TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Department of Law

Pihla Helminen

ANALYZING THE OBSCURITIES OF THE DATA PROTECTION IMPACT ASSESSMENT AND "LIKELY TO RESULT IN A HIGH RISK" UNDER ARTICLE 35 OF THE EU GENERAL DATA PROTECTION REGULATION

Bachelor's thesis
Programme HAJB08/17, specialisation European Union and international law

Supervisor: Jenna Uusitalo, MA in international law,
Ph.D Candidate at the University of Helsinki

Tallinn 2021

I declare that I have compiled the paper independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously been presented for grading.
The document length is 12 996 words from the introduction to the end of conclusion.

Pihla Helminen ……

(signature, date)

Student code: 184029HAJB

Student e-mail address: pihelm@ttu.ee

Supervisor: Jenna Uusitalo, MA in international law:

The paper conforms to requirements in force

……

(signature, date)

Chairman of the Defence Committee:

Permitted to the defence

……

(name, signature, date)

TABLE OF CONTENTS

ABSTRACT

The data protection impact assessment (DPIA) is introduced under Article 35 of the European Union General Data Protection Regulation 2016/679 (GDPR). The enforcement of Article 35 has created changes to the processing of personal data.

This paper focuses on assessing when the processing is likely to present a high risk to natural persons' rights and freedoms (RaF) under Article 35 and a DPIA shall be conducted. The aim of the paper is to assess whether Article 35 includes any obscurities, in terms of a likelihood of a high risk, which could danger the protection of data subjects' RaF and Article 35's correct interpretation and application, and to propose possible solutions to clarify the identified obscurities, if necessary. The research is conducted with qualitative methods based on the European Union legislation, guidelines, literature, and two decisions given by the Office of Data Protection Supervisory Authority in Finland Thus, the research question is whether Article 35, especially, the likelihood of a high risk and the obligation to conduct a DPIA under Article 35 includes obscurities that could endanger Article 35's correct interpretation and application, and whether those obscurities could be clarified.. The hypothesis is that there are some obscurities, concerning Article 35, to be clarified to some extent.

The results, based on legislation, guidelines, literature, and the two decisions, reflect that there are some unclarities regarding Article 35's "likely to result in a high risk", which could be clarified to ensure the protection of data subjects' RaF and compliance with the GDPR.

Keywords: the GDPR, personal data processing, a high risk, a DPIA, obscurities

LIST OF ABBREVIATION

CFR	Charter of Fundamental Rights of the European Union
CSS	Camera surveillance system
DDPO	Deputy Data Protection Ombudsman
DIS	Driving information system
DPD95	Directive 95/46/EC
DPIA	Data protection impact assessment
EU	European Union
FDPO	Finnish Data Protection Ombudsman
GDPR	General Data Protection Regulation 2016/679
IoT	Internet of Things
MS	Member States
ODPO	Office of Data Protection Ombudsman
PIA	Privacy impact assessment
RaF	Rights and freedoms
SA	Supervisory Authority
SAs	Supervisory Authorities
WP29	Article 29 Data Protection Working Party

INTRODUCTION

Contemporary technologies are evolving quickly along with science's development and in order to handle the new and altered circumstances, laws must be brought up to date.[1] Thus, the world can be seen to be in a state of flux due to the current and ongoing globalization, technologization, and digitalization, and lately, changes have also occurred in the data protection fields. To add, the usage of large amounts of data, such as personal data, is said to direct our economy.[2] Furthermore, the European Union General Data Protection Regulation 2016/679 (GDPR) as a new piece of data protection legislation came into force on 25 May 2018.[3] It is described as data protection's "Magna Carta" of which significance cannot be exaggerated.[4] One new obligation established under GDPR's Article 35 requires controllers to conduct a data protection impact assessment (DPIA), especially when using new technologies, if the personal data processing is "likely to result a high risk" to natural persons' rights and freedoms (RaF).[5]

Article 35 is an interesting research topic due to its complexity and novelty. Furthermore, the GDPR's enforcement, including a DPIA under Article 35, has brought changes to data protection and personal data processing fields. The problem addressed by this paper concerns Article 35's ambiguity and complexity, especially, concerning the correct determination of when processing is likely to cause a high risk to data subjects' RaF, thus, when to conduct a DPIA under Article 35, which might danger its correct interpretation and application. To emphasize, the GDPR does not provide definitions for Article 35's important concepts and elements that should be clear and understandable for controllers to correctly apply Article 35. The aim of this research is to analyze

[1] Bu-Pasha, S. (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). Routledge, 391-402. 391.
[2] Hijmans H. (2016) Making Article 16 TFEU Work: Analysis and Conclusions. In: *The European Union as Guardian of Internet Privacy.* Law, Governance and Technology Series, 31, (511-564). Cham: Springer International Publishing. 513.
[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, 1-88.
[4] Gal, M. S., & Aviv, O. (2020). The competitive effects of the GDPR. *Journal of Competition Law & Economics*, 16(3). Oxford University Press, 349-391. 349.
[5] Regulation 2016/679, *supra nota* 3, Art.35.

whether Article 35, especially, "likely to result in a high risk"[6] under Article 35, includes any obscurities that could endanger Article 35's correct interpretation and application, and to propose solutions to overcome the obscurities. Thus, the research question is whether Article 35, especially the likelihood of a high risk and the obligation to conduct a DPIA under Article 35 includes obscurities that could endanger Article 35's correct interpretation and application, and whether those obscurities could be clarified. The hypothesis is that there are some obscurities to be clarified concerning Article 35. The research is conducted with qualitative methods as the topic will be examined in light of relevant legislation, guidelines, literature, and two decisions on the obligation to conduct a DPIA under Article 35 given by the Finnish Data Protection Ombudsman (FDPO) and Deputy Data Protection Ombudsman (DDPO).

To highlight, to achieve the aim of this paper, thus, to identify possible obscurities of Article 35, especially, of the likelihood of a high risk under Article 35, it is necessary to first go through and understand Article 35, its relevant paragraphs, GDPR's relevant Recitals concerning the determination of likelihood of a high risk, and Article 29 Data Protection Working Party's (WP29) official guidelines that facilitate the interpretation of when there is a likelihood of a high risk in accordance with Article 35. Moreover, the DPIA's background should be looked over and some GDPR's Articles that are closely connected to Article 35 and a DPIA are useful to be assessed to reflect the impact and scope of Article 35.

Thus, chapter one introduces the data protection's legislative background, covering the GDPR's predecessor, i.e., the Data Protection Directive (DPD95)[7], and the GDPR. Chapter two briefly introduces the earlier privacy impact assessment (PIA) in relation to a DPIA and criticism address to a DPIA. It also introduces the DPIA and Article 35, covering only Article 35's paragraphs that concern this research topic, and clarifies some relevant GDPR's Articles and notions. In turn, chapter three focuses on assessing more profoundly when processing is likely to result in a high risk, also under WP29's relevant guidelines that aim to clarify when there is a likelihood of a high risk, and also analyzing and discussing some presented unclarities relating to the determination of the likelihood of a high risk and the obligation to conduct a DPIA under Article 35. Chapter 4 assesses how Article 35 has been interpreted in the two recent Finnish decisions and whether, based on the decisions, some obscurities of Article 35 can be pointed out. As the research focuses

[6] *Ibid.*
[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJ L 281,23.11.1995, 31–50.

on Article 35, the decisions are analyzed insofar as Article 35 is concerned. Those decisions were chosen because they are closely focusing on the obligation to conduct a DPIA under Article 35, and they are decisions from author's home country. Additionally, due to the research's limited word count, it is more useful to focus on them. Chapter five connects the identified obscurities of Article 35 to the proposed solutions.

1. LEGAL BACKGROUND OF DATA PROTECTION

Data is said to be "the new oil".[8] Additionally, awareness towards the data protection's significance has increased.[9] Thus, as the processing of personal data increases, more attention is also given to data protection. In fact, the right to protection of personal data is a valued EU fundamental right since the Treaty on the Functioning of the European Union and the Charter of Fundamental Rights of the European Union (CFR) both provide everyone a right to protection of personal data. However, the CFR differs from other human rights legislation by introducing the right to data protection as an individual right, while many others incorporate it into a right to privacy.[10]

1.1. Data Protection Directive 95/46/EC and General Data Protection Regulation 2016/679

Before the GDPR, a right to data protection was guaranteed by the DPD95. One of the DPD95's purposes was to harmonize data protection.[11] Yet, It did not impose a similar obligation to conduct such an impact assessment as the GDPR does.[12] Though, it emphasized that "certain processing operation are likely to pose specific risks to the rights and freedoms to data subjects by virtue of their nature, their scope or their purposes, such as that of excluding individuals from a right, benefit of a contract, or by virtue of the specific use of new technologies", yet it was voluntary for the

[8] Bhageshpur, K. (2019). *Data Is The New Oil - - And That's A Good Thing.* Forbes. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/?sh=799f82c73045, 24 March 2021.
[9] Rodotà S. (2009) Data Protection as a Fundamental Right. In: Gutwirth, S. *et al.* (Eds.) *Reinventing Data Protection?* (77-82). Dordrecht: Springer. 77.
[10] Lynskey, O. (2014). Deconstructing Data Protection: The Added-Value of Right to Data Protection in the EU Legal Order. *International and Comparative Law Quarterly*, 63(3). Cambridge University Press, 569-598. 569-570.
[11] Tikkinen-Piri, C. *et al.* (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1). Elsevier. 134-153. 136.
[12] Bieker, F *et al*. (2016). A Process for Data Protection Impact Assessment under the European General Data Protection Regulation. In: Schiffner, S. *et al.* (Eds.) *Privacy Technologies and Policy* (21-37), APF 2016, LNCS 9857, Cham: Springer, 22.

Member States (MS) to decide whether to specify those risks in their laws.[13] Moreover, MS should determine processing operations that were likely to present specific risks to data subject's RaF and check that the processing operations were examined before the start and such prior checks were done by the Supervisory Authority (SA) by the controller's or data protection officer's request.[14] Although, the DPD95 seemed to recognize some risky personal data processing operations affecting data subject's RaF, the risk assessment's role can be seen to remained rather low. Moreover, referring to above, it rather transferred the responsibility to specify processing operations, that were likely to present specific risks to data subject's RaF, to the MS.

