View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Helsingin yliopiston digitaalinen arkisto

Information & Communications Technology Law

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/cict20

The controller's role in determining 'high risk' and data protection impact assessment (DPIA) in developing digital smart city

Shakila- Bu-Pasha

To cite this article: Shakila- Bu-Pasha (2020) The controller's role in determining 'high risk' and data protection impact assessment (DPIA) in developing digital smart city, Information & Communications Technology Law, 29:3, 391-402, DOI: 10.1080/13600834.2020.1790092

To link to this article: https://doi.org/10.1080/13600834.2020.1790092

© 2020 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

Published online: 07 Jul 2020.

Submit your article to this journal

Article views: 248

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=cict20

INFORMATION & COMMUNICATIONS TECHNOLOGY LAW
2020, VOL. 29, NO. 3, 391–402
https://doi.org/10.1080/13600834.2020.1790092

Routledge
Taylor & Francis Group

OPEN ACCESS Check for updates

The controller's role in determining 'high risk' and data protection impact assessment (DPIA) in developing digital smart city

Shakila- Bu-Pasha

Faculty of Law, University of Helsinki, Helsinki, Finland

ABSTRACT
Article 35 of the General Data Protection Regulation (GDPR) states that data controllers are required to carry out data protection impact assessment (DPIA) if a processing operation, particularly involving the use of new technologies, is 'likely to result in a high risk to the rights and freedoms of natural persons'. The focus in this paper is on the role and responsibilities of data controllers in a smart city platform in assessing 'high risk' and the importance of impact assessment in relation to data processing with the latest technologies for the protection of personal data.

KEYWORDS
High risk; DPIA; smart city; GDPR; personal data; joint controllers; technology

1. Introduction

With the evolution of science, modern technologies in human civilisation are advancing rapidly. Updated laws are also being introduced to tackle the changing circumstances. The General Data Protection Regulation (GDPR)[1] is a recent addition to those laws in the European Union (EU) Member States.

Digital smart city is a modern technological innovation in which the Internet of Things (IoT), 5G technology as well as artificial intelligence, machine learning and other smart and recent technologies are or will be used. However, the concept of 'smart city' has not been defined in law. A smart city is designed, built and maintained with the use of advanced, integrated and smart technologies, devices and sensors which can provide and develop a variety of safe, fast and better services in parallel including transportation, education, power, healthcare etc.[2] Various disciplines, including information technology, economic and social development, urban planning and management, sustainable development contribute to developing a smart city.[3] The definition provided by Forrester is useful in understanding the concept. Accordingly, smart city means:

CONTACT Shakila-Bu-Pasha shakila.bu-pasha@helsinki.fi

[1]Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (2016) OJ L119/1.

[2]Robert E Hall, 'The Vision of a Smart City' in Proceedings of the 2nd International Life Extension Technology Workshop, Paris, France (28 September).

[3]Rashid Mehmood and others, *Smart Infrastructure and Applications* (Springer International Publishing, 2020), 2.

This article has been republished with minor changes. These changes do not impact the academic content of the article.

© 2020 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (http://creativecommons.org/licenses/by-nc-nd/4.0/), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way.

> 'The use of Smart Computing technologies to make the critical infrastructure components and services of a city – which include city administration, education, healthcare, public safety, real estate, transportation, and utilities – more intelligent, interconnected, and efficient'. Thus, smart computing becomes a key factor in a smart city platform.[4]

It is understood that privacy of personal and location data will be at risk in the 5G and other network-based platforms in the smart cities because of inter-connected smart sensors and devices. According to Article 35(1) of the GDPR, data controllers are required to carry out a data protection impact assessment (DPIA), if data processing activities, especially those using new technologies, are 'likely to result in a high risk to the rights and freedoms of natural persons'.[5] The GDPR neither defines 'high risk' nor DPIA. However, some criteria for constituting 'high risk' are identified in legal provisions and guidelines which are elaborately discussed in Section 4. In short, high risk may be involved in processing large amounts of data or sensitive or special categories of personal data as well as if processing operations are carried out using new technologies and for which the controller has not carried out a DPIA before.[6]

