입법평가 Issue Paper 18-15-⑤

Data Protection Impact Assessment (Art. 35 GDPR) as a Tool of Privacy Regulation

Michael Kolain

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

Data Protection Impact Assessment (Art. 35 GDPR) as a Tool of Privacy Regulation

연구자 : Michael Kolain(Research Associate and Coordinator,
German Research Institute for Public Administration Speyer)

이 연구는 한국법제연구원(KLRI)과 독일 슈파이어 공행정연구소(GRIPA)와의 MoU에 기반한 연구자 교류를 통해서 한국법제연구원에서 2018년 6월 10일부터 2018년 7월 9일까지 방문 연구를 진행한 마이클 콜라인(Michael Kolain) 연구원에 의해서 작성되었다. 유럽연합의 정보보호 영향평가에 관한 내용을 소개한 2018년 7월 4일의 정례워크숍의 결과를 확대 · 보완한 것이다.

Acknowledgement

Research Associate and Coordinator, Research area “Transformation of the state in the digital age”, (director: Prof. Dr. Mario Martini), German Research Institute for Public Administration Speyer.

*The author appreciates the valuable input of his colleague David Nink and the guidance of Prof. Mario Martini throughout the years. He wants to thank his employer for sending him to KLRI as a visiting scholar – and his wife for accompanying him. A big “Gamsahamnida!” goes out to all the smart and nice colleagues at KLRI who have contributed to an unforgettable time in Sejong-si.

CONTENTS

Issue Paper

I. Introduction

The General Data Protection Regulation (GDPR) has entered into force on the 25th May of 2018. For the first time in the history of the European Union, provisions to shape the fundamental right to protect "natural persons in relation to the processing of personal data"[1] are now directly applicable in all member states.[2] As a result, companies dealing with personal data will have to follow a fully harmonized set of rules for data protection – whether they are located in Helsinki, Prague, Lisbon, Rome or Nicosia.[3]

The new "Magna Charta of European Data Protection"[4] pursues ambitious goals: it doesn't only want to "facilitate the free flow of personal data within the Union (…), while ensuring a high level of the protection of personal data"[5] and give people control over their personal data[6] – it also wants to make sure that software is "designed to serve mankind"[7]. While the basic legal doctrine of data regulation law has its origins in the paper-based era and still mainly focusses on the processing of singular data sets (like the nationality or address of a natural person), the GDPR also tries to find a suitable normative framework that can achieve a "consistent and high level of protection of natural persons"[8].

1) Recital 1 GDPR.
2) Previously, the Directive 95/46/EC served as a common legal framework that member states had to specify fully through national legislation.
3) However, while the GDPR encompasses the processing of personal data almost entirely, there are exceptions (e.g. Art. 2 sec. 2 lit. b, d) and numerous so called "escape clauses" for the public sector. The reason for a different regulatory treatment of public entities is that the EU seeks to and must respect state sovereignty of the member states (principle of subsidiarity).
4) Martini/Kühling, EuZW 2016, 448 (449).
5) Recital 6 sentence 5 GDPR.
6) Recital 7 sentence 2 GDPR.
7) Recital 4 sentence 1 GDPR.
8) Recital 10 sentence 1 GDPR.

Nevertheless, the Union legislator is far from being ignorant about the rapid technological changes and the increased importance of privacy regulation in the digital age.[9] Nowadays, many individuals share personal data freely on the social web – and data companies (and state authorities) accumulate them through massive data collection, analyze them with the help of complex algorithms and derive sensitive knowledge about the personality of the individual. In times of globalized data capitalism, the data market also doesn't stop at the doorstep of the EU, but the information traffic rather crosses borders[10] and takes place worldwide.