Eventually, the DPD95 did not adequately correspond with privacy requisites at the time, which led to adopting the GDPR that aims to harmonize and enhance the protection of personal data.[15] To mention, unlike directives, regulations are directly applicable in all MS[16]. Moreover, it has said to be the EU's effort to tackle, for example, the DPD95's inadequacy.[17] Additionally, it aims to "raise the level of privacy for the affected individuals".[18] Thus, establishing the obligation to conduct a DPIA under Article 35 can also be seen to strengthen the fulfillment of GDPR's aims, for example, by promoting data protection. However, though the GDPR is said to provide safeguarding regulatory frames for data protection, it is criticized for being long and complex piece of legislation as it contains nearly 100 provisions and the GDPR's text is claimed to be partly obscure.[19]

[13] Directive 95/46/EC, *supra nota* 7, Rec.53.
[14] *Ibid.*, Art.20.
[15] Tikkinen-Piri, C. *et al.* (2018), *supra nota* 11, 135.
[16] Craig, P., & De, B. G. (2015). *EU law: Text, cases, and materials*. 6th edition. New York: Oxford University Press.106-108.
[17] Hoofnagle, C.J. *et al.* (2019). The European Union General Data Protection Regulation: What it is and What it Means. *Information & Communications Technology Law*, 28(1). Routledge. 65-98.71
[18] Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. (1st Ed). Cham, Switzerland: Springer International Publishing. 1.
[19] Hoofnagle, C.J. *et al.* (2019), s*upra nota* 17, 67,98.

2. ARTICLE 35 AND ITS BACKGROUND

2.1. The obligation to conduct a data protection impact assessment under Article 35

In this subsection, Article 35's paragraphs relating to this research topic are presented. Regarding the definition of a DPIA, it has been described, for example, as "an instrument to identify and analyze risks for individuals, which exist due to the use of certain technology or system by an organization in their various roles" and of which assessment's result allows to determine the adequate measures to be taken to address the recognized risks.[20] Thereby, performing a DPIA allows controllers to recognize and assess potential risks to natural persons' RaF resulting from personal data processing, and also to react to them. Moreover, it has been presented that a DPIA can have the qualities to safeguard natural persons' RaF and to be a tool to be used to obey the GDPR's obligations.[21] Thereby, it is also important to assess carefully whether there is a need to conduct a DPIA under Article 35.

According to Article 35(1), "where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purpose of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, a 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".[22] Furthermore, to assess the likelihood and severity of the identified high risk resulting from personal data processing, the DPIA shall be performed.[23] Moreover, as the DPIA

[20] Bieker, F *et al*. (2016), s*upra nota* 12, 21-22.
[21] *Ibid.*,22,36.
[22] Regulation 2016/679, *supra nota* 3, Art.35.
[23] *Ibid.,* Rec.90.

must be conducted before processing, it appears to ensure that possible risks likely to arise from the processing are recognized before they emerge.

In turn, Article 35(3) supplements Article 35(1), as it illustrates when a high risk is likely to occur stating that a DPIA is required to be done "in particular, in case of: a) systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person, b) processing on a large scale of special categories of data referred to in Article 9(1) or of personal data relating to criminal convictions and offences referred to in Article 10 or c) a systematic monitoring of a publicly accessible on a large scale".[24] According to Article 9(1), special categories cover data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".[25] Yet, also emphasized by others, the wording in the beginning of Article 35(3), signifies that situations under it are non-exhaustive, as Article 35(3) especially covers three situations in which a high risk is likely to arise and a DPIA is required. [26] Thus, other processing operations than those listed therein might be covered, for example, by Article 35(1) and be subject to a DPIA. Moreover, for assessing the likelihood of a high risk, WP29 has established "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of the Regulation 2016/679"[27] (the Guidelines).

As for the SAs' role, Article 35 leaves some discretion for a national SA who, in accordance with Article 35's paragraphs 4 and 5, can decide to make public the lists of kinds of processing operations that are and are not subject to a DPIA, and communicate the lists to the European Data Protection Board (Board) to review.[28] Moreover, the GDPR provides some flexibility to MS to

[24] *Ibid.,* Art.35(3).
[25] *Ibid.,* Art.9(1).
[26] Demetzou, K. (2019). Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation. *The Computer Law and Security Report*, 35(6), 105342. Elsevier, 1-14,6.
[27] 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. WP 248 rev 0.1,4 April 2017. Retrieved from: https://tietosuoja.fi/documents/6927448/8316711/Guidelines+on+Data+Protection+Impact+Assessment.pdf/def06c04-03f9-4505-99d2-709243ef2d35/Guidelines+on+Data+Protection+Impact+Assessment.pdf, 4 February 2021.
[28] Regulation 2016/679, *supra nota* 3, Art.35(4)-(5).

pass rules in particular areas.[29] As Article 35's last paragraph, paragraph 11 requires controllers to reassess if processing complies with the GDPR at least when there is a change of the risk represented by the processing.[30]

2.2. The privacy impact assessment versus the data protection impact assessment

A DPIA, established under the GDPR, is "the first risk management tool to be enshrined in EU data protection law".[31] Yet, an impact assessment concept, known as a PIA, has also been in use, for instance, the UK created its PIA method in 2007, and Ireland in 2010, and also other countries, for example, Australia, New Zealand, Canada, and the US have created their PIA methods.[32] A PIA is defined, for instance, as "a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary to avoid or minimize negative impacts and which helps to point out potential privacy issues".[33] As the name and the above definition already indicate, the PIA appears to focus on privacy matters. Moreover, the DPIA has been argued for not seeming to cover as much as the PIA.[34] The former as a term has also been claimed to correlate merely with verifying legal requisites laid down by the data protection framework in Europe.[35] Whereas, the latter has been said to function as not only verifying and ensuring that laws and requirements concerning privacy are being abided by but also going further in terms of a risk assessment to ensure that the potential risks are recognized and addressed.[36] Nevertheless, a DPIA has now been established as a mandatory obligation under Article 35. In fact, it has been presented that as it addresses risk

[29] Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. *International Journal of Market Research*, 59(6). SAGE Publishing, 703-705.704.
[30] Regulation 2016/679, *supra nota* 3, Art.35((11).
[31] Gellert, R. (2018). Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review*, 34(2). Elsevier, 279-288. 279.
[32] Wright, D. (2012). The State of the Art in Privacy Impact Assessment. *Computer law & Security Review*, 28(1). Elsevier, 54-61. 54-55,58.
[33] *Ibid.*,55.
[34] *Ibid.*,57, referenced in Yordanov, A. (2017). Nature and Ideal Steps of the Data Protection Impact Assessment Under the General Data Protection Regulation. *European Data Protection Law Review, 3(4)*, 486–495, 487.
[35] De Hert, P. (2012). A Human Rights Perspective on Privacy and Data Protection Impact Assessments. In: Wright, D.&De Hert, P. (Eds.) (2012) *Privacy Impact Assessment*. Law, Governance and Technology Series, 6. Dordrecht: Springer, 33-76.34, referenced in Yordanov, A. (2017), *supra nota* 34.
[36] Wright, D. (2012), *supra nota* 32, 57.

impacts on natural persons' RaF and the PIA addresses impacts on privacy, the former, covering also other rights and freedoms than privacy, could be considered broader than the latter.[37]

2.3. Related Articles and notions to Article 35

This subsection will briefly cover other GDPR's Articles and clarify some notions and actors closely connected to Article 35. Firstly, the GDPR applies to processing of personal data.[38] Thereby, a DPIA must be done only when processing personal data. In turn, personal data is referred to as "data that directly or indirectly relates to an identified or identifiable natural person".[39] For example, names, locations, and IP addresses are all considered as personal data.[40] The controller is the one starting to process personal data and bearing liability to comply with the GDPR, and if a controller fails to comply with Article 35, one is held accountable for doing so.[41] Supervisory Authorities (SAs) are introduced as independent public authorities designated by MS and they can issue the lists of such processing operations for which a DPIA is or is not required.[42] For example, the FDPO is a SA under the GDPR. Furthermore, the processing covers different types e.g., collection, storage, and use, meaning "any operation or set of operation performed on personal data or on sets of personal data, whether or not by automated means".[43]

The principle established under Article 5(2) is described as GDPR's "hallmark".[44] To emphasize, Article 5(2) states that the controller is liable for, and must be able to demonstrate compliance with Article 5(1) that introduces the data protection principles.[45] Thus, Article 5(2) obliges organizations to evidence that they in fact comply with the GDPR's data protection principles and requirements, and one way to ensure compliance with Article 5(2) is to obey Article 35.[46] Thus,

[37] Ferra, F. *et al.* (2020). Challenges in assessing privacy impact: Tales from the front lines. *Security and Privacy*, 3(2), e101. John Wiley & Sons, Ltd,1-19. 3.
[38] Regulation 2016/679, *supra nota* 3, Art.2-3.
[39] Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, 10(1). Oxford: Oxford University Press, 11–36. 12.
[40] *What is personal data*? Office of the Data Protection Ombudsman. Retrieved from https://tietosuoja.fi/en/what-is-personal-data, 4 February 2021.
[41] Demetzou, K. (2019), *supra nota* 26, 3,14.
[42] Regulation 2016/679, *supra nota* 3, Art.4(21), Art.35(4)-(5).
[43] *Ibid.,* Art.4(2).
[44] Mondschein C.F., Monda C. (2019) The EU's General Data Protection Regulation (GDPR) in a Research Context. In: Kubben P., *et al.* (eds) Fundamentals of Clinical Data Science. (55-71) Springer, Cham, 58.
[45] Regulation 2016/679, *supra nota* 3, Art.5.
[46] Bhaimia, S. (2018). The General Data Protection Regulation: The Next generation of EU Data Protection. *Legal Information Management*, 18(1). Cambridge University Press, 21-28. 25; Tikkinen-Piri, *et al.* (2018), *supra nota* 11, 139

Article 5(2) is clearly connected with Article 35. In turn, under Article 25 controllers must, when determining processing means and when processing, create "appropriate technical and organizational measures" to fulfill GDPR's requirements and protect data subjects' rights.[47]. The technical and organizational measures are to be applied to guarantee the objectives of the data protection.[48] In fact, one way to embed organizational measures under Article 25 is to conduct a DPIA.[49] Furthermore, the connection between Articles 25 and 35 can be seen to emerge also from the *ex-ante* nature of requirements to adopt the organizational measures before processing under Article 25 and to perform a DPIA before processing under Article 35.

