, the Amsterdam Privacy Commission asked for a review of the standard DPIA template used by the municipality of Amsterdam (see below, Annexes I and II). The DPIA template consists of a detailed and comprehensive set of 73 questions, some of which optional, divided into 13 sections that are titled as follows:

1. General;
2. Actors involved;
3. Lawfulness;
4. Consent;
5. Transparency;
6. Data subject rights;
7. Profiling and automated decision-making;
8. Purpose limitation and proportionality;
9. Data minimisation and subsidiarity;
10. Storage limitation;
11. Security, integrity and confidentiality;
12. Description and assessment of risks;
13. Advice obtained.

[253] Plan Do Check Act Cycle. This is an iterative design and management method used in business for the control and continual improvement of processes and products.

The questions are followed by another table where the assessor enumerates the risks identified, their risk profile (low, medium, or high), the proposed mitigating measures, and the person responsible for their implementation. The template does not contain explicit references to external documents, such as knowledge bases or guidelines, nor to the other steps of the DPIA process to be followed.

The DPIA template's content is clearly compliant with the minimum requirements set by Art. 35 of the GDPR,[254] read in light of the A29WP's acceptability criteria.[255] Its structure and content also suggest that the procedural requirements of the GDPR as interpreted by the A29WP are fulfilled by the City of Amsterdam's DPIA process: the DPIA is supposed to take place before the processing begins, it aims at identifying risks and mitigating them with technical and organisational measures, and identifies the persons responsible for their implementation. The DPIA template also foresees the involvement of the DPO, and provides for the means to avoid redundant DPIAs. Besides the minimum requirements set by Art. 35 of the GDPR, and the A29WP's acceptability criteria, there are however a few best practices identified by academic and policy literature that do not seem to have been addressed in the City of Amsterdam's DPIA method, at least as resulting from the template it uses.[256] While not required by the GDPR *per se*, those best practices would likely strengthen both the DPIA process and its output.

The first set of remarks revolves around steps preliminary to the DPIA itself: from the template, for instance, it is not clear whether there is a pre-assessment (or threshold assessment) stage, where the need to carry out a DPIA is assessed in its own merits. That allows to check, in a more structured manner, whether the processing falls under the categories under Art. 35(3) and (4) of the GDPR[257] or whichever category of processing the municipality of Amsterdam deems as high risk and thus requiring a DPIA. A structured pre-assessment also reduces the margin of error in determining whether a kind of processing does or does not involve personal data, which, on account of the broad interpretation given to the concept,[258] is sometimes not entirely straightforward. Similarly, it is not clear whether the processing's data flows are mapped, e.g. through a flowchart, before the DPIA takes place.

Stakeholder engagement is another aspect of the DPIA process that does not seem to be entirely addressed by the template. While the DPIA model does foresee a section[259] on the advice that can be obtained from DPOs, process holders, the Dutch DPA,[260] and data subjects, there is no indication of a systematic *process* on how to seek that advice, particularly vis-à-vis the data subjects involved; there does not seem to be a role for civil society organisations, either. The publication of the DPIA report, when not outweighed by overriding reasons (e.g. security, intellectual property), is also widely recognised as a best practice. The template used by the municipality of Amsterdam does not appear to be meant for publication, nor is the publishing of the DPIA report (e.g. in a public repository) mentioned anywhere. While not required by the GDPR, external or internal audit might also be an important step in making DPIAs more meaningful, particularly when the kind of processing assessed

[254] I.e. a systematic description of the envisaged processing operations and the purposes of the processing, including the legitimate interest pursued; an assessment of the necessity and proportionality of the processing operations in relation to the purposes; an assessment of the risks to the rights and freedoms of data subjects; and the measures envisaged to address the risks: GDPR, Art. 35(7).

[255] Article 29 Data Protection Working Party, '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' (n 1).

[256] With the caveat that those best practices might not be captured by the template used by the municipality of Amsterdam, but by other steps and documents in the wider DPIA process. In other words, it may be that what seems lacking from the template in itself is taken care of elsewhere.

[257] The template does not seem to refer to the lists provided for by Art. 35(4) and 35(5) of the GDPR either.

[258] See e.g. Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data WP136' (2007); Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 Law, Innovation and Technology 1; Lorenzo Dalla Corte, 'Scoping Personal Data: Towards a Nuanced Interpretation of the Material Scope of EU Data Protection Law' (2019) 10 European Journal of Law and Technology; Sandra Wachter, 'Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR' (2018) 34 Computer Law & Security Review 436.

[259] See section 13 of the DPIA template annexed below.

[260] In the context of prior checking *ex* Art. 36 of the GDPR, supposedly.

is especially complex or consequential. Even if and when auditing the DPIA is not necessary, it would be appropriate to specify a timeframe for its review.

The template, perhaps most importantly, does not explain – either directly or by reference to an external body of knowledge – any of the terminology used, nor the concepts to which it refers. While that is not necessarily an issue, provided that enough resources and expertise are allocated to the DPIA, coupling the template with additional information would stimulate consistency amongst different DPIAs carried out by the municipality of Amsterdam, reduce the degree of subjectivity inherent to this sort of assessment, and avoid some of the minor interpretation issues that may arise from a freehand use of the template. The structure and wording of the City of Amsterdam's template could indeed, lacking a corresponding knowledge base, give rise to interpretation issues that could potentially prejudice the quality of the DPIAs it is used to carry out, depending on the expertise and resources available to the assessor. By way of example, the template refers to the subsidiarity principle rather than to the necessity one, and seems to consider proportionality only in the context of the purpose limitation principle,[261] while the role of the proportionality principle in EU data protection law is much broader than that.[262]

Generally speaking, the template used by the municipality of Amsterdam does not have glaring deficiencies vis-à-vis the other templates and guidelines reviewed, and can certainly be used to produce suitable DPIAs, at least when benchmarked against the requirements set by Art. 35 of the GDPR as clarified by A29WP.[263] Its content and structure does not suggest its conflict with any of the PIA and DPIA best practices identified during our review, either. However, it must be underlined how DPIAs are processes, not products,[264] and thus most of those best practices are process-related (e.g. the publication of the DPIA report, or the independence of the assessor). It is, consequentially, not entirely possible to assess whether they are met or not only by reference to the DPIA template used: the underlying DPIA method is (or should be) broader than that.

Similarly, the development and use of a DPIA template (and, at a broader level, of a DPIA method) by an organisation should also be assessed in light of the actual purpose and objective that the template is meant to serve within that organisation specifically. Standard templates may be used as a way to make the format and content of DPIA reports uniform and comparable with a view to their publication. They could also be thought of as a way to make up for potential lack of expertise in data protection law by providing a detailed blueprint guiding the assessor through a set of core questions that must be answered for the DPIA to be meaningful. A DPIA can be devised as a mere a data protection law compliance exercise, meant to meet only the minimum requirements of Art. 35 of the GDPR, or as an actual change engine, meant to evaluate whether the benefits of a risky personal data processing operation outweigh its negative impacts, and how to achieve an optimal trade-off between the competing rights and freedoms at stake. Whether a DPIA template is fit for purpose thus depends, amongst other things, from the purpose that the template serves vis-à-vis the controller's organisation specifically, and cannot really be assessed in a vacuum.

The City of Amsterdam's DPIA template appears to be, to a large extent, devised as a GDPR compliance tool: in other words, it seems to be meant to assess whether a processing operation is compliant with secondary data protection legislation rather than its impact on data subjects' rights and freedoms. Being open-ended in structure, the DPIA template does not rule out the possibility to address the risks to the rights and freedoms of natural persons that go beyond the ones deriving from the violation of the right to personal data protection. At the same time, it does not explicitly consider other rights that

[261] Art. 5(1)(b) of the GDPR; see also Article 29 Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation WP203' (2013).

[262] See Lorenzo Dalla Corte, 'On Proportionality in the Data Protection Jurisprudence of the CJEU' [2022] International Data Privacy Law.

[263] Article 29 Data Protection Working Party, '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' (n 1).

[264] DPIA *reports* can be seen as products.

might be interfered with by personal data processing, either. It is, in other words, quite granular and comprehensive, and yet simultaneously somewhat constricted in scope, as it is eminently geared towards assessing compliance with secondary data protection law.

These considerations bring forth questions about the opportunity of pairing a DPIA method such as the one used by the City of Amsterdam with other kinds of impact assessments meant to evaluate something different from the impact of the processing on the right to personal data protection.

7.2 Pairing DPIAs and similar assessments

The Amsterdam Privacy Commission noted how other cities, such as for instance the municipality of Utrecht,[265] are combining DPIAs with other kinds of assessments, connected and yet distinct from DPIAs, such as human right impact assessments or ethical impact assessments. The Commission thus wonders about the advantages and disadvantages of this practice, and whether the DPIA processes carried out by the city of Amsterdam could benefit from that approach.