DPIA implies a systematic process to investigate, identify and minimise risks in a project or big data platform for the protection of personal data.[7] The GDPR has introduced it as a new requirement which reflects the principle of data protection by design.[8] The provision on DPIA promotes the practice of self-assessment. In addition, it assists in the state-of-the-art of a particular project and in deciding about data protection measures as well as to plan and suggest essential steps to ensure compliance with the law.[9] DPIA is also referred to as privacy impact assessment (PIA) in many parts of the world.[10]

As it is expressed in Recital 84, DPIA is essential from the controller's side to evaluate, especially, 'the origin, nature, particularity and severity' of the 'high risk' which is involved with the data processing operations. The assessment result becomes useful for the controllers in deciding and adopting appropriate measures in processing personal data as well as in complying with the GDPR.[11]

---

[4]Doug Washburn and others, *Helping CIOs Understand 'Smart City' Initiatives: Defining the Smart City, Its Drivers, and the Role of the CIO* (Forrester Research, Inc., 11 February 2010) <https://goo.gl/4XHk0F> accessed 8 June 2020.

[5]Article 35(1): '"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.'."

[6]Steve Alder, 'GDPR High Risk Data Processing' (3 May 2018) <https://www.hipaajournal.com/gdpr-high-risk-data-processing/> accessed 12 June 2020.

[7]ico., 'What is a DPIA?' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/> accessed 21 January 2020.

[8]GDPR.EU, 'Data Protection Impact Assessment (DPIA)' <https://gdpr.eu/data-protection-impact-assessment-template/> accessed 16 June 2020.

[9]Gauthier Chassang, 'The impact of the EU general data protection regulation on scientific research' ecancermedicalscience 11 (2017), 7.

[10]IT Governance, 'Data Protection Impact Assessments and the GDPR' <https://www.itgovernance.co.uk/privacy-impact-assessment-pia> accessed 5 May 2020.

[11]Recital 84: 'In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. 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. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing'.

As data controllers, organisations must prepare a DPIA if their data processing activities are likely to result in 'high risk'. Huge fines can be imposed in cases of failure to implement DPIA in the required circumstances. According to Article 83(4)(a), infringement of the requirement of DPIA can result in an administrative fine of either up to €10 million, or 2% of annual worldwide turnover (whichever is bigger).[12]

The research for this article involved an examination of whether there is 'high risk' to the rights and freedoms of the data subjects in operating modern technologies like 5G and the IoT for the digital smart city, and the need for impact assessment of the envisaged processing activities for the protection of personal data. Thus, the article does not intend to include all possible data processing operations that may contain 'high risk', rather it maintains an approach of context-basis specific analysis of legal requirements under the GDPR.

In this way, first the research explores whether the data controllers are obliged to assess the impact of data processing for the protection of personal data in the context of digital smart city in connection to the use of latest technologies, such as 5G network and IoT. If yes, then what are their obligations in assessing the impact of data processing?

Article 29 Data Protection Working Party (A29 WP) has drafted a useful set of Guidelines to determine when DPIA is necessary with respect to 'high risk' in data processing for the purposes of the GDPR (hereinafter referred to as WP 248 guidelines).[13] This article is predominantly based on the relevant GDPR provisions and the WP 248 guidelines.

2. How will the IoT and 5G endanger personal (location) data in connection to smart city?

Developing smart light poles is a common feature in many smart city projects. Taking that as an example, small cells are often integrated into city light poles using the IoT and 5G technology when only one network is feasible.[14] In this section, I have discussed why the IoT and 5G are relevant to the topic, and how they endanger personal and location data in connection to smart city, or more specifically, smart light poles, mostly from the technical point of view.