In times where digitization and globalization enforce each other's powerful impact on societies worldwide, it becomes increasingly difficult to establish legal terminology and a regulatory framework that fits for the diverse sectors and use cases of the processing of personal data. Even though the legislator has seen the problems of the old Directive[11], the GDPR still keeps its basic regulatory technique: a general ban with a reservation of authorization (German: "Verbot mit Erlaubnisvorbehalt"). As a result, all processing of personal data is forbidden in a first step and needs to rely on either consent of the data subject or another legal basis (see Art. 6(2) lit. a–f GDPR) to be legally permitted. On top, the GDPR intentionally stays strictly technology-neutral[12] and chooses highly abstract prescriptions for all forms of data processing.[13]

In order to cover the broad field of different data-driven technologies and applications, however, the GDPR has also come up with some new legal concepts. It hasn't only improved the possibilities of specification through certification mechanisms (Art. 42 GDPR), but has also strengthened the position of the European Data Protection Board (EDPB, Art. 68 GDPR). Furthermore, it has implemented legal techniques that shift

9) See Recital 6 GDPR.

10) The transfer of personal data to third countries or international organizations is regulated in the 5th Chapter of the GDPR (Art. 44 ff. GDPR).

11) See Recital 9 sentence 1: "It has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity."

12) See Recital 15. The main reason for this regulatory decision being the "risk of circumvention": If only specific sectors or applications would be subject of a general ban and others would be generally allowed, controllers would feel an incentive to pursue strategies to bypass the legal scope.

13) In order to specify the legal obligations for a certain technology or application, the GDPR establishes methods of self-regulation or certification. See for the case of blockchain technology Wirth/Kolain (2018).

the regulatory focus slightly from the single data set to the question of how much of a danger a certain processing constitutes for rights and freedoms of the individual.

One example is the Data Protection Impact Assessment (DPIA) in Art. 35 GDPR. It employs the terminology of a "high risk" as its central vehicle – and thus is widely seen as a manifestation of a risk-based approach.[14] But also apart from that, the instrument of DPIA entails a number of interesting novelties as a tool of privacy regulation, such as black- and white-lists of the data protection authorities that specify the term "high risk" (Art. 35(4) and (5) GDPR).

In front of this background, this Issue Paper will introduce the instrument of "impact assessments" firstly in a general way (B.) to then focus on the new instrument of a DPIA according to Art. 35 GDPR (C). It takes a critical look at the new regulation in order to discover possible weaknesses and limitations: The criticism is then accumulated to proposals for future reform of the GDPR that can also serve as a blueprint for non-EU countries considering to adopt the instrument of a DPIA in their national legislation (D.). The paper ends with a conclusion (E.).

1. The concept of impact assessments

The method of impact assessments is not a specific feature of data protection law.[15] Actually, it has mostly been developed and put in place in different sectors, e.g. in environmental law[16]. Furthermore, there is a long tradition of "law impact assessments" in general and "technology impact assessment", also concerning new regulation, in particular.[17] Also countries like the New Zealand, Australia or Canada

14) The instrument is not entirely new in data protection law. Art. 20 of the Directive 95/46/EG has laid down an obligation to "prior checking" for "processing operations likely to present specific risks to the rights and freedoms of data subjects".

15) Morrison-Saunder et. al. (2014), p. 3.

16) For an overview Morgan (2012).

17) For a historical overview from technology assessment to impact statement and impact assessment, Clarke, R. (2009). For a transformation into a "wider Social Impact Assessment", Edwards et. al. (2016).
In Germany there has been a tradition of impact assessments mostly carried out by the "Office of Technology Assessment at the German Bundestag" and also by the "Institute for Regulatory Impact Assessment and Evaluation (InGFA)" at the German Research Institute of Public Administration Speyer. See also the framework for standardization of ISO/IEC 29134:2017 (Guidelines for privacy impact assessment).

can look back on a longer lasting experience with the instrument of impact assessments in privacy law.[18] Also in the EU, some frameworks for a DPIA have been published.[19]

Thus, the GDPR has chosen to implement a regulatory instrument that has been tried and proven already, even though not specifically in regard to the risks of "rights and freedoms of natural persons" under data protection law.[20] At its core it is also not a legal instrument, but stems from empirical methods of social sciences.

2. Overview of Art. 35 GDPR

Art. 35 GDPR constitutes of eleven paragraphs and has included several regulatory methods. It can serve as an interesting example of the regulatory "state of the art" in EU-law, combining state law and supervision with specification and self-regulation.