The meta-regulatory nature of the obligation set by Art. 35 of the GDPR[266] makes it flexible and open-ended by default; additionally, DPIAs in the GDPR are an assessment of the impact of the envisaged processing operations on the rights and freedoms of natural persons in general, not only on their right to personal data protection. Pairing DPIAs with other kinds of assessment is clearly not incompatible with the letter of Art. 35 of the GDPR, nor with its spirit. The review above, although focussed almost exclusively on DPIAs, has highlighted how that kind of approach has been sometimes followed on the ground. The risk assessment tool provided to Spanish municipalities by the CNI,[267] for instance, is framed as potentially complementary to the DPIA process, and the French CNIL's PIA and DPIA guidelines were drawn on the basis of the EBIOS risk management methodology[268] – the link between DPIAs and risk management is indeed somewhat established in literature.[269]

Descriptively, one could envision three fashions in which neighbouring assessments could be used vis-à-vis the DPIA process. They could be used to improve it, adding more detail or structure to the DPIA process, by way of example through threat modelling.[270] Neighbouring assessments, such as human rights impact assessments,[271] could also be used to complement the DPIA process by adding a structured way to consider the impact of the processing envisaged on rights and freedoms other than data protection, mitigating the narrow focus on GDPR compliance of certain guidelines and templates. Finally, they could be merely seen as additional assessments that must be carried out when computing (personal) data, and whose process may align with the DPIA for reasons of organisational efficiency.

Pairing DPIAs and other kinds of impact assessment may have its advantages, such as an increased consideration of projects that might present risks to individuals' rights and freedoms, marginal efficiency gains, or the development of a sort of precautionary principle[272] in personal data processing. They might, however, also increase the complexity of the assessment, and the resources and expertise it requires. Risk assessment and threat modelling, for instance, seem to be kinds of assessments that can integrate seamlessly with the DPIA process, albeit at the cost of additional overhead. It does not seem very plausible, however, that issues in carrying out meaningful DPIAs could be solved by other – different – kinds of assessments in parallel.

Ultimately, determining whether the advantages of pairing DPIAs with neighbouring kinds of impact assessment outweigh its disadvantages cannot be done *in abstracto*. The answer to that question

[265] See Utrecht Data School, 'Data Ethics Decision Aid (DEDA)' (n 140); Franzke, Muis and Schäfer (n 197).

[266] See Binns (n 22).

[267] See CCN-CERT (Spanish Government National Cryptologic Center - Computer Security Incident Response Team) (n 123).

[268] Commission Nationale de l'Informatique et des Libertés, 'Privacy Impact Assessment (PIA) Methodology' (n 98).

[269] See Wright and others, 'Privacy Impact Assessment and Risk Management' (n 105); Wright and others, 'Integrating Privacy Impact Assessment in Risk Management' (n 57).

[270] See e.g. Kim Wuyts, 'LINDDUN : A Privacy Threat Analysis Framework' (2014); Wuyts and Joosen (n 184).

[271] See e.g. Mantelero (n 57); Mantelero and Esposito (n 56).

[272] See Luiz Costa, 'Privacy and the Precautionary Principle' (2012) 28 Computer Law & Security Review 14.

depends, amongst other things, from the kind of complementary impact assessment envisioned, from the kind of processing instance to be assessed, and from the objectives pursued by the introduction of the additional assessment vis-à-vis the DPIA. An additional layer to the DPIA process, e.g. through risk assessment of privacy threat modelling, could be an improvement to the DPIA framework employed by a data controller. Assessing the impact of the data processing considered on rights and freedoms other than data protection, e.g. through human rights impact assessments, is still coherent with Art. 35 of the GDPR, which mandates an assessment of the *impact* of the envisaged processing operations *on the protection of personal data*, but also an evaluation of the *likelihood* of the risks they present to all the *rights and freedoms* of the natural persons that may be involved.[273] However, it is not as immediate to see how different assessments that share something with DPIAs at a conceptual level, such as e.g. ethics or social impact assessments, but that serve different purposes, would fit within the obligation of Art. 35 of the GDPR, or improve the quality of a controller's DPIA process.

A DPIA's objective is assessing, where a personal data processing operation may present a high risk to people's rights and freedoms, the impact of that processing on their right to personal data protection. If a data controller's DPIA process has deficiencies that hamper the realisation of that objective, it stands to reason to work towards improving that process, rather than further complicating it by introducing additional assessment layers about e.g. ethics, or the processing's social impact. Conversely, if the data controller's goals go beyond what can reasonably be expected from a DPIA, carrying out other kinds of impact assessment may be a way forward. In other words a deficient DPIA process can hardly be fixed by introducing elements in the assessment that have little to do with data protection law. Likewise, DPIAs are about data protection, and are not meant to evaluate other aspects of the data processing at hand – such as its ethical dimension or its social impact – who seem to belong to the realm of policy, rather than to the one of law.

That is not to say that the impact of the processing on rights and freedoms other than data protection should not be assessed before the processing takes place, nor that it is not important to evaluate *ex ante* the ethical dimension or the social impact of projects and initiatives involving (personal) data processing. Data protection and compliance with the legal requirements of the GDPR is a relatively small fraction of all the potential issues that contemporary urbanities must face, particularly in light of the growing digitalisation of society and the rampant instrumentation and 'datafication' of the built environment. However, assessing the impact of a processing operation on the right to personal data protection can be complex and resource-intensive enough without bloating the DPIA with parallel assessments that, however meaningful on their own, do not necessarily make its process more efficient, or its output more significant.

7.3 Generic and sectoral DPIA methods and templates

The city of Amsterdam currently uses a single generic DPIA template to analyse all kinds of personal data processing operations. The municipality however carries out a broad range of public tasks, such as fraud detection in social welfare, crowd management and control, license plate recognition, and public health-related tasks, particularly after the COVID-19 pandemic. The CPA thus wonders whether it would rather be preferable to develop specific DPIA guidelines, methods, and templates, targeted to specific sectors or categories of personal data processing.

The research above showed how certain kinds of activities involving personal data processing (most notably CCTV surveillance or the provision of healthcare services) have been made object of specific guidelines by both supervisory authorities and other actors.[274] Academic research, particularly in the context of publicly funded or co-funded research projects, has also displayed a considerable amount

[273] See Art. 35(1) of the GDPR.

[274] E.g. ICO and Surveillance Camera Commissioner (n 94); Health Information and Quality Authority, 'Guidance on Privacy Impact Assessment in Health and Social Care Version 2.0' (n 162); GS1, 'Privacy and Data Protection Impact Assessment Framework for RFID Applications' (n 144); Spiekermann (n 144); Alnemr and others (n 72).

of interest towards creating DPIA methods that are targeted towards particular sectors or kinds of processing.[275]

Drafting sector-specific guidelines and templates covering particular kinds of personal data processing is definitely a promising research direction, particularly given the level of maturity reached by the generic DPIA documentation and literature available. It is also a way to further the formalisation of privacy and data protection risks[276] and harms,[277] which would likely improve the state of the art in PIAs and DPIAs more than yet another set of guidelines and templates, particularly given the open-ended nature of the obligation sanctioned by Art. 35 of the GDPR. DPIA guidelines, as much as DPIA reports, are meant to be 'living documents', to be regularly updated as the need arises and the controller's understanding of the processing increases. Still, rephrasing and reworking the same set of DPIA guidelines or writing yet another all-purpose template, given what is already currently available, would arguably lead to a lesser improvement than developing targeted, sectoral DPIA guidelines and knowledge bases.

A good DPIA report is indeed much more reliant on the assessor's resources, independence, and expertise than it is on the template followed. Suitable guidelines and documentation are certainly useful, but cannot entirely make up for structural deficiencies in the DPIA process and method employed by a data controller. Regardless, providing a targeted, sector-specific knowledge base and method could be helpful with respect to the assessment of particularly complex or delicate processing operations, or to reduce the degree of discretion available to the assessor with respect to certain kinds of personal data processing.

8. Conclusions

There are plenty of DPIA guidelines of varying quality and detail available for municipal authorities, either to directly use and customise as needed, or to consider as a basis for the development of their own DPIA framework, some of which have been refined over several years of work and through the lessons learned through other kinds of impact assessment. The meta-regulatory nature of DPIAs under Art. 35 of the GDPR means that there is, by default, an ample room for manoeuvre, so higher-level best practices (such as, at the very least, the A29WP's acceptability criteria) are fundamental to write and validate both DPIA methods and DPIA reports. It also means there is no "silver bullet" nor "one-size-fits-all" approach to be followed to guarantee the quality of a DPIA report, or that employing a particular methodology will bear fruit. That seems particularly true given how many different kinds of processing are carried out in and by cities, how multifaceted local governments are, and the fact that e.g. resource allocation by the controller or the assessor's expertise ultimately condition the carrying out of a DPIA as much as the method chosen.

Guidelines and templates, however targeted and regardless of how well made, only go so far. There is always room of improvement and specification, particularly given the receptive and evolutive nature of DPIAs, and yet this report notes the particularly high degree of homogeneity of basic DPIA best practices outlined by the policy and academic literature available at the time of writing. That might be due to having reached a high level of maturity through the experience gathered through similar kinds of assessment, most notably PIAs, or to a momentary stagnation in the topic's development, but nevertheless, what makes a good DPIA seems to have been clearly outlined by the available doctrine and policy. In that respect, a more promising avenue for further DPIA research and development could perhaps lie in the formalisation of privacy- and data protection-related risks,[278] both in terms of

[275] See section 4.4 above.

[276] As it is done e.g. in Wuyts, Scandariato and Joosen (n 181).