The IoT indicates such a system when different devices, objects and appliances are set in an inter-connected system with separate identifiers. Without human and computer interaction, the integrated sensors in the system are capable of transferring data and communicating with other systems.[15]

As IoT devices are or would be located at particular points in the smart city area including implementing smart light poles, devices are able to assist in observing and measuring the physical location of those points, and transferring that information to other devices.[16]

[12]IT governance (n 10).
[13]Article 29 Data Protection Working Party (A29 WP), *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* (4 April 2017).
[14]LuxTurrim5G, 'Building the Digital Backbone for a Smart City' <https://www.luxturrim5g.com/> accessed 6 May 2020.
[15]Margaret Rouse, 'Internet of Things (IoT)' (*IoT Agenda*) <https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT>; Michael Chui and others, 'The Internet of Things' *McKinsey Quarterly* (March 2010) <https://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things> accessed 21 January 2020.
[16]Mahmoud Elkhodr and others, 'The Internet of Things: New Interoperability, Management and Security Challenges' (2016) 8(2) International Journal of Network Security & Its Applications (IJNSA) 99.

By offering highly distributed technologies with inter-related devices and smart nodes, the IoT involves privacy threats, especially with location-aware technologies, which enhances the opportunity for secretly collecting and transferring personal data and identifying a particular individual.[17] MAC addresses[18] can be collected and an accurate location can be deduced from the sensors and nodes used in the IoT.[19] The IoT promotes automatic processing, and even anonymisation may not always be effective in protecting privacy and personal data.[20]

At the same time, fifth-generation or 5G wireless technology is one of the latest envisaged technologies and burning issues all over the world. While 4G technology is already running, the information technology system is preparing to welcome a 5G network.

A 5G network has not yet been officially announced. Using very small cells in the networks compared to the previous generation networks implies that 5G systems will be much smarter with higher speeds and capacity, (and low latency), especially facilitating mobile technologies and Internet performance.[21]

A 5G wireless network and communication system will be particularly reliant on location data. 5G positioning is an intelligent concept which is capable of measuring accurate locations in wide bandwidths by deploying dense access points.[22] A large portion of 5G devices will be highly efficient location-aware devices which will frequently use the Global Positioning System (or GPS), Wi-Fi, radio-based positioning including radio frequency identification (RFID) and Bluetooth.[23] Use of such devices, smart antennas and a variety of sensors within the network of smart poles will increase the risk to location data privacy, and thus location and positioning will become a key factor in 5G.[24]

3. Controller and joint controller

In the context of developing smart city services such as smart light poles, it is important to decide who the data controller is. Article 4(7) of the GDPR states, '"controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'. As per that definition and considering the smart city perspective, business organisations and technology companies which take the initiative to implement the smart light poles with the authority of determining the purposes and means of personal data processing, are the data controllers.

The controller is required to implement appropriate technical and organisational measures in order to ensure GDPR compliance under Article 24(1).[25] In doing that, in

[17]ibid 98.

[18]MAC or the Media Access Control address is a unique number with the help of which the physical location of the hardware network devices can be identified: 'What is a MAC Address?' (*IP Location*) <https://www.iplocation.net/mac-address> accessed 21 January 2020.

[19]Article 29 Data Protection Working Party (A29 WP), *Opinion 8/2014 on the on Recent Developments on the Internet of Things* (16 September 2014), 3, 8.

[20]Elkhodr (n 16), 98.

[21]Sascha Segan, 'What is 5G?' *PC News* (1 May 2017) <https://uk.pcmag.com/cell-phone-service-providers-products/82400/feature/what-is-5g> accessed 21 January 2020.

[22]Elena Simona Lohan and others, 'Positioning: Security and Privacy Aspects' in Madhusanka Liyanage and others (eds), *A Comprehensive Guide to 5G Security* (Wiley, 2018) 281.

[23]Rocco Di Taranto and others, 'Location-aware Communications for 5G Networks: How Location Information Can Improve Scalability, Latency, and Robustness of 5G' (2014) 31(6) IEEE Signal Processing Magazine 102–104.