Moreover, Article 36 requires controllers to consult a SA before processing if a DPIA "under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk".[50] Lastly, if controllers do not perform a DPIA under Article 35 when they should and infringe Article 35, administrative fines, that may extend up to 10 000 000 euros or, if an undertaking, up to 2% of the preceding financial year's worldwide turnover, whichever is higher, might be imposed under Article 83(4).[51] Imposing such high amounts of administrative fines might also affect controller's economy.

[47] Regulation 2016/679, *supra nota* 3, Art.25
[48] Rubinstein, I., & Good, N. (2020). The trouble with Article 25 (and how to fix it): the future of data protection by design and default. *International Data Privacy Law*, 10(1). Oxford University Press, 37–56. 37.
[49] Tikkinen-Piri, C. *et al.* (2018), *supra nota* 11, 142.
[50] Regulation 2016/679, *supra nota* 3, Art.36.
[51] *Ibid.*, Art.83(4)(a).

3. "LIKELY TO RESULT IN A HIGH RISK" AND THE IDENTIFIED OBSCURITIES

3.1. General considerations

As regards the obligation to conduct a DPIA under Article 35, it is not an obligation to be done once, but a DPIA shall be conducted continually alongside the processing.[52] Thereby, and by referring to previous, it seems that for a DPIA to function as effectively as it can and to fulfill its purposes and address risks, controllers should also make it a continual process. Furthermore, not all risks must be eliminated by conducting a DPIA, but they should be reduced to the appropriate level when considering personal data processing's purposes.[53] As known, risks are something that always exists, they cannot be fully prevented or eliminated but they can be managed and tolerated.

However, conducting a DPIA under Article 35 has been criticized as a complex obligation requiring expertise from corporations, *inter alia*, legal knowledge[54]. Moreover, costs of complying with the GDPR are claimed to be high.[55] Consequently, conducting a DPIA is said to cause and raise costs for organizations.[56] To highlight, Article 35 is a long and wide Article including 11 separate paragraphs under it. Thus, it seems not a surprise that it is considered as a complex obligation. However, there are also benefits in performing a DPIA as it, for example, provides protection for individuals, ensures compliance with the GDPR, creates financial benefits for

[52] Article 29 Data Protection Working Party (4.4.2017), *supra nota* 27, 14.
[53] *What is a DPIA?* ICO. Retrieved from: 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/#what2, 10 February 2021.
[54] Sarrat, J., & Brun, R. (2018) DPIA: How to Carry out One of the Key Principles of Accountability. In: Medina, M. *et al.* (Eds.) *Privacy Technologies and Policy* (172-182), APF 2018, LNCS 11079. Cham: Springer. 173.
[55] Layton, R (2017). How the GDPR Compares to Best Practices for Privacy, Accountability and Trust. SSRN, 1-23.2.
[56] Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, 2016(6). Elsevier, 5-8.5; Burri, M., & Schär, R. (2016). The reform of the EU data protection framework: outlining key changes and assessing their fitness for a data-driven economy. *Journal of Information Policy*, 6(1). Pennsylvania University Press, 479-511.502.

controllers, and promotes the controller's reputation and customer relations.[57] Thereby, such benefits could also be seen to function as encouragements for controllers to conduct a DPIA under Article 35.

3.2. "Likely to result in a high risk" and the obscurities

Regarding a DPIA and the risks it shall address, the GDPR states that "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" at least when processing may lead, e.g., to discrimination, identity theft, fraud, damage to a reputation, financial loss, or may concern, for example, personal data processing relating to vulnerable data subjects.[58] Furthermore, risks are said to be formed of events and consequences.[59] By referring, for example, to GDPR's Recital and the obligation to conduct a DPIA under Article 35, it can be seen that there are at least two kinds of risks established under the GDPR, i.e. a high risk and a risk[60], and Article 35 must be applied only if high risks are likely to arise.

To assess the risk's likelihood and severity, controllers must consider the nature, scope, context and purposes of processing and the assessment must be done objectively.[61] Thus, the outcome illustrates whether the risk is high and a DPIA must be conducted. Emphasis has also been given to Recital 84 that guides to assess what must be considered with regard to a high risk, that is, the risk's origin, nature, particularity and severity.[62] Eventually, the DPIA itself is conducted to determine high risk's likelihood and severity by assessing the nature, scope, context and purposes of processing and risk sources.[63] However, the GDPR neither provides any definition for a high risk nor clarifies the above concepts and elements, such as nature, scope, context and purposes of processing which all shall be assessed in order to determine correctly whether to conduct a DPIA.

[57] *What is a DPIA?*. ICO, *supra nota* 53.
[58] Regulation 2016/679, *supra nota* 3, Rec.75.
[59] Gellert, R. (2018), *supra nota* 31,280.
[60] Regulation 2016/679, *supra nota* 3, Art.35, Rec.76.
[61] *Ibid.*, Rec.76.
[62] Raab. C.D., (2020) Information privacy, impact assessment, and the place of ethics. *Computer law & security review*, 27. Elsevier, 1-16.8.
[63] Regulation 2016/679, *supra nota* 3, Rec.90.

Moreover, additional guidance for assessing the likelihood of a high risk is provided under the GDPR and a DPIA is also required, for example, for "large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk", for using new technologies on a large-scale causing a high risk to data subjects RaF, or for processing that is used to make decisions concerning particular individuals, based on profiling and when processing of biometric data or special categories of personal data, or data concerning criminal convictions and offences, and for "monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices", or if a competent SA assesses there to be a high risk to data subjects' RaF.[64] Yet, as established above, Article 35(3) provides three situations where a high risk is likely to emerge and for which a DPIA is especially required without clarifying its content or concepts, those being, for example, systematic or extensive evaluation, large-scale processing, and systematic monitoring, and the controller oneself must assess whether to conduct a DPIA for a specific processing. Additionally, the above Recital 91 provides some examples of processing operations likely to cause a high risk, yet it does not either appear to clarify its content more profoundly. To strengthen the previous argument, the GDPR does not provide clear definitions for concepts like large-scale processing, systematic monitoring, systematic and extensive evaluation, or legal or similar significant effects which are one of the criteria under Article 35(3) to be considered when determining whether the processing is likely to cause a high risk to data subjects' RaF.

As indicated, SAs have also compiled lists of kinds of processing operations requiring a DPIA in accordance with Article 35(4). As the two recent decisions analyzed in this research are Finnish decisions, it is appropriate to refer to guidance given by the Finnish Office of Data Protection Ombudsman (ODPO) regarding when to conduct a DPIA. Thereby, the FDPO has compiled a list based on the Guidelines and specifying Article 35 In short, the list requires a DPIA to be conducted for personal data processing when biometric data, genetic data or location data is processed, or data is processed in whistleblower systems.[65] In the list and for each category mentioned, criteria of large-scale processing, systematic monitoring and legal or similar significant effects are all mentioned but not defined, which might make it difficult for controllers to assess the need for a

[64] *Ibid.*, Rec.91.
[65] *List compiled by the Office of the Data Protection Ombudsman of processing operations which require data protection impact assessment (DPIA).* (2018). The Office of Data Protection Ombudsman. Retrieved from https://tietosuoja.fi/en/list-of-processing-operations-which-require-dpia, 10 February 2021.

DPIA as they have to evaluate if the data processed concerns any of the data categories mentioned, for example, location data, and if the processing is considered as of those under the above criteria. Thus, controllers must use discretion to assess whether the processing falls under the FDPO's list.

3.2.1. Analysis of "likely to result in a high risk" under Article 29 Data Protection Working Party's Guidelines

In this subsection, the Guidelines and their usefulness regarding the determination of whether there is a likelihood of a high risk, in accordance with Article 35, are assessed. The WP29, nowadays the Board, has formed nine criteria in the Guidelines to facilitate determining when the processing is likely to present a high risk to natural persons' RaF. WP29 defines a risk as "a scenario describing an event and its consequences, estimated in terms of severity and likelihood".[66] Although the Guidelines do not have the corresponding legal status with the GDPR, they seem to be useful to be referred to when assessing whether a DPIA should be conducted as they provide some clarification for interpreting the obligation to conduct a DPIA under Article 35. Moreover, the Guidelines are also referred to in the two Finnish decisions analyzed later, therefore, it is also important to analyze them.

The first criterion is "evaluation or scoring, including predicting and profiling"[67], forming also a part of Article 35(3)(a). The GDPR defines profiling as "any form of automated processing of personal data consisting of the use of personal data to evaluate specific personal aspects relating to natural persons, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements".[68] The second criterion, also mentioned under Article 35(3)(a), is "automated decision-making with legal or similar significant effect" individuals, and in order that the criterion is fulfilled, the effect cannot be little or non-existent.[69] Yet, the second criterion, espeacially the legal or similar significant effects, is not determined very clearly under the Guidelines and thus, remains vague. Thereby, discretion is left for controllers to assess whether the effect is such that falls under Article 35.

[66] Article 29 Data Protection Working Party (4.4.2017), *supra nota* 27, 6.
[67] *Ibid.*,9.
[68] Regulation 2016/679, *supra nota* 3, Art.4(4).
[69] Article 29 Data Protection Working Party (4.4.2017), *supra nota* 27, 9.

The third criterion is the "systematic monitoring" relating to personal data processing used for monitoring, controlling or observing data subjects, covering data collected via networks or the systematic monitoring under Article 35(3)(c).[70] WP29 has stated that data could be collected in situations where data subjects might not be aware of the processing or its purposes, therefore, systematic monitoring is considered as one criterion.[71] Systematic monitoring is further interpreted under the "Guidelines on Data Protection Officer ('DPO')", (DPO Guidelines), according to which, systematic is considered as denoting to take place through a system, or is prearranged, organized or methodical, or occurs as part of a general plan for data collection, or is performed as part of a strategy, for example, location tracking, loyalty programs or monitoring health data through wearable devices.[72] Thus, in order to make the correct decision on whether to conduct a DPIA, controllers should also assess DPO Guidelines to analyze more thoroughly whether the processing is considered systematic monitoring.