[277] See the ICO's research on privacy and data protection harms: ICO, 'Overview of Data Protection Harms and the ICO's Taxonomy' (2022) <https://ico.org.uk/media/about-the-ico/documents/4020144/overview-of-data-protection-harms-and-the-ico-taxonomy-v1-202204.pdf>; Sam Wood and others, 'Review of Literature Relevant to Data Protection Harms' (2022).

[278] E.g. through tools and methods like LINDDUN LINDDUN.org (n 179); Wuyts, Scandariato and Joosen (n 181).

assessing their likelihood and their impact, and of the harms that might derive from personal data processing. Another fruitful endeavour would be tailoring DPIA best practices, guidelines, or templates to the characteristics and needs of particular data controllers and of their organisations,[279] or to specific types of personal data processing: meta-regulation is, after all, bound to be somewhat plastic, and DPIAs are living instruments. Regardless, the state of the art contains enough material to permit an adequately resourced and motivated data controller to undertake, with the assistance of a DPO with sufficient expertise and independence, a satisfactory DPIA – or at the very least one that complies with the minimum criteria set by EU data protection law.

The surveys and interviews used to triangulate the findings of the documental research carried out confirmed that the prevailing tendency is to use off-the-shelf guidelines, templates, and tools, customising and adapting them to the needs and requirements of the data controller's organisation. This customisation process, and the risk categories or profiles it might introduce in the guidelines and templates used by the data controller, is conditioned by the object of the DPIA and by the purpose of the processing assessed. There is no 'one-size-fits-all' DPIA method that can seamlessly cover all the disparate kinds of personal data processing carried out by contemporary municipalities, which range from straightforward CCTV deployments to complex processing instances in social security matters, nor a complete and exhaustive checklist of the risks and harms that may derive from the processing of personal data.

Both the challenges and the best practices highlighted in the survey and interviews also match what has been reported by the relevant academic and policy literature for well over a decade. The challenges mentioned the most pertain, on the one hand, to the issues in adapting existing guidelines, tools, and templates to the specificities and particularities of the personal data processing instances assessed, and on the other hand to organisational issues that appear to be broader than DPIAs, such as internal resistance to data protection compliance and external pressures towards the adoption and deployment of certain technologies. The best practices emphasised by the interviewees revolve around the data protection expertise and the degree of independence and autonomy that an assessor must necessarily have regardless of the DPIA methodology or template used, to the multi-disciplinary character of 'good' DPIAs, and to the fact that ethics and values should come into play at the early stages of a project, next to the DPIA. The meta-regulatory nature of DPIAs[280] makes it so that both the reports generated after each DPIA, and the guidelines, methods, and templates used to produce them, should be seen as living documents, to be regularly developed, refined, and updated. Software solutions and automation could certainly help vis-à-vis the administrative and organisational aspects of the DPIA process, but it is not apparent how they could be beneficial to its content, which –provided that the minimum requirements set by Article 35 the GDPR are fulfilled– is rather contingent on the resources, expertise, and autonomy of the assessor, and on the characteristics of the kind of personal data processing object of the assessment itself.

[279] See e.g. the work reported in Marco Todde and others, 'Methodology and Workflow to Perform the Data Protection Impact Assessment in Healthcare Information Systems' (2020) 19 Informatics in Medicine Unlocked.

[280] See *supra* and Binns (n 22).

Annex I – City of Amsterdam DPIA template

1	Algemeen
1	Is dit een nieuw proces, of een nieuwe versie van een bestaand proces?
2	Is er een DPIA gedaan voor eerdere versies van dit proces?
3	Is iets veranderd sinds de laatste DPIA is uitgevoerd?
4	Beschrijf het proces en de (voorgenomen) verwerkingsactiviteiten en/of het voorgenomen beleid/regelgeving waarvoor deze DPIA wordt uitgevoerd.
5	Beschrijf eventuele (nieuwe) technologieën voor zover daarvan gebruik wordt gemaakt bij dit proces? Bijvoorbeeld internet of things, wifi tracking of behavioral advertising.
6	Betreft deze DPIA een enkele verwerking, of een reeks verwerkingen met een vergelijkbaar risico?
7	Wat zijn de doelen van de verwerkingen van persoonsgegevens binnen het proces?
8	Beschrijf de (categorieën van) betrokkenen waarvan persoonsgegevens worden verwerkt. Benoem of er sprake is van kwetsbare groepen.
9	Geef aan welke (categorieën van) persoonsgegevens worden verwerkt?
10	Worden er ook bijzondere persoonsgegevens, strafrechtelijke persoonsgegevens en/of BSN verwerkt? Zo ja geef aan welke gegevens.
11	Geef aan op welke gegevensdrager de persoonsgegevens worden opgeslagen (hardware, software, netwerken).
12	Zijn de bewaartermijnen in kaart gebracht? Zo ja, geef aan wat de bewaartermijnen zijn.
13	Van hoeveel individuen worden er (ongeveer) persoonsgegevens verwerkt in het kader van dit proces?

2	Betrokken actoren
14	Zijn alle partijen die in contact komen met de persoonsgegevens in kaart gebracht?
15	Welke interne en externe verantwoordelijken zijn betrokken bij dit proces?
16	Zijn er afspraken gemaakt met andere verantwoordelijken over de verwerking van persoonsgegevens?
17	Zijn er verwerkers betrokken bij het proces? Zo ja, noem de verwerkers.
	.

18	Is er een verwerkersovereenkomst afgesloten met de verwerkers?
19	Zijn er ontvangers betrokken bij dit proces? Zo ja, is er een overeenkomst met de ontvanger?
20	Worden persoonsgegevens doorgegeven naar landen buiten de Europese Unie? Zo ja, geef aan om welke partijen het gaan en welke waarborgen hiervoor zijn genomen.

3	Rechtmatigheid
21	Is van alle verwerkingen in kaart gebracht of een rechtmatige grondslag van toepassing is? Zo ja, geef aan elke rechtmatige grondslag van toepassing is, of welke grondslagen van toepassing zijn. Motiveer waarom die grondslag van toepassing is.
22	Indien de verwerkingsactiviteiten zijn gebaseerd op het uitvoeren van een overeenkomst, geef aan om welke overeenkomst dit gaat en neem zo mogelijk een verwijzing naar de overeenkomst op.
23	Indien de verwerkingsactiviteiten zijn gebaseerd op een wettelijke plicht, geef aan om welke wettelijke plicht dit gaat. Vermeld hierbij het wetsartikel.
24	Indien de verwerkingsactiviteiten zijn gebaseerd op de vitale belangen van de betrokkene, geef aan om welke belangen dit gaat.
25	Indien de verwerkingsactiviteiten zijn gebaseerd op een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen, geef aan om welke taak dit gaat en noem het wetsartikel.
26	Indien de verwerkingsactiviteiten zijn gebaseerd op een gerechtvaardigd belang, geef aan om welk belang dit gaat en beschrijf de afweging die hierbij is gemaakt.
	.
27	Is de verwerking van bijzondere persoonsgegevens, strafrechtelijke persoonsgegevens en/of het BSN toegestaan? Geef aan waarom.

4	Toestemming
28	Indien de verwerkingsactiviteiten zijn gebaseerd op toestemming: is de toestemming vrij, specifiek, op informatie gebaseerd en ondubbelzinnig gegeven door de betrokkene?
29	Is de toestemming gegeven door middel van een duidelijke actieve handeling?
30	Is of wordt bijgehouden hoe en wanneer de betrokkene toestemming heeft gegeven?
31	Heeft de betrokkene de mogelijkheid om toestemming op ieder moment in te trekken en zonder negatieve gevolgen?
32	Omvatten de verwerkingsactiviteiten websites, apps of andere online diensten van de informatie maatschappij gericht op/aangeboden aan kinderen onder de leeftijd van 16 jaar?

33	Wordt toestemming bij de situatie in de vorige vraag gevraagd door de persoon die ouderlijke verantwoordelijkheid voor het kind draagt?

5	Transparantie
34	Indien de persoonsgegevens direct bij de betrokkene worden verzameld; welke informatie wordt ten tijde van de verzameling gecommuniceerd?
35	Indien de persoonsgegevens niet direct bij de betrokkene worden verzameld; welke informatie wordt ten tijde van de verzameling (of ten minste binnen een maand na verkrijging) gecommuniceerd?
36	Is het privacy statement geschreven in duidelijke bewoordingen en makkelijk vindbaar voor de betrokkenen?
37	Indien de verwerking betrekking heeft op een samenwerkingsverband waarbij meerdere verwerkingsverantwoordelijken betrokken zijn, worden de relevante afspraken dan duidelijk gecommuniceerd aan de betrokkenen?

6	Rechten betrokkenen
38	Is bij het proces rekening gehouden met een effectieve uitoefening van het recht op inzage?
39	Is bij het proces rekening gehouden met een effectieve uitoefening van het recht op rectificatie?
40	Is bij het proces rekening gehouden met een effectieve uitoefening van het recht op wissing/verwijdering van persoonsgegevens?
41	Kan worden voldaan aan een verzoek om dataportabiliteit?
42	Is bij het proces rekening gehouden met een effectieve uitoefening van het recht op bezwaar?
43	Is bij het proces rekening gehouden met een effectieve uitoefening van het recht op beperking?
44	Is de kwaliteit van de gegevens gewaarborgd, dat wil zeggen: zijn de gegevens actueel, juist en volledig

7	Profilering en geautomatiseerde besluitvorming
45	Worden er profielen opgesteld van de betrokkenen, al dan niet geanonimiseerd?
46	Indien profielen worden opgesteld, kan het profiel tot uitsluiting of stigmatisering leiden?
47	Is er sprake van geautomatiseerde besluitvorming? Zo ja, op basis van welke grondslag?