[24]Tampere University of Technology, 'Positioning and Location-Awareness in Future 5G Networks' <https://www.tut.fi/5G/positioning/> accessed 21 January 2020.

addition to other factors, it needs to consider 'the risks of varying likelihood and severity for the rights and freedoms of natural persons'. This provision conveys the controller's general obligation, which although does not mention DPIA, it implies DPIA in certain circumstances with the obligation to manage the risks appropriately.[26]

Article 26(1) states, 'Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation'. As per the requirement of Article 26, joint controllers need to agree on an arrangement regarding their respective responsibilities, for example to provide information to the data subjects regarding personal data processing so that the data subjects can exercise their rights properly. It will be convenient for the data subjects if the arrangement designates a contact point. However, in the smart city framework, such arrangements can be done with the DPIA. In other words, several controllers can carry out the joint DPIA.[27]

It is probable that the joint controllers will conduct the processing operation in a smart city ecosystem in connection to smart light poles and other services. In such a case, they should decide on their respective obligations, and the DPIA should ascertain each of their responsibilities for tackling the risks and to protect data subjects' rights and freedoms.[28] As an example, such a pilot project will most possibly attempt to develop and maintain a data ecosystem in which different parties will be involved, for example, companies which will serve the smart city, network operators, end-users, app-developers, city operator, smart city operations centre and so on. In addition, the market area of the ecosystem will include customers (who may process the data further to enhance their solutions and improve quality), data brokers, device vendors, and public authorities (including cities) etc.

Here the end-users will be the data subjects, and the app developers should be data processors or in special circumstances may act as data controllers. Depending on the nature of the processing and the available information, the processor should take part or have contribution in the DPIA. The roles and responsibilities of the processors should also be defined with contractual measures.[29]

It is important to determine the roles of the other entities as mentioned above, since many of them can act as joint controllers. In this respect, it is relevant to mention the recent landmark judgment of the Court of Justice of the European Union (CJEU) in the *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV* case.[30] It was decided that a website operator who featured the Facebook 'Like' button and caused the transmission of website visitors' personal data to Facebook can become a joint controller, along with

[25]Article 24(1): 'Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary'.

[26]WP 248 guidelines (n 13), 4, 19.

[27]Lydia F de la Torre, 'What is a 'Data Protection Impact Assessment' (DPIA) under EU Law?' *Golden Data* (13 march 2019) <https://medium.com/golden-data/what-is-a-data-protection-impact-assessment-dpia-under-eu-law-644e46ce9b62> accessed 21 January 2020.

[28]WP 248 guidelines (n 13), 6.

[29]OneTrust DataGuidance, 'EU: The How, When and Why of Carrying Out a DPIA' (August 2019) <https://platform.dataguidance.com/opinion/eu-how-when-and-why-carrying-out-dpia> accessed 5 May 2020.

[30]C-40/17, (CJEU, 29 July 2019).

Facebook, under the EU data protection law.[31] The CJEU took a broad outlook in interpreting the concept of joint controllership under GDPR through this judgement.[32]

4. 'High risk' and the requirements of DPIA under the GDPR

This section describes the controller's role as well as the question of determining 'high risk' from the legal point of view, and the requirements of DPIA with some legal analysis.

4.1. Requiring DPIA in relation to 'high risk'

Article 35 is a comprehensive provision in the context of identifying 'high risk' in data processing and its impact assessment on the protection of personal data. Under Article 35(1), the controllers are required to assess or identify if a 'high risk' is likely and therefore to carry out DPIA with regard to the processing of personal data.[33] And they should do it prior to the processing. Preferably, organisations as data controllers should draw up their DPIA before and during the initial planning of their new projects regarding smart cities.[34]

If a set of similar processing operations presents similar 'high risks', then a single DPIA may be enough, in circumstances in which it is reasonable and economical [Recital 92, Art. 35(1)]. Therefore, several processing operations that pose similar high risks may be covered under a single DPIA, provided that, 'the nature, scope, context and purposes of the processing' are adequately considered. It is relevant to note that, 'similar' does not mean 'identical'. Here it may mean that using same type of technologies to conduct the same sort of processing in order to fulfil nearly the same purposes.[35] In a smart city, although different services would be offered, a single DPIA may be possible, unless dissimilar processing operations are evident.