"Sensitive data or data of highly personal nature" is the fourth criterion, also listed under Article 35(3)(b), and WP29 emphasizes that the criterion covers special categories of data under Article 9, such as political opinions, and personal data relating to criminal convictions or offences under Article 10.[73] However, there could also be other data types raising the risk to be high, since such personal data concerns activities relating to household, or affects fundamental rights, or because infringing such personal data clearly and severely affects data subject's everyday life.[74] Thus, the scope of sensitive data categories, subject to processing and potentially to a DPIA, is broad, potentially covering more than stated under Article 35(3)(b). In turn, large-scale processing is the fifth criterion under the Guidelines, also covered by Article 35. The Guidelines by referring to the DPO Guidelines aim to clarify the concept by stating that the amount of data subjects concerned, data's volume or different data items' range, permanence or duration and the geographical extent of the processing activity must be considered when assessing the occurrence of large-scale processing.[75] Thus, by assessing the above factors, controllers could evaluate whether the processing falls under the criterion of being subject to a DPIA. Yet, the Guidelines and DPO

[70] *Ibid.*
[71] *Ibid.*
[72] Article 29 Data Protection Working Party. Guidelines on Data Protection Officer. WP 243. 13 December 2016, 9. Retrieved from: https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A, 4 February 2021.
[73] Article 29 Data Protection Working Party (4.4.2017), *supra nota* 27, 9-10.
[74] *Ibid.*
[75] Article 29 Data Protection Working Party (13.12.2016), *supra nota* 72, 7.

Guidelines only provide some factors to be considered when assessing the criterion of large-scale but do not clearly define it.

The sixth criterion is "matching or combining datasets" and the seventh concerns vulnerable data subjects' data and is listed under the Guidelines due to the power imbalance prevailing between controllers and data subjects, for example, between an employee and an employer, also children fall under this criterion.[76] The eighth criterion is the "innovative use or applying new technological or organizational solutions" as a high risk can emerge due to using such above solutions that may contain new data usage or collection types.[77] The use of new technologies is also listed under Article 35(1) and Recital 91. Examples of processing applying new innovative technologies can cover, e.g., the use of artificial intelligence [78] and Internet of Things (IoT).[79] Moreover, applying smart devices in processing of personal data would likely fall under Article 35.[80] To note, regarding the IoT and artificial intelligence, the Commission has emphasized that the increased use of such solutions will create benefits, yet new risks will also emerge.[81] Lastly, the ninth criterion states, by referring to the GDPR, that if the processing "prevents data subjects from exercising a right or using a service or a contract", there might be an obligation to perform a DPIA as a high risk is likely to occur.[82]

To conclude, as can be seen the Guidelines provide some facilitation for assessing whether the processing is likely to present a high risk and a DPIA should be conducted under Article 35 by issuing nine criteria to be assessed in terms of deciding whether to conduct a DPIA. However, especially regarding the concepts of systematic monitoring, large-scale processing, systematic and extensive evaluation and legal or similar significant effects, WP29 rather specifies what is to be considered when assessing those concepts, but some of them, such as large-scale processing, still appears to remain subject to interpretation under WP29's guidelines as well. Furthermore, based

[76] Article 29 Data Protection Working Party (4.4.2017), *supra nota* 27, 10.
[77] *Ibid.*
[78] Ivanova Y. (2020) The Data Protection Impact Assessment as a Tool to Enforce Non-discriminatory AI. In: Antunes L., *et al.* (eds) *Privacy Technologies and Policy*. APF 2020. LNCS, 12121. Springer, Cham, 3-24. 5
[79] Bu-Pasha, S (2020), *supra nota* 1, 399.
[80] Lindqvist, J. (2018). New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things? *International journal of law and information technology*, 26(1). Oxford University Press, 45-63.57.
[81] European Commission Communication from the Commission to the European Parliament, the European Council, the, Council, the European Economic and Social Committee and the Committee of the Regions (2020), *The EU Security Union* Strategy. 3. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605, 6 March 2021.
[82] Article 29 Data Protection Working Party (4.4.2017), *supra nota* 27, 11.

on the above analysis, for example in terms of assessing and interpreting whether the processing is considered as systematic monitoring, it could be wise to also review the DPO Guidelines when assessing the concepts to correctly interpret it and to comply with Article 35. Moreover, as in some situations, the fulfillment of not two, but one criterion may require conducting a DPIA[83], which means that the controller oneself must assess the situation and make the decision on whether to conduct it.

3.2.2. Unclarities and aspects to consider

Although a DPIA under Article 35 is a new obligation it has been addressed to some extent, also in terms of the likelihood of a high risk. Moreover, some obscurities and issues regarding a DPIA under Article 35 are found and discussed below.

It has been presented that the data protection field does not have a uniform perception of what even constitutes a risk.[84] Referring to the previous sentence, thus, it appears possible that risks could be understood and defined differently. For example, as regards the GDPR, it has been presented that the risk concept in the GDPR, can be seen as a "compliance risk" denoting that, "the lower the compliance or the higher the "non-compliance event" the higher the (vernacular) risk (i.e., consequence or harm) to the data subjects' fundamental rights".[85] Referring to the previous sentence and its risk concept, to conclude, if controllers do not comply with the obligations and requirements established under the GDPR and its provisions, including Article 35, it affects negatively data subjects' RaF. Moreover, the described concept of a risk does not seem to consider only the compliance with the GDPR, but also the protection of data subjects' RaF. Thereby, referring to the above concept of risk, it could be indicated that compliance and protection of data subjects' RaF go hand in hand.

In turn, the phrase of likely to present a high risk to natural persons' RaF under Article 35(1) can be seen as ambiguous and vague. WP29 has stated by referring to the GDPR that risks are measured in terms of likelihood and severity.[86] Moreover, the notion of high is said to relate to the risk's high

[83] *Ibid.*
[84] Centre of Information Policy Leadership (CIPL), Hunton & Williams LLP. (2016). Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR. *CIPL GDPR Interpretation and Implementation Project. 13.* Retrieved from *https://iapp.org/resources/article/risk-high-risk-risk-assessments-and-data-protection-impact-assessments-under-the-gdpr/,* 10 February 2021.
[85] Gellert, R. (2018), *supra nota* 31, 279,282.
[86] Article 29 Data Protection Working Party (4.4.2017), *supra nota* 27, 6.

severity and high likelihood, thus, controllers shall estimate the severity of a risk and the likelihood of whether it emerges to assess whether to conduct a DPIA under Article 35.[87] Furthermore, the nature, scope, context and purposes of the processing are elements to be assessed every time personal data is processed to determine the risk stage, and by assessing risks objectively it is possible to determine whether risks or high risks arise from data processing.[88] Hence, by analyzing the above elements, controllers can decide which obligations they must take to comply with the GDPR. Regarding the determination of the likelihood of a high risk, the GDPR is said to guide controllers to assess different high risky processing operations through a method of denotation by providing non-exhaustive examples of risky processing operations for controllers.[89] Moreover, as Article 35(3) covers three situations that especially require a DPIA, thus, not all risky processing operations requiring a DPIA are covered by it, which could potentially create a gap for Article 35's interpretation and application. In other words, there might be processing operations likely to cause a high risk which do not fall under Article 35(3) but still require a DPIA to be conducted under Article 35(1). This can be considered problematic because Article 35(1) remains vague to some extent regarding the undefined concepts under it and in turn, Article 35(3) does not cover all processing operations that might still require a DPIA, which could danger the protection of data subjects' RaF and compliance to conduct a DPIA under Article 35.

As written and emphasized earlier, the DPIA under Article 35 has been criticized as being a complex obligation to conduct, and thus, expertise is required.[90] If there is a lack of sufficient knowledge to conduct a DPIA, there is a chance that controllers do not apply Article 35 correctly, which could lead to endangering data subject's RaF. Regarding the concepts under Article 35, e.g., systematic monitoring, large-scale processing, legal or similar significant effects, new technologies or the processing's nature, scope, context, purposes[91], Article 35 or the GDPR do not clarify such concepts or how to interpret them. Actually, the vagueness of the terminology is argued to be a reason for many issues concerning the responsibility to perform a DPIA under Article 35.[92] For now, interpretation is needed when assessing whether the processing is, for instance, large-scale.

[87] Demetzou, K. (2019), *supra nota* 26, 5.
[88] Regulation 2016/679, *supra nota* 3, Rec.76.
[89] Demetzou, K. (2019), *supra nota* 26,6-8.
[90] Sarrat, J., & Brun, R. (2018), *supra nota* 54,173.
[91] Regulation 2016/679, *supra nota* 3, Art.35.
[92] Kloza, D. *et al.* (2019). Towards a Method for Data Protection Impact Assessment: Making sense of GDPR Requirements. *d.pia.lab Policy Brief*, 1(2019), 1-8.2.

However, as for the nature, scope, context and purposes, for example, the ODPO has given examples to consider when assessing those elements and consequently, the likelihood of a high risk. It has instructed that when assessing the nature of processing, controllers must pay attention to, e.g., personal data's special categories, data subjects' vulnerability and new innovations and technologies, and in turn, when determining the scope, one needs to consider the amount of data subjects, data's volume and geographical ambit.[93] In turn, when assessing the purposes, controllers estimate whether data is processed, for instance, to monitor, track, evaluate or rate data subjects, or whether there are legal effects arising from automated decision-making, and as for the context, the attention shall be given to confidentiality, privacy's protection and combining collected personal data in varying contexts.[94] Yet, these are only national examples that can be considered when assessing the above elements, also established under Article 35(1), to help determining risk's likelihood and severity.

Moreover, it has been emphasized that as the obligation to conduct a DPIA covers many different processing cases, it might be very challenging for controller to assess the situation in question and to conclude whether the processing would be subject to the obligation to do a DPIA under Article 35.[95] To demonstrate and as indicated above, Article 35(3) covers three processing operation cases for which a DPIA is especially required without clarifying the important concepts mentioned also earlier. Thus, it seems to be subject to interpretation. In turn, a DPIA under Article 35(1) has been questioned for its ambivalent wording, since it is challenging to identify what the impact assessment's object is – the likelihood of high risk to data subject's RaF or the effects on personal data protection.[96] By referring to Article 35's wording, it seems that the objective is to assess the likelihood of the risks to data subjects' RaF. Yet, as Article 35(1) does not clarify its content and the related concepts, it can also be seen to be subject to interpretation.