8	Doelbinding & Proportionaliteit

48	Worden de persoonsgegevens gebruikt voor een ander doel dan waarvoor zij verzameld zijn?
49	Indien de vorige vraag met 'ja' is beantwoord: is het doel waarvoor de persoonsgegevens verwerkt gaan worden verenigbaar met het oorspronkelijke doel?
50	Worden de persoonsgegevens gebruikt voor een ander doel dat niet specifiek is omschreven?
51	Is sprake van koppeling, verrijking of vergelijking van gegevens uit verschillende bronnen?
52	Is de (voorgenomen) verwerking effectief om het beoogde doel te bereiken? Geef aan waarom.
53	Staat de impact voor de persoonlijke levenssfeer van de betrokkene van de voorgenomen verwerking van persoonsgegevens in redelijke verhouding tot het doel? Geef aan waarom.

9	Dataminimalisatie & Subsidiariteit
54	Kan het proces ook worden gerealiseerd op een manier die minder ingrijpend is voor de impact op de privacy van betrokkenen? Geef aan waarom wel/niet. Geef aan welke alternatieven zijn overwogen om het proces te realiseren op een manier die minder ingrijpend is voor de impact op de privacy van de betrokkenen?
55	Zijn alle persoonsgegevens noodzakelijk om het beoogde doel te bereiken?
56	Hoe is geborgd dat de standaardinstellingen van de betrokken apparatuur of applicaties zodanig zijn dat alleen de persoonsgegevens worden verzameld die noodzakelijk zijn voor het specifieke doel? Geef aan welke maatregelen zijn getroffen.

10	Opslagbeperking
57	Worden de persoonsgegevens verwijderd op het moment dat zij niet meer noodzakelijk voor het bereiken van het doel?
58	Op welke manier wordt gerealiseerd dat de data daadwerkelijk worden verwijderd/geanonimiseerd?
59	Indien geen bewaartermijnen zijn gedefinieerd, zijn er maatregelen genomen om de persoonsgegevens desalniettemin te verwijderen?

11	Beveiliging, integriteit en vertrouwelijkheid
60	Zijn er op basis van de VRA extra maatregelen nodig, naast de BIG maatregelen?
61	Is voor dit proces aangesloten bij een goedgekeurde gedragscode? Zo ja, vermeld de gedragscode.
62	Zijn de persoonsgegevens gepseudonimiseerd waar mogelijk?

63	Zijn de persoonsgegevens versleuteld waar mogelijk?
64	Zijn toegangsmaatregelen genomen waardoor alleen personen toegang hebben tot persoonsgegevens voor zover dat noodzakelijk is voor de uitoefening van hun taak?

12	Beschrijving en beoordeling risico's
65	Omschrijf welke negatieve privacy gevolgen voor betrokkenen mogelijk kunnen optreden bij de uitvoering van dit proces.
66	Hoe groot is de kans dat de omschreven risico's zich voordoen?
67	"Omschrijf het restrisico voor de betrokkenen. Geef aan of dit restrisico hoog is.
	.
68	Omschrijf de voorgestelde maatregelen om het restrisico te mitigeren.

13	Ingewonnen advies
69	Is er advies ingewonnen van de Functionaris Gegevensbescherming (FG) bij het uitvoeren van deze DPIA?
70	Is er advies ingewonnen van de Autoriteit Persoonsgegevens bij het uitvoeren van deze DPIA? Geef aan waarom wel of geen advies is ingewonnen.
71	Indien advies is ingewonnen van de Autoriteit Persoonsgegevens, geef aan op welke manier invulling is gegeven aan dit advies.
72	Is de betrokkenen (of hun vertegenwoordigers) gevraagd om hun visie te geven over de verwerkingsactiviteiten? Geef aan waarom wel/niet.
73	Geef aan op welke manier opvolging is gegeven aan de visie van betrokkenen. Indien geen opvolging is gegeven aan deze visie, motiveer waarom dat niet is gedaan.

Risico's en maatregelen			
Risico's / negatieve gevolgen voor de privacy van betrokkenen	Classificatie risico (hoog, midden, laag)	Voorgestelde maatregelen + actiehouder	Datum gereed

Annex II – City of Amsterdam DPIA template (English working translation)

1	General
1	Is this a new process, or a new version of an existing process?
2	Was a DPIA done for earlier versions of this process?
3	Has anything changed since the last DPIA was conducted?
4	Describe the process and the (intended) processing activities and/or the intended policy/regulations for which this DPIA is conducted.
5	Describe any (new) technologies insofar as they are used in this process. For example internet of things, Wi-Fi tracking, or behavioural advertising.
6	Does this DPIA concern a single processing activity, or a series of processing activities with comparable risk?
7	What are the purposes of the processing of personal data within the process?
8	Describe the (categories of) data subjects whose personal data is processed. State whether there are vulnerable groups.
9	Indicate which (categories of) personal data are processed?
10	Are special categories of personal data, criminal personal data and/or BSN (social security number) also processed? If yes, indicate which personal data.
11	Indicate on which medium the personal data is stored (hardware, software, networks).
12	Have the data retention periods been mapped out? If so, indicate what the data retention periods are.
13	The personal data of how many individuals (approximately) are processed in the context of this process?

2	Actors involved
14	Have all parties that come into contact with the personal data been identified?
15	Which internal and external data controllers are involved in this process?
16	Have contracts been made with the other data controllers regarding the processing of personal data?
17	Are there data processors involved in the process? If so, name the data processors.

18	Has a contract been concluded with the data processors?
19	Are recipients involved in this process? If so, is there an contract with the recipient?
20	Are personal data transferred to countries outside the European Union? If so, indicate which parties are involved and which guarantees have been taken for this.

3	Lawfulness
21	Has it been mapped out for all data processing activities whether a lawful basis applies? If so, please indicate which lawful basis applies, or which bases apply. Justify why that lawful basis applies.
22	If the processing activities are based on the performance of a contract, indicate which contract this concerns and include a reference to the contract if possible.
23	If the processing activities are based on a legal obligation, please indicate which legal obligation this concerns. Mention the article of law.
24	If the processing activities are based on the vital interests of the data subject, indicate which interests this concerns.
25	If the processing activities are based on a task carried out in the public interest or in the exercise of official authority vested in the controller, indicate which task this concerns and mention the article of law.
26	If the processing activities are based on a legitimate interest, indicate which interest this concerns and describe the consideration that has been made in this regard.
27	Is the processing of special categories of personal data, criminal personal data and/or the BSN (social security number) permitted? State why.

4	Consent
28	If the processing activities are based on consent: is the consent freely given, specific, informed and an unambiguous indication given by the data subject?
29	Was the consent given through a clear affirmative act?
30	Is it (being) recorded how and when the data subject has given consent?
31	Does the data subject have the option to withdraw consent at any time and without negative consequences?
32	Do the processing activities include websites, apps or other online information society services aimed at/offered to children under the age of 16?

33	For the situation described in the previous question, is consent requested by the person who has parental responsibility for the child?

5	Transparency
34	If the personal data is collected directly from the data subject; what information is communicated at the time of data collection?
35	If the personal data is not obtained from the data subject; what information is communicated at the time of data collection (or at least within one month after obtaining the personal data)?
36	Is the privacy statement written in clear language and easily accessible to the data subjects?
37	If the processing relates to a joint controllership, are the relevant arrangements clearly communicated to the data subjects?

6	Data subjects rights
38	Has the process taken into account an effective exercise of the right to access?
39	Has the process taken into account an effective exercise of the right to rectification?
40	Has the process taken into account an effective exercise of the right to erasure/deletion of personal data?
41	Can a request for data portability be met?
42	Has the process taken into account an effective exercise of the right to object?
43	Has the process taken into account an effective exercise of the right to restrict processing?
44	Is the quality of the data guaranteed, i.e. are the data up-to-date, accurate and complete?

7	Profiling and automated decision-making
45	Are data subjects being profiled, whether or not they are anonymized?
46	If profiling occurs, can the profile lead to exclusion or stigmatisation?
47	Is there automated decision-making? If so, on what basis?

8	Purpose Limitation & Proportionality
48	Are the personal data used for a purpose other than that for which they were collected?
49	If the previous question is answered with 'yes': is the purpose for which the personal data will be processed compatible with the original purpose?

50	Are the personal data used for another purpose that is not specifically described?
51	Does linking, enriching or comparison of data from different sources occur?
52	Is the (intended) processing activity effective for achieving the intended purpose? State why.
53	Is the impact for the privacy of the data subject of the intended processing activity of personal data in reasonable proportion to the purpose? State why.