It is the responsibility of the data controller to carry out DPIA, or it can authorise another body to perform that duty with the controller's accountability. When a data protection officer is designated, the controller has to take their advice [Art. 35(2)]. According to Article 39(1)(c), it is a responsibility of the data protection officer to advise after being requested by the controller regarding DPIA and monitor its performance as per Article 35.

Reviewing the risk at regular intervals is necessary in order to determine if a processing operation is likely to result in 'high risks' at some point after the platform (here smart city) is established, considering risks which did not exist before.[36] Although the final version of the GDPR did not include the European Parliament's proposal for compulsory biannual

[31]Natascha Gerlach and others, 'CJEU Judgment in the Fashion ID Case: The Role as Controller Under EU Data Protection Law of the Website Operator that Features a Facebook "Like" Button' *Cleary Cybersecurity and Privacy Watch* (2 August 2019) <https://www.clearycyberwatch.com/2019/08/cjeu-judgment-in-the-fashion-id-case-the-role-as-controller-under-eu-data-protection-law-of-the-website-operator-that-features-a-facebook-like-button/> accessed 21 January 2020.
[32]Kalle Hynönen and Jussi Latola, 'CJEU Gives a Thumbs Up for Joint Controllership of Personal Data' *Krogerus* (21 August 2019) <https://www.krogerus.com/news_events/newsletters/cjeu-gives-a-thumbs-up-for-joint-controllership-of-personal-data> accessed 21 January 2020.
[33]Felix Bieker and others, 'A Process for Data Protection Impact Assessment under the European General Data Protection Regulation' (4th Annual Privacy Forum, Springer, Cham, 2016) 24.
[34]GDPR.EU (n 8).
[35]Ruben Zeegers, *Privacy & Data Protection Foundation Courseware – English* (Van Haren Publishing, 2018) 44.
[36]ibid.

review in the context of risk assessment and DPIA, Article 35(11) of the GDPR asserts an obligation on the controller to conduct a review, especially if the processing incurs a change in the risk.[37] Such a change could happen with the change and development of the latest technologies.[38] In this way, a controller who has started developing smart city before the GDPR came into force and has been processing personal data, should also conduct a review and carry out a DPIA.[39]

Article 35(7) demonstrates the minimum features which a DPIA should contain: for example, a systematic description which will include the purposes of the processing operations and the controller's legitimate interest in applicable cases. At the same time, it should comprise the necessity and proportionality assessment regarding the purposes of the processing operation and risk assessment in relation to the rights and freedoms of data subjects under Article 35(1).[40] Along with Article 35(7)(d), Recital 90 communicates that the DPIA should include the envisaged measures, e.g. security measures, safeguards and mechanisms in order to address and mitigate the risk as well as to ensure the protection of personal data and comply with the GDPR. In assessing the risk, in addition to considering 'the nature, scope, context and purposes' of the data processing, data controllers need to consider the sources of the risk and severity of the possible consequences.

Adoption of an appropriate code of conduct by the controllers under Article 40 to comply with the GDPR will be considered as a positive measure towards assessing the impact of data processing [Art. 35(8)]. In appropriate circumstances, the controller is required to 'seek the views of data subjects or their representatives' [Art. 35(9)]. In case the data controllers differ from the data subjects' views in final decision for DPIA, they should document the reason.[41] It is important to remember that there is no direct parameter to identify what constitutes 'high risk'. However, Article 35(3) provides three areas in which DPIA is required. Such examples are included in the discussion in the next section.

4.2. Determining 'high risk' in the light of Article 29 working party guidelines (WP 248)

After considering the relevant provisions of the GDPR, especially the specific elements of Article 35(1) and 35(3), the A29 WP listed nine criteria in its guidelines, which should be considered in order to decide whether processing operations are 'likely to result in a high risk' and require a DPIA.