Additionally, despite the criticism regarding, for instance, the vagueness of certain concepts, as written above, the obligation to conduct a DPIA under Article 35 depends on whether there is a likelihood of a high risk. Thus, some flexibility and interpretation regarding a DPIA should also be provided for organizations.[97] Furthermore, regarding the WP29's Guidelines and the criteria,

[93] *Risk assessment and data protection planning*. Office of Data Protection Ombudsman. Retrieved from https://tietosuoja.fi/en/risk-assessment-and-data-protection-planning, 22 February 2021.
[94] *Ibid.*
[95] Voigt, P., & Von dem Bussche, A. (2017), *supra nota* 18,48.
[96] Gellert, R. (2018), *supra nota* 31, 280.
[97] CIPL, Hunton & Williams LLP. (2016), *supra nota* 84, 5–6,29.

such as large-scale processing, it has been emphasized that applying the criteria requires interpretation from the organizations as they have to "specify" the criteria under the Guidelines to match with their processing operations.[98] Moreover, as regards the large-scale processing, for example, in the *Taksi Helsinki Oy* decision analyzed later, processing personal data of hundreds of thousands of data subjects has considered to constitute a large-scale processing.[99] Yet to mention, as the Guidelines, by referring to the DPO Guidelines, only provide different factors to be considered when assessing if the criterion of large-scale processing is met, it seems that the criterion could cover processing operations in a wide range and interpretation is required.

3.3. Other unclarities

In addition to the above issues and aspects, there are still other unclarities to address, concerning Article 35. As written, Article 35(1) requires a DPIA to be conducted when a high risk is likely to affect data subject's rights and freedoms, i.e., RaF.[100] Article 35 does not specify which rights the notion of the RaF covers. However, based on the wording, i.e., rights and freedoms, the notion can be seen to expose itself to a broad interpretation regarding the protection given to individuals.[101] According to WP29, RaF may cover not only rights of data protection and privacy but also other fundamental rights, such as the right to freedom of speech.[102] However, it has been argued that as the GDPR, including a DPIA, applies only to personal data processing, the protection provided for other fundamental rights than the right to data protection and those impacted by personal data protection might not be adequate.[103]

Another thing to consider, in terms of Article 35(1), concerns processing operations initiated before the GDPR's enforcement. This is a matter that has been addressed also by others as it has been pondered what the situation is with processing operations commenced before the GDPR was enforced, because one cannot conduct a DPIA to such operations before initiating them.[104] Directly

[98] Sarrat, J., & Brun, R. (2018), *supra nota* 54, 174.
[99] Tietosuojavaltuutettu, 8393/161/2019, 26.5.2020.24,27.
Retrieved from https://finlex.fi/fi/viranomaiset/tsv/2020/20200602, 12 February 2021.
[100] Regulation 2016/679, *supra nota* 3, Art.35
[101] Yordanov, A. (2017). Nature and Ideal Steps of the Data Protection Impact Assessment Under the General Data Protection Regulation. *European Data Protection Law Review*, 3(4), 486–495,489.
[102] Article 29 Data Protection Working Party (4.4.2017), *supra nota* 2, 6.
[103] Kloza, D. *et al.* (2017). Data Protection Impact Assessments in the European Union: completing the new legal framework towards a more robust protection of individuals. *d.pia.lab Policy Brief*, 1/2017, 1-4.3.
[104] Feiler, L. *et al.* (2018). *The EU General Data Protection Regulation (GDPR): A Commentary.* (1st Ed.) Surrey: Globe Law and Business Ltd.173.

inferring by Article 35(1)'s wording as it requires that the DPIA is done before the processing[105], it seems not an automatic obligation to conduct a DPIA for personal data processing that has started before the GDPR's enforcement. However, by referring to the GDPR, if there is a change of the risk arising from processing operations, a controller must estimate whether the processing complies with Article 35 and whether a DPIA should be conducted.[106] Hence, if there is a change of a risk arising from a processing operation initiated before GDPR's enforcement, then a controller should at least assess the possible need for a DPIA, which might lead to conducting one under Article 35.

Moreover, regarding SAs' role, it has been pondered that although SAs assumingly have the required knowledge of a DPIA, it cannot be assumed that they also know the newest personal data processing processes.[107] Thereby, in a situation where the SA has the appropriate knowledge of the obligation to conduct a DPIA under Article 35, but one is not familiar with the development of new processes and activities to be used to process personal data, the lack of knowledge might negatively affect SAs' work, e.g., to the content of the list compiled in accordance with Article 35(4)-(5), the decisions, and SAs' advices to controllers.

Additionally, the language associated with data protection in the EU is based on legal terminologies and language, yet it has been said that using only such language around a DPIA could have detrimental impacts on it since it might be seen only as a compliance check.[108] Regarding the language, the use of broader and common language could potentially provide facilitation for controllers to comply with Article 35 and consequently, to protect data subjects' RaF. Moreover, as there most likely are controllers that do not have a profound legal knowledge, it might be easier to understand the obligation to conduct a DPIA under Article 35 if the language would not be as legal as it is now, but more understandable. To mention, the use of wide concepts has been said to enhance GDPR's technology neutrality.[109]

[105] Regulation 2016/679, *supra nota* 3, Art.35(1)
[106] Regulation 2016/679, *supra nota* 3, Art.35(11).
[107] Binns, R. (2017). Data protection impact assessments: a meta-regulatory approach. *International Data Privacy Law*, 7(1). Oxford Publishing Limited, 22-35.32.
[108] Ferra, F. *et al.* (2020) *supra nota* 37, 14-15.
[109] Demetzou, K. (2019), *supra nota* 26, 8.

4. THE TWO FINNISH DECISIONS IN TERMS OF ARTICLE 35

This chapter examines how the FDPO and the DDPO in the ODPO in Finland have interpreted the obligation to conduct a DPIA, especially whether a high risk is likely to emerge, under Article 35, WP29's guidelines and FDPO's list, and ended up concluding the controllers' failure to conduct a DPIA for processing operations that would have required the DPIA under Article 35 in the following cases. The cases are analyzed insofar they concern Article 35.

4.1. *Taksi Helsinki Oy*

The case concerns the controller *Taksi Helsinki Oy's* failure to conduct a DPIA under Article 35 for location data processing, security camera surveillance and automated decision-making, including profiling, the latter in the context of the company's loyalty program.[110] The emphasis of this analysis is on assessing the controller's obligation to conduct a DPIA in the context of camera surveillance and automated decision-making. The processing of location data in question concerns more the DPIA's content and Article 35(7) since the DPIA was eventually conducted for location data processing, yet the controller has assessed that it should not have conducted a DPIA for camera surveillance or automated decision-making.[111]

Regarding camera surveillance through the camera surveillance system (CSS), the controller has not conducted a DPIA under Article 35 even one should have.[112] Although the camera surveillance's purpose is to protect drivers and customers, the DDPO has considered personal data processing through the CSS as systematic monitoring, large-scale processing and to concern vulnerable data subjects and one has considered the data processed as sensitive or highly personal,

[110] Tietosuojavaltuutettu (26.5.2020), *supra nota* 99.
[111] *Ibid.*,10-11.
[112] *Ibid.*,10,25.

all mentioned under the Guidelines, which indicates the need for conducting a DPIA.[113] Since all taxis have the CSS and the surveillance is conducted continuously, the processing is therefore already considered as systematic, i.e., over 2000 taxis offer rides.[114] To mention, as the CSS is installed to all taxis, the monitoring can also be seen to occur as a general part of data collection and it takes place via a system, i.e., the CSS, in accordance with WP29's guidance[115], thus being systematic. The processing has also been considered large-scale since the amounts of personal data processed and the data subjects affected, i.e., factors to assess, have been notable since the data subjects affected has been counted in hundreds of thousands and the number of taxi rides per year has been approximately four million.[116] Additionally, the fact the camera surveillance has been time-specific and location-specific, increasing the amount of personal data processed, further strengthens the processing as being large-scale.[117] To mention, the factors assessed concerning the large-scale processing in the context of camera surveillance are similar to those under the DPO Guidelines.

WP29 has emphasized that sensitive data and highly personal data also cover data relating to data subject's household and private activities.[118] Consequently, telephone calls made in taxis are considered to fall under this category as they might reveal sensitive information about data subjects.[119] Additionally, the DDPO has noted that the controller has not provided information about the collection of audio in a clear manner, thereby the majority of data subjects might not have been aware of the audio collection and not able to consider it in terms of their behavior, and it was also concluded that there were vulnerable data subjects, for instance, children and older people, affected by the processing as taxi rides were not limited to specific groups, but offered to all.[120] All the four abovementioned criteria are requirements under the Guidelines, and based on Article 35(1), such personal data processing through the CSS has been considered likely to cause a high risk to data subject's RaF, thus, a DPIA should have been done to camera surveillance in accordance with Article 35, neither has the controller complied with Article 5(2).[121] Thus to note, the DDPO's decision can be seen to reflect the close connection between the obligation under Article 5(2) and he obligation to conduct a DPIA under Article 35.