9	Data Minimization & Subsidiarity
54	Can the process also be realized in a manner that is less intrusive for the impact on the privacy of data subjects? Indicate why/not. Indicate which alternatives have been considered to realize the process in a way that is less intrusive for the impact on the privacy of the data subjects.
55	Are all personal data necessary to achieve the intended purpose?
56	How is it ensured that the default settings of the equipment or applications concerned are such that only the personal data necessary for the specific purpose are collected? Indicate which measures have been taken.

10	Storage limitation
57	Are the personal data deleted at the moment they are no longer necessary for achieving the purpose?
58	How is it ensured that the data is actually deleted/anonymised?
59	If no retention periods are defined, have measures been taken to nevertheless delete the personal data?

11	Security, Integrity and Confidentiality
60	Are additional measures necessary on the basis of the VRA, in addition to the BIG measures?
61	Is this process covered by an approved code of conduct? If so, state the code of conduct.
62	Are the personal data pseudonymised where possible?
63	Are the personal data encrypted where possible?
64	Have access measures been taken to ensure that only individuals have access to personal data insofar as this is necessary for the performance of their duties?

12	Description and assessment of risks

65	Describe which negative privacy consequences for data subjects could possibly occur when carrying out this process.
66	What is the probability that the risks described will materialize?
67	Describe the residual risk for the data subjects. Indicate whether this residual risk is high.
68	Describe the proposed measures to mitigate the residual risk.

13	Advice obtained
69	Has advice been sought from the Data Protection Officer (DPO) when carrying out this DPIA?
70	Has advice been obtained from the Dutch Data Protection Authority when carrying out this DPIA? Indicate why or why not advice has been sought out.
71	If advice has been obtained from the Dutch Data Protection Authority, please indicate how this advice has been implemented.
72	Have the data subjects (or their representatives) been asked to give their views on the processing activities? Indicate why yes/no.
73	Indicate how the views of the data subjects have been followed up. If this vision has not been followed up, justify why this has not been done.

Risks and measures			
Risks / negative consequences for the privacy of data subjects	Risk classification (**high**, medium, **low**)	Proposed measures + action holder	Date finished

Bibliography

AEPD, 'Checklist for Determining the Formal Adequacy of a DPIA and the Submission of Prior Consultation' <https://www.aepd.es/es/documento/checklist-dpia-submission-prior-consultation.docx> accessed 10 March 2022

——, 'Facilita EMPRENDE' <https://www.aepd.es/en/guias-y-herramientas/tools/facilita-emprende> accessed 10 March 2022

——, 'Facilita RGPD' <https://www.aepd.es/en/guides-and-tools/tools/facilita-rgpd> accessed 10 March 2022

——, 'Gestiona EIPD' <https://gestiona.aepd.es/> accessed 10 March 2022

——, 'Guía Práctica de Análisis de Riesgos En Los Tratamientos de Datos Personales Sujetos Al RGPD' (AEPD 2018)

——, 'Guía Práctica Para Las Evaluaciones de Impacto En La Protección de Los Datos Sujetas Al RGPD' (AEPD 2018)

——, 'Risk Management and Impact Assessment in the Processing of Personal Data' (2021) <https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf>

——, 'Template For Data Protection Impact Assessment Report (DPIA) For Private Sector' (2022) <https://www.aepd.es/es/documento/modelo-informe-EIPD-sector-privado-en.rtf>

——, 'Template For Data Protection Impact Assessment Report (DPIA) For Public Administrations' (2022) <https://www.aepd.es/es/documento/modelo-informe-EIPD-AAPP-en.rtf>

Agencia de Acceso a la Información Pública de Argentina (AAIP) and Unidad Reguladora y de Control de Datos Personales (URCDP), 'Guía de Evaluación de Impacto En La Protección de Datos' (2020) <https://www.argentina.gob.ar/sites/default/files/guia_final.pdf>

Alnemr R and others, 'A Data Protection Impact Assessment Methodology for Cloud' in Bettina Berendt and others (eds), *Lecture Notes in Computer Science* (Springer 2015)

APDCat, 'Data Protection Impact Assessment Tool' <https://apdcat.gencat.cat/en/documentacio/programari/aipd-programari/> accessed 22 March 2022

——, 'Guia Pràctica Avaluació d'impacte Relativa a La Protecció de Dades' (2017) <https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/Guia-Practica-avaluacio-impacte-proteccio-de-dades-2019.pdf>

——, 'Guide Data Protection Impact Assessment' (2017) <https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/DPIA-Guide.pdf>

Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data WP136' (2007)

——, 'Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications WP 175' (2010)

——, 'Opinion 9/2011 on the Revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications WP 180' (2011)

——, 'Opinion 03/2013 on Purpose Limitation WP203' (2013)

——, '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)

——, '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 WP209' (2013)

——, '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' (2017)

Autoriteit Persoongegevens, 'Data Protection Impact Assessment (DPIA)' <https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia> accessed 10 March 2022

Bayley R and others, 'Privacy Impact Assessments: International Study of Their Application and Effects' (UK Information Commissioner's Office 2007)

Bieker F and others, 'A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation' in Stefan Schiffner and others (eds), *Privacy Technologies and Policy. APF 2016.* (Springer 2016)

Binns R, 'Data Protection Impact Assessments: A Meta-Regulatory Approach' (2017) 7 International Data Privacy Law 22

Bitkom, ‘Risk Assessment & Data Protection Impact Assessment Guide’ (2017) <https://www.bitkom.org/Bitkom/Publikationen/Risk-Assessment-Data-Protection-Impact-Assessment.html>

——, ‘Risk Assessment & Datenschutz-Folgenabschätzung Leitfaden’ (2017) <https://www.bitkom.org/Bitkom/Publikationen/Risk-Assessment-Datenschutz-Folgenabschaetzung.html>

Böröcz I, ‘Risk to the Right to the Protection of Personal Data: An Analysis Through the Lenses of Hermagoras’ (2016) 2 European Data Protection Law Review 467

Breuer J, Heyman R and Pierson J, ‘Mapping DPIA (Best) Practices in Smart Cities D 2.1’ (*SPECTRE project*) <https://spectreproject.be/output/downloads-1/mapping-dpia-best-practices-in-smart-cities>

Bundesamt für Sicherheit in der Informationstechnik (BSI), ‘BSI-Standard 100-3: Risk Analysis Based on IT-Grundschutz’ (2008)

CCN-CERT (Spanish Government National Cryptologic Center - Computer Security Incident Response Team), ‘PILAR’ (2022) <https://pilar.ccn-cert.cni.es/index.php/en/> accessed 15 July 2022

Christofi A, ‘Smart Cities and Data Protection Framework in Context’ (2020) SPECTRE Project, Deliverable 1.2

City of Helsinki, ‘Data Protection Impact Assessment’ (2019) <https://www.hel.fi/helsinki/en/administration/information/data-protection/data-protection-impact-assessment> accessed 22 March 2022

Clarke R, ‘A History of Privacy Impact Assessments’ (2004) <http://www.rogerclarke.com/DV/PIAHist.html>

——, ‘Privacy Impact Assessment: Its Origins and Development’ (2009) 25 Computer Law & Security Review 123

——, ‘An Evaluation of Privacy Impact Assessment Guidance Documents’ (2011) 1 International Data Privacy Law 111

Coglianese C and Mendelson E, ‘Meta-Regulation and Self-Regulation’ in Robert Baldwin, Martin Cave and Martin Lodge (eds), *The Oxford Handbook of Regulation* (2010)

Commission Nationale de l’Informatique et des Libertés, ‘Measures for the Privacy Risk Treatment’ (2012)

——, ‘Methodology for Privacy Risk Management’ (CNIL 2012)

——, ‘Privacy Impact Assessment (PIA) Application to Connected Objects’ (CNIL 2018)

——, ‘Privacy Impact Assessment (PIA) Knowledge Bases’ (CNIL 2018)

——, ‘Privacy Impact Assessment (PIA) Methodology’ (CNIL 2018)

——, ‘Privacy Impact Assessment (PIA) Templates’ (CNIL 2018)

——, ‘The Open Source PIA Software Helps to Carry out Data Protection Impact Assessment’ (2021) <cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment> accessed 15 July 2022

Conference of the Independent Data Protection Authorities, ‘The Standard Data Protection Model: A Concept for Inspection and Consultation on the Basis of Unified Protection Goals’ (2016)

——, ‘Das Standard Datenschutzmodell Eine Methode Zur Datenschutzberatung Und -Prüfung Auf Der Basis Einheitlicher Gewährleistungsziele’ (2020)

——, ‘The Standard Data Protection Model – A Method for Data Protection Advising and Controlling on the Basis of Uniform Protection Goals Version 2.0b’ (2020)

Costa L, ‘Privacy and the Precautionary Principle’ (2012) 28 Computer Law & Security Review 14

Dalla Corte L, ‘Scoping Personal Data: Towards a Nuanced Interpretation of the Material Scope of EU Data Protection Law’ (2019) 10 European Journal of Law and Technology

——, ‘On Proportionality in the Data Protection Jurisprudence of the CJEU’ [2022] International Data Privacy Law

Danezis G and others, ‘Privacy and Data Protection by Design - from Policy to Engineering’ (European Union Agency for Network and Information Security 2014)

Data Protection Commission, *Guidance Note: Guide to Data Protection Impact Assessments (DPIAs)* (Data Protection Commission / An Coimisiún um Chosaint Sonraí 2018)