Those nine criteria are briefly mentioned below. If a criterion seems to have a connection with smart city services, it has been highlighted for the convenience of understanding.

[37] Article 35(11) GDPR: 'Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations'.

[38] Bieker (n 33) 24.

[39] WP 248 guidelines (n 13) 11.

[40] Article 35(7): 'The assessment shall contain at least:

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

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

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

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

[41] OneTrust DataGuidance (n 29).

(1) Evaluation, scoring or building profiles, for example, building behavioural or marketing profiles by monitoring website usage, or predicting 'aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements' [Recitals 71, 75; Art. 4(4)];
(2) Automated processing or decision making which legally or similarly can produce significant effects [Article 35(3)(a)];
(3) **Systematic monitoring**, for example, of a publicly accessible area [Art. 35(3)(c)];
(4) **Sensitive or special categories of personal data** or data of a highly personal nature (Arts. 9 & 10),
(5) **Large scale processing**, which aims 'to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects' (Recital 91), [Points 4 and 5 combinedly relates to Article 35(3)(b)];
(6) Matching or combining datasets;
(7) **Data relating to vulnerable data subjects**, for example, children or employees (Recital 75);
(8) **Innovative use or new technological or organisational solutions** [Art. 35(1) and Recitals 89 and 91] – In this era of rapid technological expansion, unforeseeable legal challenges can appear with the risk to personal data and privacy; and
(9) If processing in itself 'prevents data subjects from exercising a right or using a service or a contract' (Art. 22 and recital 91).

It is presumed that if data processing meets at least two of the above-mentioned criteria, that would involve 'high risk' and require a DPIA. Processing that meets more criteria will increase the likelihood of having 'high risk', although in certain cases, meeting only one strong criterion may also need a DPIA.[42] Services under a smart city ecosystem would meet directly at least five criteria that are marked above. In addition to those five, it may meet other criteria in particular circumstances.

4.3. Analysis of the listed points in the smart city context

This section offers discussion about how the above highlighted marked points create 'high risks' in a smart city platform and necessitate a DPIA.

Firstly, smart city services, for example, smart light poles should be located in public places. Hence, systematic monitoring of a publicly accessible area is a relevant factor for smart light poles in a smart city ecosystem, because under such a platform, if the individuals are not informed beforehand about the processing of their personal data, they may remain ignorant about who collected the data, and for what purpose. In many cases, being subject to such processing in public places may become unavoidable for them.

Secondly, in addition to smart light poles, some smart city implementation authorities are already experimenting with offering smart healthcare services. For that purpose, they need to collect health data by processing patients' medical records, which would relate to sensitive or special categories of personal data and would require a DPIA. Moreover, after a smart city framework has been started thoroughly, data controllers can also see people going to doctor even if they do not offer medical services.

[42]WP 248 guidelines (n 13) 7–9.

Thirdly, although the term 'large scale' is not defined in the GDPR, in developing a smart city ecosystem, data controllers can consider the explanation about large scale processing which was expressed in a provision of the earlier version of the GDPR in 2014: if the personal data of more than 5000 data subjects are processed during a consecutive 12-month period, that would constitute large scale processing.[43] It can be anticipated that data processing under a smart city platform would constitute large scale processing.

Fourthly, apparently smart city may not be concerned about data relating to vulnerable data subjects, e.g. children's data, but questions would arise about collecting data concerning children who come into contact with smart city services, for example, smart light poles near kindergartens or smart bus stops in the street.