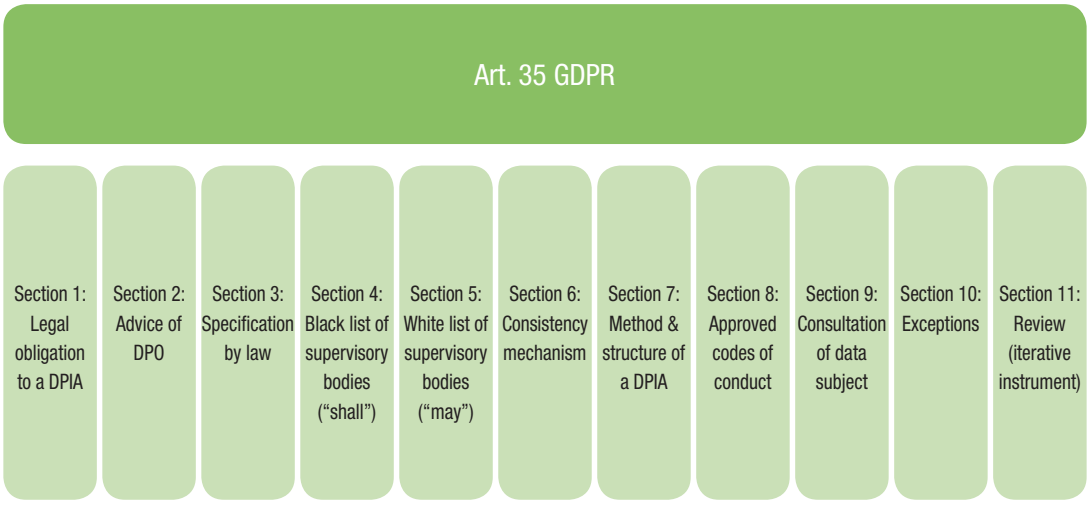

Figure 1: Basic normativie structure of Art. 35 GDPR

18) For an overview of "privacy impact assessments" before the GDPA has come into force, Wright et. al. (2013), especially the overview on p. 172. See also Bamberger/Mulligan (2013), p. 1660 ff.

19) For an overview, see Article 29 Data Protection Working Party (2017), p. 21 (Annex 1).

20) See also Martini (2018), paragraph 3: A DPIA is a subset of technology impact assessments.

However, instead of commenting each section individually, this paper chooses a different method: After giving further insights about what a DPIA according to Art. 35 GDPR is (I.), why the legislator has implemented the instrument (II.) and who is involved in carrying it out (III.), it takes a closer look on the term of a "high risk for the rights and freedoms of natural persons" (IV.). Afterwards, it briefly answers the questions: when a DPIA has to take place (V.) and how it shall be conducted in an ideal way (V.). Thus, hopefully, a comprehensive description of the content of Art. 35 GDPR for the readers can be achieved.

1) What is a DPIA?

A DPIA is a process for building and demonstrating compliance with data protection regulation, respectively identifying those data processing operations that are not (yet) GDPR-compliant.[21] It incentivizes data controllers to reflect on the legality and robustness of their application before they put them to practical use. Subject of the DPIA can either be a single or a set of similar processing operations.[22]

Since the DPIA has to take place before a product comes onto the market, it has the potential to serve as an "early warning system"[23] for controllers. It encourages them to an ex ante reflection about the potential risks of their applications – and spares the supervisory bodies some effort in controlling software applications on an ex post basis. Furthermore, it can serve as a tool to improve the overall quality of products and services – and thus create trust in digital technologies.

21) Some suggest that "data protection" is too narrow, and propose to focus on the term "Privacy Impact Assessment". See Wright et. al. (2013), p. 162. They define a PIA as a "methodology for assessing the impacts on privacy of a project, technology, product, service, policy, programme or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimize negative impacts."