[113] *Ibid.*,24-25.
[114] *Ibid.*,24.
[115] Article 29 Data Protection Working Party. (13.12.2016), *supra nota* 72, 8.
[116] Tietosuojavaltuutettu (26.5.2020), *supra nota* 99, 24–25.
[117] *Ibid.*
[118] *Ibid.*
[119] Article 29 Data Protection Working Party (4.4.2017) *supra nota* 27, 9–10.
[120] Tietosuojavaltuutettu (26.5.2020), *supra nota* 99, 24–25.
[121] *Ibid.*

In turn, Article 35(3)(c) states that a DPIA shall be performed, "in particular, in case of: c) a systematic monitoring of a publicly accessible area on a large scale".[122] As the criterion of systematic monitoring has already been met, the next aspect to consider is the fulfillment of monitoring of a publicly accessible area on a large scale, although the DDPO has not assessed this criterion. The monitoring through the CSS is directed not only to the taxis' interior but also the outside environment of taxis.[123] Thus, the question is whether the CSS also monitors publicly accessible areas on a large scale. WP29 has interpreted the publicly accessible area as being "any open place to any member of the public, for example, piazza, a shopping centre, a street, a market place, a train station or a public library".[124] Thereby, it could be concluded that the taxi's interior is unlikely to be considered a publicly accessible area since it is not an open place accessible for all people at any time. As a rule, taxi rides are accessible for a certain period for persons who order and pay for them. Another question is whether the camera recording the outside environment of taxis could be considered directed to monitor publicly accessible areas on a large scale as the camera might record images in publicly accessible areas depending on where taxis drive and to which direction cameras appoint. However, despite the outcome of whether the camera surveillance is considered to cover a publicly accessible area on a large-scale under Article 35(3)(c), it does not change the outcome that a DPIA should have been conducted for camera surveillance because criteria of systematic monitoring, large-scale processing, vulnerable data subjects and sensitive personal data are met.[125]

Automated decision-making, including profiling, for which the controller has failed to conduct a DPIA, has been used in connection with the company's loyalty program and limited only to identifying the number of orders made via telephones or the application to assess the VIP customer's status.[126] It has been analyzed whether the processing in question falls under Article 35(3)(a). Yet, although the processing is considered as systematic since the automated decision-making takes place in every order made, the DDPO has stated that the processing does not relate to data subject's personal aspects but rather to the frequency of orders made via telephones and the application, and customer's status and thus, it has concluded that the processing does not fall under Article 35(3)(a) and a DPIA is not required under 35(3)(a).[127] Yet, the processing is considered to

[122] Regulation 2016/679, *supra nota* 3, Art.35(3)(c).
[123] Tietosuojavaltuutettu (26.5.2020), *supra nota* 99,10.
[124] Article 29 Data Protection Working Party (4.4.2017) *supra nota* 27, 9.
[125] Tietosuojavaltuutettu (26.5.2020), *supra nota* 99, 25.
[126] *Ibid.*, 10,26.
[127] *Ibid.*,26–27.

fall under Article 35(1) and based on the Guidelines, it is likely to present a high risk natural persons' RaF, thus subject to Article 35.[128]

Regarding evaluation and scoring in automated decision-making, as the personal data processed in automated decision-making indicates only how much a data subject uses taxi rides to assess the data subject's possible VIP-status, the personal data processing concerning scoring, mentioned under the Guidelines, does not cause a high risk to data subjects' RaF in accordance with Article 35(1).[129] By referring to the Guidelines, the DDPO has also considered that neither the threshold of legal effects nor similar significant ones under Article 35(1) is met as the effects arising from the processing relate only to how fast data subjects can have taxis, thus the effects are considered minor.[130] However, when considering the extent of the processing, due to the extensive amount of data processed in connection with automated decision-making – over one million orders are subject to automated processing – the DDPO considers the processing as large-scale.[131] As in connection with camera surveillance, also vulnerable data subjects have probably been subject to automated decision-making resulting in fulfillment of the Guidelines' two criteria and based on Article 35(1), there is a likelihood of a high risk and a DPIA should have been performed not only for camera surveillance but also for automated decision-making.[132]

4.2. *Kymen Vesi Oy*

The case concerns the processing of location data through the electronic driving information system (DIS) that was introduced in 2017 to monitor the working time of 47 employees, i.e., data subjects, by the employer *Kymen Vesi Oy* that, as a controller, has not performed a DPIA because it has not considered a need for it.[133] The controller has failed to perform a DPIA under Article 35 for processing of location data, that is considered as personal data, because the processing would have required a DPIA since the location data processing is considered as systematic monitoring

[128] *Ibid.*,26.
[129] *Ibid.*26–27.
[130] *Ibid.*
[131] *Ibid.*,27.
[132] *Ibid.*
[133] Tietosuojavaltuutettu, 531/161/2020, 18.5.2020.1.
Retrieved from https://finlex.fi/fi/viranomaiset/tsv/2020/20200582, 12 February 2021.

and the data processed is vulnerable data subjects' personal data under Article 35, Finnish SA's list established in accordance with Article 35(4), and the Guidelines.[134]

Regarding systematic monitoring, the FDPO has stated that monitoring of working time has been systematic under the Guidelines and FDPO's list.[135] To evidence the systematic monitoring, the Guidelines are to be relied on and according to which, systematic monitoring means, *inter alia,* processing used to observe or monitor data subjects.[136] Here, data subjects and their location data are monitored through the DIS. Also, as the monitoring covers tracking location[137], it can be seen to further strengthen the monitoring being systematic. Furthermore, as data subjects are employees and the controller is their employer, there is an imbalance between them as employees are the weaker parties, indicating that they are vulnerable data subjects under Article 35, the Guidelines and the FDPO's list.[138] As the FDPO's list covers the location data that is processed in the context of systematic monitoring and considers the data as vulnerable data subjects' personal data, and systematic monitoring and vulnerable data subjects are also criterion under the Guidelines, a DPIA must be conducted to such personal data processing under Article 35.[139]

Another aspect to assess is the criterion of large-scale processing and whether location tracking would fall into it. The FDPO has not directly stated that the processing is considered large-scale. The controller has argued that it is not a matter of large-scale processing, but when determining administrative fine's amount, it has been stated that the processing affects a significant part of the controller's staff, i.e., 47 employees are affected by processing and the relatively small number cannot mitigate the fine.[140] Thus the issue is whether it is possible to interpret the criterion of large-scale processing in a way that the processing could be seen as large-scale when considering the factors related to large-scale processing and established by DPO Guidelines, even if the amount of data subjects affected is rather low. However, compared to the staff size, the number of data subjects affected could perhaps be considered high. Yet, despite the outcome of large-scale processing, as already two criteria under the Guidelines are met, the controller should have performed a DPIA under Article 35 for processing employees' location data.[141]

---

[134] *Ibid.*,5.
[135] *Ibid.*
[136] Article 29 Data Protection Working Party (4.4.2017) *supra nota* 27, 9.
[137] Article 29 Data Protection Working Party (13.12.2016), *supra nota* 72, 9.
[138] Tietosuojavaltuutettu (18.5.2020), *supra nota* 133, 5.
[139] *Ibid*,.4–5.
[140] *Ibid.*,15,10.
[141] *Ibid.*

Additionally, as regards using new technological or organizational solutions, the DIS is a technological solution used for collecting data subjects' location data to monitor their working time.[142] The Guidelines provide examples of the new technological solutions, for example, combining facial recognition and using fingerprints for improved physical access control, and the IoT.[143] Thus, the DIS as a technological solution, used only for collecting location data, is unlikely to be seen as a new one and should not be contrasted with, for example, the IoT. Neither has the FDPO considered this criterion nor that processing would fall into it. Therefore, it is not likely that the criterion of applying new technological or organizational solutions is met.

Another aspect to consider, also assessed by the FDPO, relates to evaluation and scoring. Yet, the FDPO has not mentioned this criterion as a reason to conduct a DPIA under Article 35. However, referring to the Guidelines' criterion of evaluation and scoring, e.g., aspects concerning data subject's performance at work, location or movements referred to in the GDPR[144], would it be possible to consider that collecting location data for monitoring data subjects' working time falls under this criterion? DIS's purpose is to monitor and evaluate employees' working time by tracking their location data, which might be seen as evaluating the performance at work or location under the criterion. Thereby, the issue is whether the collected location data is used for evaluating data subjects' personal characters, i.e., performance at work or location, which remains unclear in FDPO's decision. Yet, based on the Guidelines, location data processing might perhaps be considered fulfilling the criterion of evaluation and scoring.

4.3. Notices from the decisions

Based on the analysis of the decisions, when assessing whether the processing causes a high risk to data subjects' RaF, many factors and concepts indicating the need for a DPIA under Article 35, must be assessed and interpreted, for example, systematic monitoring, large-scale processing, and the legal or similar significant effects to data subjects arising from processing. Thus, there are lot to be aware of to make a right decision on the whether a high risk is likely to emerge and whether or not to conduct a DPIA under Article 35. It also assumingly requires time, carefulness and knowledge from controllers to assess the above concepts to determine them correctly in order to

[142] *Ibid.*,1.
[143] Article 29 Data Protection Working Party (4.4.2017) *supra nota* 27, 10.
[144] *Ibid.*,9.

ensure that Article 35 is complied with. As the decisions reflect, the detailed assessment and the interpretation of factors and criteria which all affect the outcome of whether a high risk is likely to arise and whether to conduct a DPIA, are not straightforward and the concepts and factors seem to be subject to interpretation. Thus, it might be challenging to assess them fully correctly.

5. CONNECTING THE FINDINGS TO THE PROPOSALS

5.1. Obscurities

Based on the analysis above, it has become clear that there are obscurities concerning Article 35 and the determination of when the processing is likely to present a high risk to data subjects' RaF. To emphasize, if the personal data processing falls at least under Article 35's paragraphs 1 or 3, or the SA's list established in accordance with paragraph 4, a DPIA should be conducted.

As a DPIA under GDPR's Article 35 is a new legal obligation, some controllers may not have profound knowledge of assessing risks to natural persons' RaF. Thus, the clearer and more unambiguous Article 35 is, the more uncomplicated it most likely is for controllers to assess whether to perform a DPIA and to comply with Article 35. Yet, as written, Article 35 is a long and challenging Article covering 11 paragraphs. The controller must assess whether the concerned processing falls under the scope of Article 35(3) or Article 35(1) and a DPIA should be conducted for the specific processing operation. As presented, one challenge can be seen to be the existence of different and, to some extent, ambiguous concepts and factors, established under Article 35, SA's lists and also WP29's guidelines, to be assessed when conducting a DPIA, which is materialized also in the Finnish decisions. Furthermore, the number of different sources of which the controller should be aware is broad, e.g., the GDPR, guidelines and SAs' lists. Additionally, WP29 states that if it is not clear whether to conduct a DPIA, it is better to conduct it.[145] Such instructions can be seen as vague and it seems to be solely the controller's responsibility to estimate and decide, in an unclear situation, whether to conduct a DPIA, even for good measure.