——, *List of Types of Data Processing Operations Which Require a Data Protection Impact Assessment* (Data Protection Commission / An Coimisiún um Chosaint Sonraí 2018)

Datatilsynet and Justitsministereit, ‘Konsekvensanalyse’ (2018)

De Hert P, ‘A Human Rights Perspective on Privacy and Data Protection Impact Assessments’ in Paul De Hert and David Wright (eds), *Privacy Impact Assessment* (Springer 2012)

De Hert P, Kloza D and Wright D, 'Recommendations for a Privacy Impact Assessment Framework for the European Union' (2012) <https://piafproject.files.wordpress.com/2018/03/piaf_d3_final.pdf>

De 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 & Security Review 130

——, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 Computer Law & Security Review 179

De SJ and Le Métayer D, 'PRIAM: A Privacy Risk Analysis Methodology' (Giovanni Livraga and others eds, *INRIA Research Report*, 2016) 221 <https://hal.inria.fr/hal-01302541/file/RR-8876.pdf>

DeNardis L, *The Internet in Everything* (Yale University Press 2020)

Deng M and others, 'A Privacy Threat Analysis Framework: Supporting the Elicitation and Fulfillment of Privacy Requirements' (2011) 16 Requirements Engineering 3

EDPS, 'Opinion of the European Data Protection Supervisor on the Commission Recommendation on Preparations for the Roll-out of Smart Metering Systems' (2012)

——, 'Accountability on the Ground: Guidance on Documenting Processing Operations for EU Institutions, Bodies and Agencies Summary' (2019)

——, 'Accountability on the Ground Part I: Records, Registers and When to Do Data Protection Impact Assessments' (2019)

——, 'Accountability on the Ground Part II: Data Protection Impact Assessments & Prior Consultation' (2019)

——, 'Decision of the European Data Protection Supervisor of 16 July 2019 on DPIA Lists Issued Under Articles 39(4) And (5) of Regulation (EU) 2018/1725' (2019) <https://edps.europa.eu/data-protection/our-work/publications/guidelines/data-protection-impact-assessment-list_en>

——, 'EDPS Survey on Data Protection Impact Assessments under Article 39 of the Regulation (Case 2020-0066)' (2020)

Edwards L, 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective' (2016) 2 European Data Protection Law Review

ENISA, 'Guidelines for SMEs on the Security of Personal Data Processing' (ENISA 2017)

——, 'Handbook on Security of Personal Data Processing' (ENISA 2018)

Esteves AM, Franks D and Vanclay F, 'Social Impact Assessment: The State of the Art' (2012) 30 Impact Assessment and Project Appraisal 34

Ferris JM, 'The ISO PIA Standard for Financial Services' in David Wright and Paul De Hert (eds), *Privacy Impact Assessment* (Springer 2012)

Finch K and Tene O, 'Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town' (2013) 41 Fordham Urb. LJ 1581

Foitzik P, 'Using NIST's Risk Management Framework to Conduct GDPR-Compliant DPIAs' (*IAPP - The Privacy Advisor*, 2019) <https://iapp.org/news/a/using-nists-risk-management-framework-to-conduct-gdpr-compliant-dpias/> accessed 22 March 2022

Forde A, 'The Conceptual Relationship Between Privacy and Data Protection' (2016) 1 Cambridge L. Rev. 135

Franzke AS, Muis I and Schäfer MT, 'Data Ethics Decision Aid (DEDA): A Dialogical Framework for Ethical Inquiry of AI and Data Projects in the Netherlands' [2021] Ethics and Information Technology 1

Friedewald M and others, 'Deliverable 4: Final Report — A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies' (*PRESCIENT project*, 2013) <https://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT_deliverable_4_final.pdf>

——, 'Die Datenschutzfolgenabschätzung – Ein Werkzeug Für Einen Besseren Datenschutz' (2016)

——, 'Data Protection Impact Assessments in Practice' in Sokratis Katsikas and others (eds), *ESORICS 2021 International Workshops* (Springer International Publishing 2022)

Fuster GG, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer Law, Governance and Technology Series 2014)

Garaga A and others, 'D:C-6.2 Prototype for the Data Protection Impact Assessment Tool' (*Cloud Accountability Project (A4Cloud)*, 2014) <http://cloudaccountability.eu/sites/default/files/D36.2 Prototype for the data protection impact assessment tool.pdf>

Garante per la Protezione dei Dati Personali, 'Valutazione Di Impatto Sulla Protezione Dei Dati (DPIA)' <https://www.garanteprivacy.it/regolamentoue/DPIA>

Gegevensbeschermingsautoriteit, 'Aanbeveling Nr. 01/2018 van 28 Februari 2018 Aanbeveling Uit Eigen Beweging Met Betrekking Tot de Gegevensbeschermingseffectbeoordeling En Voorafgaande Raadpleging (CO-AR-2018-001)' (2018) <https://www.gegevensbeschermingsautoriteit.be/publications/aanbeveling-nr.-01-2018.pdf>

Gellert R, 'Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative' (2015) 5 International Data Privacy Law

Gellert R, 'The Article 29 Working Party's Provisional Guidelines on Data Protection Impact Assessment' (2017) 3 European Data Protection Law Review (EDPL) 212

Gellert R, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34 Computer Law & Security Review 279

——, *The Risk-Based Approach to Data Protection* (Oxford University Press 2020)

Gerards J and others, 'Impact Assessment Mensenrechten En Algoritmes' (*Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*, 2021) <https://www.uu.nl/sites/default/files/Rebo-IAMA.pdf>

——, 'Fundamental Rights and Algorithms Impact Assessment (FRAIA)' (*Ministry of the Interior and Kingdom Relations*, 2022) <https://www.government.nl/documents/reports/2021/07/31/impact-assessment-fundamental-rights-and-algorithms>

Gilad S, 'It Runs in the Family: Meta-Regulation and Its Siblings' (2010) 4 Regulation & Governance 485

Gonscherowski S and others, 'Durchführung Einer Datenschutz-Folgenabschätzung Gem. Art. 35 DSGVO Auf Der Methodischen Grundlage Eines Standardisierten Prozessablaufes Mit Rückgriff Auf Das SDM Am Beispiel Eines "Pay as You Drive"-Verfahrens (V 0.10)' (2017) <https://www.datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20171106-Planspiel-Datenschutz-Folgenabschaetzung.pdf>

Green B and others, 'Open Data Privacy: A Risk-Benefit, Process-Oriented Approach to Sharing and Protecting Municipal Data' (Berkman Klein Center for Internet and Society 2017)

GS1, 'GS1 EPC/RFID Privacy Impact Assessment Tool' <https://www.gs1.org/standards/rfid/pia> accessed 20 March 2022

——, 'Industry Proposal–Privacy and Data Protection Impact Assessment Framework for RFID Applications' (2010) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp175_annex_en.pdf>

——, 'Privacy and Data Protection Impact Assessment Framework for RFID Applications' (2011)

Health Information and Quality Authority, 'Guidance on Privacy Impact Assessment in Health and Social Care' (2010) <https://www.hiqa.ie/sites/default/files/2017-03/HI_Privacy_Impact_Assessment.pdf>

——, 'Guidance on Privacy Impact Assessment in Health and Social Care Version 2.0' (2017) <https://www.hiqa.ie/sites/default/files/2017-10/Guidance-on-Privacy-Impact-Assessment-in-health-and-social-care.pdf>

Hoorn E and Montagner C, 'Starting with a DPIA Methodology for Human Subject Research' (2018) <https://www.rug.nl/research/research-data-management/downloads/c2-dataprotection-dl/dpia_guidance_doc_v1_pub.pdf>

Hosein G and Davies S, 'Empirical Research of Contextual Factors Affecting the Introduction of Privacy Impact Assessment Frameworks in the Member States of the European Union' <https://piafproject.files.wordpress.com/2018/03/piaf_d2_final.pdf>

HR-Recycler project, 'D2.2 – HR-Recycler Impact Assessment Method' (2019) <https://www.hr-recycler.eu/wp-content/uploads/2020/02/D2.2.pdf>

IAB Europe Legal Committee, 'GDPR Data Protection Impact Assessments (DPIA) for Digital Advertising under GDPR' (2020) <https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf>

IAB UK, 'IAB UK Digital Advertising Guidance: Data Protection Impact Assessments under the GDPR' (2020) <https://www.iabuk.com/sites/default/files/public_files/IAB-UK Digital-advertising-guidance-Data-Protection-Impact-Assessments-under-the-GDPR.pdf>

ICO, 'Privacy Impact Assessment Handbook' (ICO 2007)

——, 'Privacy Impact Assessment Handbook v 2.0' (ICO 2009)

——, 'Conducting Privacy Impact Assessments Code of Practice' (2014)

——, 'Sample DPIA Template' (2018) <https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf> accessed 10 March 2022

——, ‘Age Appropriate Design: A Code of Practice for Online Services’ (2020) <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/>

——, ‘Sample Data Protection Impact Assessment: Connected Toy’ (2020) <https://ico.org.uk/for-organisations/childrens-code-hub/sample-data-protection-impact-assessment-connected-toy/>

——, ‘Guide to the General Data Protection Regulation (GDPR)’ (2021) <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf>