22) See Art. 35(1) sentence 2 and Recital 92 GDPR. Article 29 Data Protection Working Party (2017) gives examples for similar processes ("a group of municipal authorities that are each setting up a similar CCTV system" or "a railway operator (single controller) could cover video surveillance in all its train stations with one DPIA", p. 7) or for a technology product ("the relationship between manufacturers of smart meters and utility companies", p. 8).

23) Wright et. al. (2013), p. 162.

An inherent part of the current Art. 35 GDPR is that the risk assessment of a certain application is not a singular event – in two ways:

- First, the obligation to review a DPIA when the risk changes (Art. 35(11) GDPR) makes it a recurring control mechanism. To fulfill the legal requirements, companies that process personal data will have to implement a corporate compliance system for risk management.[24] In this way, a rise in awareness about privacy risks in software products as well as more sophisticated management practices concerning privacy issues can be expected.
- Second, and more importantly, the assessment always has to consider and – in the best-case scenario – trigger adequate countermeasures in order to confront the "high risk". Thus, the questions of "is there a risk?" and "how can we reduce the risk?" need to be addressed together.

A considerable fact about the concept of a DPIA according to Art. 35 GDPR is the distribution of responsibilities between the controller and the supervisory authority. Art. 36 GDPR (and Recital 84 GDPR) makes clear that a notification of the supervisory authority is only necessary – especially after a DPIA has been carried out by the controller – if there is a residual high risk in spite of all possible countermeasures to mitigate the risk. In other words: If the controller detects a high risk initially, but is able to reduce it significantly through technical and organizational measures in the course of the DPIA, he does not have to notify the supervisory authority at all. If there remains a "high risk", the controller is obligated to consult the supervisory authority prior to processing.[25]

24) According to Wright et. al. (2013), p. 173, it should be "embedded as part of the project management framework". See also Hamidovic, H. (2010), p. 5 ("needs to be conducted as part of a formalized process").

25) To go into the details of the procedure of Art. 36 GDPR would go beyond the scope of this paper.

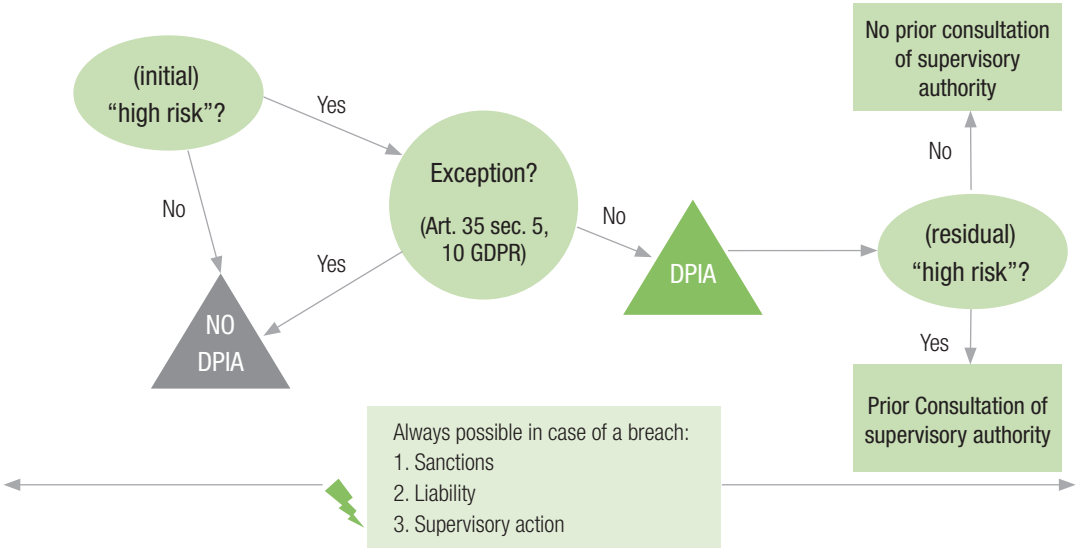

Figure 2: DPIA and prior consultation of supervisory authority

The chosen procedure has two faces: On the one hand it uses methods of self-regulation, involves the controller in a process of Privacy by Design and reduces the bureaucratic burden for the public administration. On the other hand, it opens room for a control deficit since there is no obligatory supervision of the internal task to assess whether there is a (initial or residual) high risk. A rather loose control system can thus serve as an incentive for companies to not take the obligation to carry out a DPIA too serious and, in the worst case, trigger a tendency towards cognitive dissonance in assessing the risk of their own application.[26] In other words: A key success factor of the instrument is for it not to be "conducted in a mechanical fashion for the purposes of satisfying a legislative or bureaucratic requirement"[27].