Additionally, as emphasized earlier Article 35(3) lays down three examples of cases that especially require a DPIA. Thus, some processing operations that do not fall under Article 35(3) might still require a DPIA to be conducted, for example under Article 35(1), as it was in the *Taksi Helsinki*

[145] Article 29 Data Protection Working Party (4.4.2017) *supra nota* 27, 8.

Oy decision.[146] Yet, Article 35(1) is also quite ambiguous in terms of determination of when to conduct a DPIA as the concepts established under it have not been clarified under it or the GDPR. Thus, another possible challenge relates to some vague and ambiguous concepts under Article 35, which could possibly result in broad and ununiform interpretations of such concepts and consequently, ununiform interpretation of Article 35, which could harm the GDPR's harmonization goal as regards the data protection. As emphasized earlier, the GDPR does not provide clear definitions for Article 35's important concepts and elements. For example, there are no definitions for concepts of a high risk, new technologies, systematic monitoring, large-scale processing or nature, scope, context and purpose of processing[147]. This could be problematic since they are significant concepts and elements to be assessed when determining whether to conduct a DPIA, and they should be clear for controllers to apply Article 35 correctly. However, as written earlier, it has been emphasized that broad concepts ensure that the GDPR remains as technology-neutral legislation.[148] As for the legal language used in the GDPR and around a DPIA[149], if the language around a DPIA and consequently, Article 35, was modified to be less legal, it could also be easier to interpret and apply the obligation to conduct DPIA under Article 35.

However, as the above concepts have not been specified under the GDPR, controllers should also be aware of the guidance provided by WP29 and SAs. The obligation to conduct a DPIA is novel and there is no relevant case law that could help interpreting Article 35. Moreover, not much help for interpreting Article 35 and assessing the likelihood of a high risk is provided by SAs' decisions as there are only 10 publicly given decisions on Article 35's infringements.[150] If the controller is not aware of, for instance, WP29's guidelines, including the Guidelines and DPO Guidelines, or SA's lists, it is possible that one fails to conduct a DPIA under Article 35, which may lead to facing administrative fines under GDPR's Article 83(4) and endangering the protection of data subjects' RaF. This was the situation in the *Kymen Vesi Oy* decision where the controller claimed challenging to apply Article 35 as the legislation was ambiguous and there was no guidance provided to interpret Article 35.[151]

[146] Tietosuojavaltuutettu (26.5.2020), *supra nota* 99, 26–27.
[147] Regulation 2016/679, *supra nota* 3, Art.35.
[148] Demetzou, K. (2019), *supra nota* 26, 8.
[149] Ferra, F. *et al.* (2020), supra nota 37, 14-15.
[150] *GDPR Enforcement Tracker*. CMS Law. Tax. Retrieved from: https://www.enforcementtracker.com, 28 March 2021.
[151] Tietosuojavaltuutettu (18.5.2020), *supra nota* 133, 10.

5.2. Clarifications

There is a use for a DPIA in today's world where personal data processing affects data subjects RaF, because a DPIA can be seen to promote the fulfillment of compliance and protection of data subjects' RaF. However, there are also some obscurities to overcome so that a DPIA can work as effectively as possible from the data subjects' and controllers' perspectives.

Due to the fast-developing technologization, the first thing to ensure is that Article 35 is kept up to date alongside the development and also amended if needed to guarantee the protection of data subjects' RaF and also to avoid the undesirable replacement of current legislation, i.e., the GDPR, which happened to its predecessor. Thus, if it seems that other types of processing operations than those under Article 35(3) are likely to cause a high risk, Article 35(3) should, at least, be reviewed and, if necessary, broaden to cover also the new identified high-risk processing types. As there might be other processing operations that require a DPIA, yet not directly falling under Article 35(3), it would perhaps be wise to review the three situations that are now established under it.

Moreover, regarding the vague concepts that have been described and mentioned above and that are subject to interpretation, and the vague language used around a DPIA under Article 35, it would be advisable to define and clarify more precisely some of Article 35's concepts in order to also ensure that they are interpreted and applied uniformly. Thus, as there are no clear definitions for such concepts and elements under the GDPR, they should be clarified more precisely to facilitate the controller's decision on assessing the likelihood of a high risk and the need for a DPIA, and to guarantee that Article 35 is applied correctly. At the moment, some concepts are explained by WP29's guidelines and SAs' lists. Yet, it would be advisable to clarify the concepts, to some extent, under the GDPR that is directly applicable regulation. To note, ensuring the uniform interpretation and application of the concepts and eventually, of Article 35 would also promote the fulfillment of the GDPR's harmonization goal.

However, in order that the GDPR's application scope remains wide, the language used around a DPIA in Article 35 and the concepts under Article 35 should not be too specific, limited or dependent on the technology used in the processing, yet they should be understandable. Moreover, if concepts and criteria are too specific, it could lead to a situation where Article 35 would not be up-to-date and need to be amended continually alongside technologization, which would be burdensome. Then again, to provide some clarification for the terminology and language used

under Article 35 would still be advisable. Furthermore, as the obligation to conduct a DPIA under Article 35 is new one, it might be challenging for the controllers to be aware of all the sources, e.g., WP29's guidelines and SAs' lists, that facilitate the determination of a likelihood of a high risk and even if one is aware of them, the above concepts are still vague and require interpretation to some extent.

One way to guarantee compliance with Article 35 and protect data subjects' RaF could be to find the so-called golden mean when it comes to determining and clarifying the concepts and clarifying the language used under Article 35. The concepts under Article 35 should not be too specific to avoid Article 35's continual amendments and to ensure that it covers different processing types. Yet, Article 35 and the concepts cannot be too vague to avoid their incorrect interpretations and the difficulties for controllers to decide whether to conduct a DPIA. Furthermore, as written, regarding processing operations commenced before the GDPR's enforcement and to which the DPIA cannot be conducted before initiating processing personal data, controllers should assess, for example, whether there is this change of a risk in accordance with GDPR's Article 35(11) and whether the DPIA would be required.

CONCLUSION

This paper has focused on examining obscurities concerning the obligation to conduct a DPIA under GDPR's Article 35, especially when the personal data processing is likely to cause a high risk to natural persons' RaF and when to conduct a DPIA under Article 35. Thus, it has aimed to assess whether Article 35, regarding the likelihood of a high risk, includes any obscurities that could danger Article 35's correct interpretation and consequently, danger the protection of data subjects' RaF, and to provide some proposals to overcome the obscurities. Additionally, from controllers' perspectives, not complying with Article 35 can result in imposing administrative fines under the GDPR's Article 83(4). Thereby, understanding the challenges, identifying obscurities and responding to them is crucial to avoid the above scenarios for data subjects and controllers. Thus, the GDPR, including Article 35, should be clear enough to adequately address and overcome the current challenges. The hypothesis, that there are some obscurities regarding Article 35 which could be clarified to some extent, for instance, through legislative changes, has proved to be true. As for the future research, how to conduct a DPIA under Article 35 could be examined as Article 35(7) provides only non-exhaustive requirements for DPIA's content and neither a specific process on how to conduct a DPIA has been established under the GDPR.

Establishing Article 35 has brought challenges to personal data processing and as seen, some amount of questioning has been addressed to Article 35. As indicated, if processing falls under Article 35(1) or Article 35(3), or the SA's list established under Article 35(4) a DPIA should be conducted. Yet, Article 35(1) appears to be quite ambiguous and vague as new technologies or the elements of processing's nature, scope, context and purposes have not been defined under the GDPR. Moreover, Article 35(3) provides only three different examples of risky processing operations that especially require a DPIA leaving discretion for controllers to assess whether one's processing operation falls under Article 35(3). Regarding the vague concepts, for example, large-scale processing and systematic monitoring which are not defined under the GDPR, establishing more precise definitions in the GDPR would potentially help controllers to determine whether to conduct a DPIA for a specific processing operation, desirably resulting in Article 35's correct

interpretation and application. It is somehow illogical that Article 35 that obliges to conduct a DPIA does not provide a clear expression for a DPIA or the high risk. Also, due to the legal language used in the GDPR, there is a risk that using such language creates difficulties for controllers that do not have legal expertise to interpret and apply Article 35. However, too detailed definitions should also be avoided to guarantee that the GDPR remains applicable in broad scope, bear time, and do not need to be amended continually. Too specific definitions could also create gaps in the interpretations of Article 35 as not all situations requiring a DPIA would potentially be covered by Article 35. Despite the above, the GDPR and Article 35 must remain up to date alongside technologization, which means that they might have to be amended at some point. Though, frequent amendments are burdensome, not desirable. Thereby, it would be advisable to clarify the concepts to some extent by legislative changes, i.e., by more exact regulation and Article 35, to ensure the correct interpretation and application of the obligation to conduct a DPIA under Article 35.

The GDPR has established new rights and obligations, including the obligation to conduct DPIA under Article 35. It is a novel regulation and the challenges it has created must be coped with. When determining the likelihood of a high risk, there are different concepts, elements, and also sources, e.g., the GDPR, especially Article 35, SA's lists and WP29's guidelines, of which controllers should assess to correctly apply Article 35. Thus, there a lot to be aware of for a controller who must comply with Article 35 and in case of an infringement of 35, one might be charged with high administrative fines under GDPR's Article 83. As can be seen, the number of different factors and sources, and the concepts' broad interpretation have been materialized also in the Finnish decisions. Furthermore, vague concepts and challenging language might result in a broad interpretation of concepts and eventually of Article 35. Consequently, Article 35's varying interpretations could result in its ununiform application, which might danger GDPR's harmonization goal in the EU's data protection area.

This paper considers paramount to find the so-called golden mean for clarifying the vague concepts and the terminology used around Article 35 to guarantee the protection of data subjects' RaF and ensure Article 35's uniform application. As written, there are no clear definitions for some important concepts under Article 35 or the GDPR. Thus, the terminology should be understandable and clarified but not in a too specific way to ensure that the application ambit of the GDPR remains wide. In the future, amounts of SAs' decisions on Article 35 will most likely increase, as already have, providing more clarity for interpreting Article 35. Currently, the amount of SAs' publicly

given decisions on infringements of Article 35 is not very high and amending the GDPR would take time. Thus, regarding Article 35's interpretation, controllers should ensure that they are at least aware of current legislation, WP29's guidelines and SAs' lists, advice and the SAs' already given decisions. Although, as this paper has shown, there are obscurities concerning Article 35 and the likelihood of a high risk, one effective way to protect data subjects' RaF and also strengthen the data protection is to assess whether the high risks and risks arising from personal data processing are likely to emerge and if needed, to conduct a DPIA under Article 35.