Fifthly, in developing all the services in a smart city ecosystem, innovative use of technologies or new technological or organisational solutions will be applied. For example, as Section 2 of this paper shows, IoT and future 5G technology have a significant impact on individuals' private lives; and thereby necessitate a DPIA. However, innovative technology may include artificial intelligence, machine learning, autonomous vehicles, smart technologies, market research involving neuro-measurement, IoT and 5G technologies and so on.[44]

In addition, transferring personal data outside the EU region (Recital 116, Arts 44–49) is also a correlated ground. Big multinational technology companies are located in a range of countries, most commonly the USA. Under the current technological scenario, especially in developing a smart city platform, transfer of personal data outside the EU region is very likely, which may entail the need for a DPIA as well.[45]

5. How should the DPIA be carried out?

Since DPIA is a part of the principle of data protection by design, controllers should start designing it as early as possible, even if they still do not know all of the processing operations. This approach is beneficial for a number of reasons. For example, they can identify the possible risks in an early stage which is easier and economical to handle. The organisations can become aware beforehand regarding privacy and data protection and will be less likely to breach the provisions of the GDPR. Thus, individuals as data subjects or users of the services of the smart cities will receive positive effects.[46]

The WP 248 guidelines has included two annexes from which controllers can find examples of general and sector-specific existing DPIA frameworks in the EU, and criteria for acceptable DPIA, respectively. However, although it is not intended in this article to engage in elaborate discussion about the contents of those annexes, it would be wise for data controllers to go through those annexes before or during an implementation of a smart city platform.

Different organisations have different working practices. They can enjoy flexibility, but only to a limited extent, in structuring and forming their DPIAs in order to cope it with their existing work practices. Taking into account existing DPIA frameworks, organisations as

[43]Chassang (n 9) 6–7.
[44]ICO, 'Accountability and governance: Data Protection Impact Assessments (DPIAs)' (May 2018) 22 <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias-1-0.pdf>.
[45]Shakila-Bu-Pasha, 'Location Data, Personal Data Protection and Privacy in Mobile Device Usage: An EU Law Perspective' (Doctoral dissertation, University of Helsinki 2018) 31–32.
[46]IT Governance (n 10).

controllers may apply different methodologies and sector-specific contexts. This is not only convenient for the controllers drawing up the DPIAs, but it is also useful in addressing the particularity of specific types of processing operation. However, the controllers have to comply with the criteria set out in Annex 2 of the WP 248 Guidelines, precisely which include:

- 'a systematic description of the processing' [Art. 35 (7)(a)]
- Assessing necessity and proportionality which will include general principles and lawfulness of processing, as well as the rights of the data subjects
- Managing 'risks to the rights and freedoms of data subjects' by considering the sources of risks, potential threats and impacts to those rights etc.
- Involving interested parties, for example, seeking data protection officer's advice or data subjects' or their representatives' views.

Thereby, in practice, organisations can develop a DPIA, either with a new template or by using an existing organisational template; however, in both cases, they have to fulfil the criteria listed in Annex 2. In addition, a template can be used in accordance with the advice by a supervisory authority.[47]

6. Conclusion

Most of the supervisory authorities of the EU Member States have submitted lists pursuant to Article 35(4) to the European Data Protection Board (EDPB) stating the data processing operations which can expose 'high risks', and therefore require a DPIA.[48] After that, as per the obligation under Article 64(1), the EDPB issued opinions on the lists submitted.[49] EDPB opined that the lists should be non-exhaustive in nature which complement and further specify the WP 248 guidelines. Pursuant to the Board's request, supervisory authorities included and are supposed to include certain types of data processing on their lists that should be consistent and harmonised with each other, but should not be identical.[50]

In addition to the criteria specified by the A29 WP 248 guidelines, the EDPB specifically mentioned about the processing of biometric data (such as, using face recognition technology), genetic data (for example, DNA testing) and location data which require DPIA if it is done in conjunction with at least one of the nine criteria of the A29 WP 248 guidelines. Furthermore, the Board opined that a DPIA is required if personal data are processed using innovative technology, or data are disclosed to third parties under Article 19 of the GDPR 'where the information of recipients would prove impossible or require a disproportionate effort', however, when involving at least one other criterion.[51]