However, the obligation to carry out a DPIA is more than a toothless tiger. An erroneous and unlawful

26) Companies will regularly feel the incentive to bring their product to the market as fast as possible in order to be able to monetize their ideas and solutions. This urge will generally be stronger than the effort of building a system that uses, accumulates and transfers as little personal data as possible. As a consequence, especially on the management level, there need to be strong reasons to carefully conduct a DPIA rather than seeing it as a "tick on the to-do-list" on the way to a marketable product.

27) Hamidovic (2010), p. 5.

self-assessment within the DPIA can still release sanctions (Art. 83, 84 GDPR), supervisory actions (Art. 58 GDPR) and liability claims (Art. 82 GDPR).[28)]

2) Why is a DPIA necessary?

The legislator of the EU has chosen the DPIA as a regulatory instrument that allows both specification of legal obligations as well as flexibility for controllers.

First of all, the DPIA is – as well as the GDPR as a whole – a reaction to the dangers related to new digital technologies. Not only are digital applications growingly invading the individual lives of citizens – as a convenient replacement for analog processes of the past, but also in the economic interest of those trying to collect and monetize data. The more important personal data has become for economic success and the more profitable the data market is, the more relevant becomes the need for a well-suited, balanced and human-centered regulation. Additionally, many public scandals have diminished society's trust in emerging technologies: the US-American whistleblower Edward Snowden has pointed out the scope of online surveillance through state actors, and the case of Cambridge Analytica has intensely shaken the trust in the business models of social networks.

Secondly, the DPIA is an expression of the risk-based approach that the GDPR has started to carefully implement in the legal framework of European data protection law. Yet, it is not specified what exactly constitutes a "high risk". However, it is precisely this circumstance that opens space for a more collaborative and distributed way of specifying legal obligations – and transferring them into technical standards.[29)] The past has shown that the supervisory authorities – equipped not only with limited resources, but also with a legal framework that needed big efforts of interpretation – were overstrained with their duties. Before this background, the DPIA can be a major mainstay for involving the data industry in defining high privacy standards. Additionally, it might serve as a door opener for technology- and sector-specific[30)] regulation.

28) See Article 29 Data Protection Working Party (2017), p. 4 and Martini (2018), paragraph 77.
29) For details, see below C. IV.
30) An example of a sector-specific DPIA-framework for Smart Grids already exists, see https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf.

Since the DPIA bears the potential to trigger new compliance systems in data processing companies, it can become an integral part of bringing the idea of "Privacy by Design" to life. The GDPR has implemented the concept in Art. 25(1) GDPR. The main thoughts behind Privacy by Design are to use proactive instruments in order to achieve a high level of privacy from an early stage of IT-development – it switches the control mechanisms from ex post to ex ante. Its motto could be paraphrased as "self-reflection before action". The method aims to integrate as many technical, organizational and legal measures to protect personal data while keeping the system fully functional.

3) Who has to carry out a DPIA?

The DPIA is a duty of the controller.[31] He doesn't not only have to assess whether there is a "high risk" and come up with adequate countermeasures, but should also document this process[32].