——, ‘Overview of Data Protection Harms and the ICO’s Taxonomy’ (2022) <https://ico.org.uk/media/about-the-ico/documents/4020144/overview-of-data-protection-harms-and-the-ico-taxonomy-v1-202204.pdf>

ICO and Surveillance Camera Commissioner, ‘Data Protection Impact Assessments – Guidance for Carrying out a Data Protection Impact Assessment on Surveillance Camera Systems’ (ICO; Surveillance Camera Commissioner 2020)

——, ‘DPIA Template’ (2020) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/886883/SCC__ICO_DPIA_Template_V4_.docx> accessed 10 March 2022

IMY, ‘Så Här Gör Man En Konsekvens-bedömning’ (2021) <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/konsekvensbedomningar-och-forhandssamrad/sa-har-gor-man-en-konsekvensbedomning/> accessed 10 March 2022

Informacijski pooblaščenec, ‘Ocene Učinkov Na Varstvo Podatkov Smernice Informacijskega Poobla Ščenca’ (2017)

Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales, ‘Guía Para La Elaboración de Evaluaciones de Impacto a La Privacidad’ (2020) <https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/guiaeip.pdf>

Ioannidis N and others, ‘PERSONA Deliverable D3.2: PERSONA Assessment Method (Final Version)’ (*PERSONA project*, 2021) <https://cris.vub.be/ws/portalfiles/portal/66227166/PERSONA_D3.2_v2.2_final_clean_PP_download_.pdf>

ISO, ‘ISO/IEC 29134:2017(En) Information Technology — Security Techniques — Guidelines for Privacy Impact Assessment’ (2017)

Janssen HL, ‘An Approach for a Fundamental Rights Impact Assessment to Automated Decision-Making’ (2020) 10 International Data Privacy Law 76

Kaminski ME and Malgieri G, ‘Algorithmic Impact Assessments under the GDPR: Producing Multi-Layered Explanations’ [2020] International Data Privacy Law 19

Kežmah B and others, ‘D3.6 Guidelines for GDPR Compliant User Experience’ (*CyberSec4Europe project*, 2020) <https://cybersec4europe.eu/wp-content/uploads/2021/02/D3.6-Guidelines-for-GDPR-compliant-user-experience-Revision-2.0.pdf>

Kitchin R and Dodge M, *Code/Space: Software and Everyday Life* (MIT Press 2011)

Kloza D and others, ‘The Concept of Impact Assessment’ in J Peter Burgess and Dariusz Kloza (eds), *Border Control and New Technologies* (Uitgeverij ASP)

——, ‘Data Protection Impact Assessments in the European Union. Complementing the New Legal Framework towards a More Robust Protection of Individuals’ (*d.pia.lab Policy Brief No. 1/2017*, 2017) <https://cris.vub.be/ws/portalfiles/portal/32009890/dpialab_pb2017_1_final.pdf>

——, ‘Towards a Method for Data Protection Impact Assessment: Making Sense of GDPR Requirements’ (*d. pia. lab Policy Brief No. 1/2019*, 2019) <https://cris.vub.be/ws/portalfiles/portal/48091346/dpialab_pb2019_1_final.pdf>

——, ‘Data Protection Impact Assessment in the European Union: Developing a Template for a Report from the Assessment Process’ (*d.pia.lab Policy Brief No. 1/2020*, 2020) <https://researchportal.vub.be/en/publications/data-protection-impact-assessment-in-the-european-union-developin>

Klüver L, Nielsen RØ and Jørgensen ML, *Policy-Oriented Technology Assessment Across Europe* (Springer Nature 2015)

Kool L and others, ‘Opwaarderen - Borgen van Publieke Waarden in de Digitale Samenleving’ (*Rathenau Instituut*, 2017) <https://www.rathenau.nl/sites/default/files/2018-02/Opwaarderen_FINAL.pdf>

Kosta E, ‘Article 35 Data Protection Impact Assessment’ in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): a commentary* (Oxford University Press 2020)

LINDDUN.org, ‘LINDDUN - Home’ (2020) <https://www.linddun.org/> accessed 20 March 2022

LINDDUN, ‘LINDDUN GO’ <https://www.linddun.org/go> accessed 20 March 2022

Lynskey O, ‘Deconstructing Data Protection: The “Added-Value” of a Right to Data Protection in the EU Legal Order’ (2014) 63 International and Comparative Law Quarterly 569

Mantelero A, ‘AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment’ (2018) 34 Computer Law & Security Review 754

——, *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI* (Springer 2022)

Mantelero A and Esposito MS, ‘An Evidence-Based Methodology for Human Rights Impact Assessment (HRIA) in the Development of AI Data-Intensive Systems’ (2021) 41 Computer Law & Security Review

Maras M-H, ‘Internet of Things: Security and Privacy Implications’ (2015) 5 International Data Privacy Law 99

Marnau N and others, ‘D1.2.4 Cloud Computing – Data Protection Impact Assessment’ (*TClouds project*, 2013) <https://tclouds.schunter.org/downloads/deliverables/TC-D1.2.4-Cloud-Computing-Privacy-Impact-Assessment-V1.1-Public.pdf>

Martin N and others, *Die Datenschutz-Folgenabschätzung Nach Art. 35 DSGVO: Ein Handbuch Für Die Praxis* (Fraunhofer Verlag 2020)

——, *The Data Protection Impact Assessment According to Article 35 GDPR. A Practitioner’s Manual.* (Fraunhofer Verlag 2020)

Mas R and others, ‘Creació de La Metódólógia per a l’avaluació de l’impacte Relativa a La Prótecció de Dades En Salut (AIPD)’ (*Universitat de Barcelona, Observatori de Bioètica i Dret – Càtedra UNESCO de Bioètica*, 2020) <https://ticsalutsocial.cat/wp-content/uploads/2021/07/aipd_creacio-metod_221220.pdf>

McCallister E, Grance T and Scarfone KA, ‘Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) – Special Publication 800-122’ (National Institute of Standards and Technology 2010)

Moss E and others, ‘Assembling Accountability: Algorithmic Impact Assessment for the Public Interest’ (2021)

Nas S and Terra F, ‘DPIA on Microsoft Teams, OneDrive Sharepoint and Azure AD (June 2021) Data Protection Impact Assessment on the Processing of Diagnostic Data’ (*SLM Rijk and SURF*, 2022) <https://www.rijksoverheid.nl/documenten/publicaties/2022/02/21/public-dpia-teams-onedrive-sharepoint-and-azure-ad>

Ni Loideain N, ‘Cape Town as a Smart and Safe City: Implications for Governance and Data Privacy’ (2017) 7 International Data Privacy Law 314

NIST, ‘NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0’ (2020) <https://doi.org/10.6028/NIST.CSWP.01162020>

——, ‘NIST Risk Management Framework’ (2022) <https://csrc.nist.gov/Projects/risk-management/sp800-53-controls> accessed 22 March 2022

NOREA, ‘NOREA Handreiking Data Protection Impact Assessment’ (2020)

Notario N and others, ‘PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology’, *2015 IEEE Security and Privacy Workshops* (IEEE 2015)

Oetzel MC and others, ‘Privacy Impact Assessment Guideline for RFID Applications’ (Julian Cantella ed, 2011) <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Langfassung.pdf?__blob=publicationFile&v=1>

Oetzel MC and Spiekermann S, ‘A Systematic Methodology for Privacy Impact Assessments: A Design Science Approach’ (2014) 23 European Journal of Information Systems 126

Office of the Australian Information Commissioner, ‘Guide to Undertaking Privacy Impact Assessments’ (2020)

Office of the Privacy Commissioner of Canada, ‘Expectations: OPC’s Guide to the Privacy Impact Assessment Process’ (2020) <https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/> accessed 22 March 2022

Parker C, *The Open Corporation: Effective Self-Regulation and Democracy* (Cambridge University Press 2002)

Personal Data Protection Commission, ‘Guide to Data Protection Impact Assessments’ (2021)

Privacy Commissioner, ‘Privacy Impact Assessment Toolkit’ (2015) <https://www.privacy.org.nz/publications/guidance-resources/privacy-impact-assessment/> accessed 22 March 2022

Purtova N, ‘The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law’ (2018) 10 Law, Innovation and Technology 1

Raab CD, ‘Information Privacy, Impact Assessment, and the Place of Ethics’ (2020) 37 Computer Law & Security Review

Rijksoverheid, ‘Data Protection Impact Assessments DPIA’s Office 365 ProPlus, Windows 10 Enterprise, Office 365 Online and Mobile Apps’ (2019)

——, 'Data Protection Impact Assessment' (2021) <https://www.kcbr.nl/beleid-en-regelgeving-ontwikkelen/integraal-afwegingskader-voor-beleid-en-regelgeving/verplichte-kwaliteitseisen/data-protection-impact-assessment> accessed 10 March 2022

Ruiz J and others, 'Deliverable 4.4 Final Report on PESIA' (*VIRT-EU project*, 2019) <https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c3b3de47&appId=PPGMS>

Scudiero L and Ziegler S, 'SynchroniCity D1.4 Privacy by Design Methodology & PIA' (2017)

Seto Y, 'Study on the Application of the Privacy Impact Assessment in Smart City' (2013) 98 Electronics and Communications in Japan 52