[47]OneTrust DataGuidance (n 29).
[48]Müge Fazlioglu, 'What's Subject to a DPIA under the GDPR? EDPB on Draft Lists of 22 Supervisory Authorities', *iapp* <https://iapp.org/news/a/whats-subject-to-a-dpia-under-the-gdpr-edpb-on-draft-lists-of-22-supervisory-authorities/> accessed 21 January 2020.
[49]European Data Protection Board, *Opinions* <https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en> accessed 21 January 2020.
[50]Fazlioglu (n 48). This approach of EDPB reflects the harmonised way of data protection under GDPR for the Member States considering the national circumstances. (Relevant provision: Recital 10 GDPR).
[51]Fazlioglu (n 48).

Considering all the preceding discussion, the nine criteria of the WP 248 guidelines as well as the specific mention of location data and use of innovative technology by the EDPB, it can be concluded that 'high risk' to personal and location data is likely to exist in operating 5G and IoT in initiating various services under smart city platforms. Therefore, data controllers have an obligation to carry out an assessment of the impact of the envisaged processing activities on the protection of personal data.

As privacy and protection of personal location data may be seriously endangered in the 5G and IoT network-based platforms and with the use of other modern technologies, the smart city service providers as data controllers should follow privacy laws at certain levels by ensuring that there are appropriate features in implementing a smart city project. Refraining from processing particular types of data can be effective in reducing the risk, but this may not always be practical. In that case, adopting additional technical safety measures to protect personal data, ensuring anonymisation and pseudonymisation properly, as well as training staff to manage the risk will be efficient steps.[52]

As per Article 35(10) of the GDPR, the service providers (or controllers) in the smart city platform can enjoy exemption from carrying out a DPIA if they process data with a legal basis under EU or national law, which law exempts the requirement of conducting a DPIA. Carrying out a DPIA is assumed with the implementation of a general impact assessment in adopting that legal basis, for example, if processing is necessary for the public interest or in exercising official authority vested on them under Article 6 (1)(e).[53]

When the organisations carry out DPIAs properly, that supports the principle of accountability under Article 5(2) for the compliance with the GDPR.[54] If the DPIA reveals the existence of 'high risk' in data processing and the controllers become unable to mitigate the 'high risk' because of the technological reason and implementation cost, then they must consult the supervisory authority prior to the processing [Art. 36(1), Recitals 84, 94]. In that consultation, the controller will inform the supervisory authority about their responsibilities, the purposes and means of processing, what measures and safeguards they have adopted so far for the protection of rights and freedoms of data subjects, and all other relevant information [Art. 36(3)]. Additionally, if required by a Member State law, controllers will need to consult the supervisory authority in processing data as part of the performance of a task, for example, to protect social and public health [Art. 36(5)].

Risk assessment or DPIA is important not only to comply with the requirements of the GDPR, but also it can help organisations to enhance cyber security and address and minimise problems.[55] Even if the 'high risk' is not likely, conducting a DPIA by the controller

[52]Camden Woollven, '7 Key Stages of the Data Protection Impact Assessment (DPIA)' *IT Governance* (4 September 2019) <https://www.itgovernance.co.uk/blog/gdpr-six-key-stages-of-the-data-protection-impact-assessment-dpia> accessed 5 May 2020.

[53]Article 35(10): 'Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1–7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities'.

[54]IT Governance (n 10).

[55]Luke Irwin, 'Why Risk Assessments Are Essential for GDPR Compliance' *IT Governance* (15 October 2019) <https://www.itgovernance.co.uk/blog/why-risk-assessments-are-essential-for-gdpr-compliance> accessed 21 January 2020.

would still be a wise practice to reduce liabilities in data processing and ensure data protection.[56]

Acknowledgements

The author would like to thank Professor Päivi Korpisaari for revising and commenting on the initial draft of this article before submission for publication.

Disclosure statement

No potential conflict of interest was reported by the author.

Funding

This work is supported by the LuxTurrim5G ecosystem, as part of the Neutral Host Pilot project funded by the participating companies and Business Finland.

[56]GDPR.EU (n 8).