However, according to Art. 35(10) GDPR, it is not always the controller to be committed to the obligations of Art. 35 (1).[33] This is especially the case if the legislator itself has already conducted a general regulatory impact assessment in the law-making process that has included matters of data protection.[34]

The Data Protection Officer (DPO, Art. 38 & 39 GDPR) takes part only in an advisory role, as Art. 35(2) GDPR clarifies. As a result, the DPO is not liable for a faulty, in particular incomplete DPIA.[35] If the data processing is shared between the controller and a data processor:[36] the processor has to assist the controller in carrying out the DPIA (Art. 28(3) lit. f and Recital 95 GDPR). As an interesting novelty, Art. 35(9) GDPR states that "the views of data subjects or their representatives" have to be considered in the

31) Legal definition in Art. 4(7) GDPR: "'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (…)".
32) This obligation mainly stems from Art. 30 GDPR.
33) A list of exception can also be found at Article 29 Data Protection Working Party (2017), p. 12 ff.
34) For details Martini (2018), paragraphs 64–71.
35) This consequence is mostly a result of how the GDPR defines and creates the position of a DPO. Foremost, the EU-legislator has chosen to shun the DPO from sanctions. For details (in German) Martini/Wagner/Wenzel (2018), p. 306, especially about the question if national law can deviate from the GDPR and establish sanctions for the DPO.
36) He is defined as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" (Art. 4(8) GDPR).

GPRI: Even though the obligation stays vague,[37] it opens a door to a more participatory process of impact assessment and can thus possibly increase the privacy level.[38]

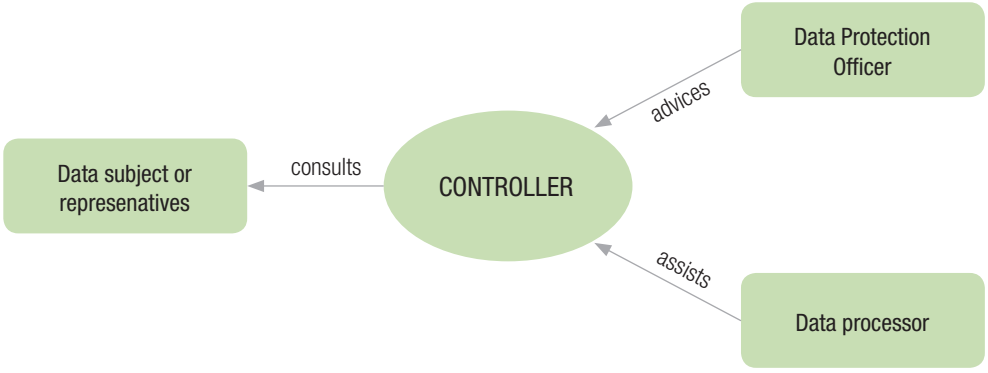

Figure 3: Actors involved in a DPIA

4) High risk for the rights and freedoms of a natural person

A DPIA is necessary, if there is a “high” (3.) “risk” (1.) to the “rights and freedoms of a natural person” (2.).

(1) Risk

The GDPR offers no definition of a “risk”. In general terms, when we speak of a “risk”, we are focusing on a certain event and its possible consequences.[39] The risk itself is the product of the likelihood and severity of a potential damage.[40] To be more precise: The possibilities range from a very likely and high damage, a small damage that is very likely, a high damage that is unlikely to the point of a very unlikely and small damage.

39) Martini (2018), paragraph 15a.
40) Article 29 Data Protection Working Party (2017), p. 5.

(2) Rights and freedoms of natural persons

When the GDPR talks about "the rights and freedoms of a natural person", it mainly focusses on the right to privacy in terms of the protection of personal data. However, also other fundamental rights can be at stake – such as freedom of speech, thought and movement as well as the prohibition of discrimination.[41] On top of that, Recital 85 illustrates how a violation of privacy regulations can, potentially, affect one's rights and freedoms;[42] also Art. 32(2) GDPR lists some potential damages that can occur.[43] As is the rule, a "damage" can be physical, material or non-material (Recital 75 sentence 1 GDPR). Furthermore, "certain types of processing and the extent and frequency of processing" ought to be considered.[44]

However, even though other parts of a technical system could lead to different damages,[45] or a device could have enormous general social consequences,[46] there always needs to be a connection to the processing of personal data. The factors that may lead to a risk in terms of Art. 35(1) GDPR are limited to the "nature, scope, context and purposes of the processing [of personal data]".

(3) Specification of a "high risk"

The GDPR chooses a graduated system of specifying the indeterminate legal concept of a "high risk". It involves specification by law, national and EU supervisory authorities and self-regulation.