LIST OF REFERENCES

Scientific books

1. Craig, P., & De, B. G. (2015). *EU law: Text, cases, and materials.* (6th ed.) New York, US: Oxford University Press

2. Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide,* (1st ed.) Cham, Switzerland: Springer International Publishing.

Scientific articles

3. Bhaimia, S. (2018). The General Data Protection Regulation: The Next generation of EU Data Protection. *Legal Information Management*, 18(1). Cambridge, UK: Cambridge University Press, 21-28.

4. Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., & Rost, M. (2016). A Process for Data Protection Impact Assessment under the European General Data Protection Regulation. In: Schiffner, S., Serna J., Ikonomou D. & Rannenberg K. (Eds.), *Privacy Technologies and Policy* (21-37), APF 2016, LNCS 9857. Cham: Springer.

5. Binns, R. (2017). Data protection impact assessments: a meta-regulatory approach. *International Data Privacy Law*, 7(1). Oxford: Oxford Publishing Limited, 22-35.

6. Bu-Pasha, S. (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). Routledge, 391-402.

7. Burri, M., & Schär, R. (2016). The reform of the EU data protection framework: outlining key changes and assessing their fitness for a data-driven economy. *Journal of Information Policy*, 6(1), Pennsylvania State University Press, 279-511.

8. De Hert, P. (2012). A Human Rights Perspective on Privacy and Data Protection Impact Assessments. In: Wright, D. & De Hert, P. (Eds.) (2012) Privacy Impact Assessment. Law, Governance and Technology Series, 6, (33-76). Dordrecht: Springer.

9. Demetzou, K. (2019). Data Protection Impact Assessment: A tool for accountability and the

unclarified concept of 'high risk' in the General Data Protection Regulation. *The Computer Law and Security Report,* 35(6), 105342. Elsevier, 1-14.

10. Ferra, F., Wagner, I., Boiten, E., Hadlington, L., Psychoula, I., Snape, R. (2020). Challenges in assessing privacy impact: Tales from the front lines. *Security and Privacy*, 3(2), e101. John Wiley & Sons, Ltd, 1-19.

11. Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law,* 10(1). Oxford University Press, 11-36.

12. Gal, M. S., & Aviv, O. (2020). The competitive effects of the GDPR. *Journal of Competition Law & Economics*, 16(3). Oxford University Press, 349-391.

13. Gellert, R. (2018). Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review*, 34(2), 279-288. Elsevier.

14. Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. *International Journal of Market Research*, 59(6). SAGE Publications, 703-705.

15. Hijmans H. (2016) Making Article 16 TFEU Work: Analysis and Conclusions. In: *The European Union as Guardian of Internet Privacy*. Law, Governance and Technology Series, 31, (511-564). Cham: Springer International Publishing.

16. Hoofnagle, C. J., van der Sloot, B., Borgesius, F. Z. (2019). The European Union General Data Protection Regulation: What it is and What it Means. *Information & Communications Technology Law*, 28(1). Routledge, 65-98.

17. Lindqvist, J. (2018). New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things? *International journal of law and Information Technology*, 26(1). Oxford University Press, 45-63.

18. Layton, R (2017). How the GDPR Compares to Best Practices for Privacy, Accountability and Trust. SSRN, 1-23.

19. Lynskey, O. (2014). Deconstructing Data Protection: The Added-Value of Right to Data Protection in the EU Legal Order. *International and Comparative Law Quarterly*, 63(3). Cambridge University Press, 569-598.

20. Mondschein C.F., Monda C. (2019) The EU's General Data Protection Regulation (GDPR) in a Research Context. In: Kubben P., Dumontier M., Dekker A. (eds) *Fundamentals of Clinical Data Science*. (55-71) Springer, Cham.

21. Raab. C.D., (2020) Information privacy, impact assessment, and the place of ethics. *Computer law & security review*, 27. Elsevier, 1-8.

22. Rodotà S. (2009) Data Protection as a Fundamental Right. In: Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C., Nouwt, S. (Eds.) *Reinventing Data Protection*? (77-

82). Dordrecht: Springer.

23. Rubinstein, I., & Good, N. (2020). The trouble with Article 25 (and how to fix it): the future of data protection by design and default. *International Data Privacy Law*, 10(1). Oxford University Press, 37–56.

24. Sarrat, J., & Brun, R. (2018) DPIA: How to Carry out One of the Key Principles of Accountability. In: Medina, M., Mitrakas, A., Rannenberg K., Schweighofer E., & Tsouroulas N. (Eds.) *Privacy Technologies and Policy* (172-182), APF 2018, LNCS 11079. Cham, Switzerland: Springer.

25. Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, 2016(6). Elsevier, 5–8.

26. Tikkinen-Piri, C., Rohunen, A., Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review,* 34(1). Elsevier, 134-153.

27. Ivanova Y. (2020) The Data Protection Impact Assessment as a Tool to Enforce Non-discriminatory AI. In: Antunes L., *et al.* (eds) *Privacy Technologies and Policy*. APF 2020. LNCS, 12121. Springer, Cham, 3-24

28. Wright, D. (2012). The State of the Art in Privacy Impact Assessment. *Computer law & Security Review*, 28(1). Elsevier, 54-61.

EU legislation

29. Charter of Fundamental Rights of the European Union (EU) 2012/C 326/02, OJ C 326, 26.10.2012.

30. Consolidated version of the Treaty on the Functioning of the European Union OJ C 326/47-326/390, 26.10.2012.

31. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJ L 281, 23.11.1995, 31-50.

32. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, 1-88.

Other sources

33. 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". WP 248 rev 0.1, 4 April 2017. Retrieved from: https://tietosuoja.fi/documents/6927448/8316711/Guidelines+on+Data+Protection+Impact+Assessment.pdf/def06c04-03f9-4505-99d2-709243ef2d35/Guidelines+on+Data+Protection+Impact+Assessment.pdf, 4 February 2021.

34. Article 29 Data Protection Working Party. Guidelines on Data Protection Officer. WP 243, 13 December 2016. Retrieved from: https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A, 4 February 2021.

35. Bhageshpur, K. (2019). *Data Is The New Oil - - And That's A Good Thing.* Forbes. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/?sh=799f82c73045, 24 March 2021.

36. Centre of Information Policy Leadership (CIPL), Hunton & Williams LLP. (2016). Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR. *CIPL GDPR Interpretation and Implementation Project*. Retrieved from https://iapp.org/resources/article/risk-high-risk-risk-assessments-and-data-protection-impact-assessments-under-the-gdpr/, February 10, 2021

37. Feiler, L. *et al.* (2018). *The EU General Data Protection Regulation (GDPR): A Commentary.* (1st Ed.) Surrey: Globe Law and Business Ltd.

38. *GDPR Enforcement Tracker*. CMS Law. Tax. Retrieved from: https://www.enforcementtracker.com, 28 March 2021.

39. Kloza, D, Van Dijk, N., Casiraghi S., Vaquez Maymir, S., Roda, S., Tanas, A., Konstantinou, I. (2019). Towards a Method for Data Protection Impact Assessment: Making sense of GDPR Requirements. *Brussels Laboratory for Data Protection & Privacy Impact Assessments*.

40. Kloza, D., Van Dijk, N., Gellert, R., Böröcz, I., Tanas, I., Mantovani, E., Quinn, P. (2017). Data Protection Impact Assessments in the European Union: completing the new legal framework towards a more robust protection of individuals. *Brussels Laboratory for Data Protection & Privacy Impact Assessments*.

41. European Commission Communication from the Commission to the European Parliament, the European Council, the, Council, the European Economic and Social Committee and the Committee of the Regions (2020), *The EU Security Union Strategy*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC06056, 7 March 2021.

42. *List compiled by the Office of the Data Protection Ombudsman of processing operations which require data protection impact assessment (DPIA).* (2018). The Office of Data Protection Ombudsman. Retrieved from https://tietosuoja.fi/en/list-of-processing-operations-which-require-dpia, February 10, 2021.

43. *Risk assessment and data protection planning.* Office of Data Protection Ombudsman. Retrieved from https://tietosuoja.fi/en/risk-assessment-and-data-protection-planning, 22 February 2021.

44. *What is a DPIA*? ICO. Retrieved from 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/#what2, 10 February 2021.

45. *What is personal data?* Office of the Data Protection Ombudsman. Retrieved from https://tietosuoja.fi/en/what-is-personal-data, 4 February 2021.

46. Tietosuojavaltuutettu, 8393/161/2019, 26.5.2020, Retrieved from https://finlex.fi/fi/viranomaiset/tsv/2020/20200602, 2 February 2021.

47. Tietosuojavaltuutettu, 531/161/2020, 18.5.2020. Retrieved from https://finlex.fi/fi/viranomaiset/tsv/2020/20200582, 2 February 2021.

48. Yordanov, A. (2017). Nature and Ideal Steps of the Data Protection Impact Assessment Under the General Data Protection Regulation. *European Data Protection Law Review,* 3(4), 486–495.

APPENDICES

Appendix 1. Non-exclusive licence

Non-exclusive licence for reproduction and for granting public access to the graduation thesis[1]

I Pihla Helminen

1.Give Tallinn University of Technology a permission (non-exclusive licence) to use free of charge my creation

Analyzing the obscurities of the data protection impact assessment and "likely to result in a high risk" under Article 35 of the EU General Data Protection Regulation,

supervised by supervised by Jenna Uusitalo,

1.1. to reproduce with the purpose of keeping and publishing electronically, including for the purpose of supplementing the digital collection of TalTech library until the copyright expires;

1.2. to make available to the public through the web environment of Tallinn University of Technology, including through the digital collection of TalTech library until the copyright expires.

2. I am aware that the author also retains the rights provided in Section 1.

3. I confirm that by granting the non-exclusive licence no infringement is committed to the third persons' intellectual property rights or to the rights arising from the personal data protection act and other legislation.

[1] *The non-exclusive licence is not valid during the access restriction period with the exception of the right of the university to reproduce the graduation thesis only for the purposes of preservation.*