SGTF EG2, 'Smart Grid Task Force 2012-14 Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment' (2018) <https://energy.ec.europa.eu/system/files/2018-09/dpia_for_publication_2018_0.pdf>

Sion L and others, 'Interaction-Based Privacy Threat Elicitation', *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (IEEE 2018)

Smart Grid Task Force 2012-14 Expert Group 2: Regulatory Recommendations for Privacy Data Protection and Cyber-Security in the Smart Grid Environment, 'Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems' (2014)

Smits R, Leyten J and Den Hertog P, 'Technology Assessment and Technology Policy in Europe: New Concepts, New Goals, New Infrastructures' (1995) 28 Policy sciences 271

Spiekermann S, 'The RFID PIA–Developed by Industry, Endorsed by Regulators' in Paul De Hert and David Wright (eds), *Privacy impact assessment* (Springer 2012)

Tancock D, Pearson S and Charlesworth A, 'Analysis of Privacy Impact Assessments within Major Jurisdictions', *2010 Eighth International Conference on Privacy, Security and Trust* (2010)

Tancock D, Pearson S and Charlesworth A, 'The Emergence of Privacy Impact Assessments' (2010)

——, 'A Privacy Impact Assessment Tool for Cloud Computing' in Siani Pearson and George Yee (eds), *Privacy and Security for Cloud Computing* (Springer London 2013)

TIC Salut Social, 'DPIA Tool' (2020) <https://ticsalutsocial.cat/dpd-salut/dpia-tool/> accessed 20 March 2022

TIC Salut Social and Universitat de Barcelona O de B i D, 'Avaluació d'impacte Relativa a La Protecció de Dades (Aipd) En Salut – Metodologia d'aplicació' (2020) <https://ticsalutsocial.cat/wp-content/uploads/2021/07/aipd_formacio-metodologia.pdf> accessed 20 March 2022

Tietosuojavaltuutetun toimisto, 'Tietosuojan Vaikutustenarvioinnin Ohje' (2021)

Todde M and others, 'Methodology and Workflow to Perform the Data Protection Impact Assessment in Healthcare Information Systems' (2020) 19 Informatics in Medicine Unlocked

Úřad pro ochranu osobních údajů, 'Metodika Obecného Posouzení Vlivu Na Ochranu Osobních Údajů' (2020)

Úradu na ochranu osobných údajov, 'Vyhláška – Úradu Na Ochranu Osobných Údajov Slovenskej Republiky z 29. Mája 2018 o Postupe Pri Posudzovaní Vplyvu Na Ochranu Osobných Údajov' (2018)

Urząd Ochrony Danych Osobowych, 'Jak Rozumieć Podejście Oparte Na Ryzyku?' (2018)

Utrecht Data School, 'Data Ethics Decision Aid (DEDA)' <https://dataschool.nl/en/deda/> accessed 30 March 2022

——, 'De Ethische Data Assistent (DEDA)' <https://dataschool.nl/deda/> accessed 15 July 2022

——, 'Beraadslagingsinstrument Voor Algoritmische Systemen (BIAS)' (2022)

van Dijk N, Gellert R and Rommetveit K, 'A Risk to a Right? Beyond Data Protection Risk Assessments' (2016) 32 Computer Law & Security Review 286

van Zoonen L, 'Privacy Concerns in Smart Cities' (2016) 33 Government Information Quarterly

Vandercruysse L, Buts C and Dooms M, 'A Typology of Smart City Services Based on DPIA-Costs D.3.2' (*SPECTRE project*, 2019)

——, 'Economic Costs of the DPIA D.3.1' (*SPECTRE project*, 2019) <https://spectreproject.be/output/downloads-1/deliverable-d3-1-economic-costs-of-the-dpia.pdf>

——, 'Selecting a Data Protection Approach for Procurement of Smart City Services: Matching Policy Feasibility with Intrinsic Service Characteristics D.3.4' (*SPECTRE project*, 2019)

——, 'A Typology of Smart City Services: The Case of Data Protection Impact Assessment' (2020) 104 Cities 102731

Vandercruysse L, Dooms M and Buts C, 'The DPIA: Clashing Stakeholder Interests in the Smart City?' in Dara Hallinan, Ronald Leenes and Paul De Hert (eds), *Data Protection and Privacy, Volume 14: Enforcing Rights in a Changing World* (Bloomsbury 2021)

Vemou K and Karyda M, 'An Evaluation Framework for Privacy Impact Assessment Methods', *MCIS 2018 Proceedings* (2018)

——, 'Evaluating Privacy Impact Assessment Methods: Guidelines and Best Practice' (2019) 28 Information & Computer Security

Vereniging van Nederlandse Gemeenten / Informatiebeveiligingsdienst voor gemeenten (IBD), 'Handreiking Data Protection Impact Assessment (DPIA) Een Operationeel Kennisproduct Ter Ondersteuning van de Implementatie van de Baseline Informatiebeveiliging Overheid (BIO)' (2020) <https://www.informatiebeveiligingsdienst.nl/product/handreiking-dpia-bio/> accessed 30 March 2022

Vig NJ and Paschen H, *Parliaments and Technology: The Development of Technology Assessment in Europe* (Suny Press 2000)

Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens, 'Sjabloon VTC Voor GEB/DPIA' <https://overheid.vlaanderen.be/sjabloon-vtc-voor-geb/dpia> accessed 15 July 2022

VNG, 'IRPA-Tool' <https://www.informatiebeveiligingsdienst.nl/irpa-tool/> accessed 30 March 2022

VUB-LSTS, 'D2.2 – Framework for Impact Assessment against RRI - ELSA Requirements' (*PARENT project*, 2016) <https://www.parent-project.eu/wp-content/uploads/D2.2_Framework-for-impact-assessment-against-ELSA-requirements.pdf>

Wachter S, 'Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR' (2018) 34 Computer Law & Security Review 436

Wadhwa K and Rodrigues R, 'Evaluating Privacy Impact Assessments' (2013) 26 Innovation: The European Journal of Social Science Research 161

Warren A and others, 'Privacy Impact Assessments: International Experience as a Basis for UK Guidance' (2008) 24 Computer Law & Security Review 233

Weber RH, 'Internet of Things – New Security and Privacy Challenges' (2010) 26 Computer Law & Security Review 23

——, 'Internet of Things: Privacy Issues Revisited' (2015) 31 Computer Law & Security Review 618

Wood S and others, 'Review of Literature Relevant to Data Protection Harms' (2022)

Wright D, 'A Framework for the Ethical Impact Assessment of Information Technology' (2011) 13 Ethics and Information Technology 199

——, 'The State of the Art in Privacy Impact Assessment' (2012) 28 Computer Law & Security Review 54

——, 'Making Privacy Impact Assessment More Effective' (2013) 29 The Information Society 307

——, 'How Good Are PIA Reports – and Where Are They?' (2014) 25 European Business Law Review 407

——, 'Sorting out Smart Surveillance' (2010) 26 Computer Law & Security Review 343

——, 'A Privacy Impact Assessment Framework for Data Protection and Privacy Rights' (2011) <https://piafproject.files.wordpress.com/2018/03/piaf_d1_21_sept2011revlogo.pdf>

——, 'Privacy Impact Assessment and Risk Management' (Office of the Information Commissioner 2013)

——, 'Integrating Privacy Impact Assessment in Risk Management' (2014) 4 International Data Privacy Law 155

——, 'Surveillance Impact Assessment Manual' (*SAPIENT project*, 2014) <https://publica.fraunhofer.de/eprints/urn_nbn_de_0011-n-3161367.pdf>

Wright D, Finn R and Rodrigues R, 'A Comparative Analysis of Privacy Impact Assessment in Six Countries' (2013) 9 Journal of Contemporary European Research

Wright D and Friedewald M, 'Integrating Privacy and Ethical Impact Assessments' (2013) 40 Science and Public Policy 755

Wright D, Friedewald M and Gellert R, 'Developing and Testing a Surveillance Impact Assessment Methodology' (2015) 5 International Data Privacy Law 40

Wright D and Mordini E, 'Privacy and Ethical Impact Assessment' in Paul De Hert and David Wright (eds), *Privacy Impact Assessment* (Springer Netherlands 2012)

Wright D and Raab CD, 'Constructing a Surveillance Impact Assessment' (2012) 28 Computer Law & Security Review 613

Wuyts K, 'LINDDUN : A Privacy Threat Analysis Framework' (2014)

Wuyts K and Joosen W, 'LINDDUN Privacy Threat Modeling: A Tutorial' (2015) CW Reports 685

Wuyts K, Scandariato R and Joosen W, 'Empirical Evaluation of a Privacy-Focused Threat Modeling Methodology' (2014) 96 Journal of Systems and Software 122

——, 'LIND(D)UN Privacy Threat Tree Catalog' (2014) CW Reports 675

Wuyts K, Sion L and Joosen W, 'Linddun Go: A Lightweight Approach to Privacy Threat Modeling', *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (IEEE 2020)

Yskout K and others, 'Threat Modeling: From Infancy to Maturity', *2020 IEEE/ACM 42nd International Conference on Software Engineering: New Ideas and Emerging Results (ICSE-NIER)* (IEEE 2020)