41) Article 29 Data Protection Working Party (2017), p. 6.

42) "loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

43) "(…) from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed"

44) Recital 94 sentence 2 GDPR.

45) For example: A robot that also processes personal data could be a danger for the health of a person because of faulty hardware, e.g. optical sensors. However, this particular risk is not associated to the processing of personal data and wouldn't fall into the scope of a DPIA. On the contrary, risks that stem from the processing of personal data shall be considered in a DPIA (e.g. if the firmware of the robot malfunctions using facial recognition and denies a patient access to his medication) – and then it also includes financial or physical risks.

46) Using a smartphone is changing the modes of communication, bears addictiveness and simplifies surveillance. These broad aspects are not subject of a DPIA per se, but only if there is a risk factor that stems from the processing of personal data (e.g. if a certain OS is transmitting personal data to government agencies or a phone can easily be hacked).

a) Specification by law

Art. 35(1) GDPR clarifies the scope of the term "high risk" by stating that "the nature, scope, context and purposes of the processing" are to be taken in account. Furthermore, Art. 35(3) GDPR defines some specific cases where a DPIA "shall in particular be required":[47]

- When a "systematic and extensive evaluation of personal aspects […] which is based on automated processing, including profiling" leads to legal or similar effects for the natural person.[48] (The DPIA has to consider the minimum requirements and measures laid down in Art. 22(3) GDPR.)
- When special categories of data referred to Art. 9(1) GDPR (such as health data, biometric data or data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs) or data relating to criminal convictions (Art. 10GDPR) are processed on a large scale.[49]
- When publicly available areas are systematically monitored on a large scale. (The requirement mostly points towards CCTV-technology in public spaces).

b) Specification by supervisory authorities

The data protection supervisory authorities of the member states, their collaboration among each other, and the European Data Protection Board (EDPB) play an important role in the new privacy regime of the EU. The supervisory authorities have to be equipped with "complete independence"[50] and shall be "provided with the financial and human resources, premises and infrastructure necessary for the effective performance of their tasks"[51].

If the GDPR would consider it sufficient to establish three exclusive rule examples about constellations where a DPIA is compulsory necessary in Art. 35(3) GDPR, the consequence would be legal insecurity.

47) The list is "non-exhaustive", Article 29 Data Protection Working Party (2017), p. 9.For further details about the interpretation Martini (2018), paragraphs 28–32.
48) See also Recital 71.
49) See also Recital 75.
50) Recital 117 sentence 1 GDPR.
51) Recital 120 sentence 1 GDPR.

The specification of the abstract clauses would solely be left to courts, whose jurisdiction can take up to many years to be complete. In order to allow the EDPB and the member states to specify the terminology of a "high risk" more efficiently, Art. 35(4) ("shall") and (5) ("may") GDPR give the supervisory authorities the opportunity to come up with black and white lists. With these instruments, they can specify applications, sectors or other scenarios that need or do not need to be subject of a DPIA. In the meantime, some national supervisory authorities have already published their first black lists.[52)]

In order to harmonize the black and white lists, Art. 35(6) GDPR obliges the national supervisory authorities to employ the so-called "consistency mechanism"[53)]. Furthermore, the EDPR itself can issue guidelines, recommendations and best practices to specify the "high risk" (Art. 70(1) 1 lit. e GDPR).[54)] In spite of the possibilities to harmonize the black and white lists of the member states, the EDPR has so far given his opinion on 22 different concepts from the Member States.[55)] It can be expected that the way to a common understanding and legal certainty all over the EU is still long.

Even before the GDPR has come into force, the Article 29 Data Protection Working Party that was set up under the old Directive, has already released its opinion on how to specify the "high risk".[56)] In particular, it has come up with nine criteria[57)] to specify the "high risk" – if two of them are met, the controller shall consider to carry out a DPIA. It also gives some guidelines on when a processing operation should be part of a white list.[58)] The guidelines seem to have widely inspired the lists of the national supervisory authorities.

52) See for example the list of the data protection authority of the city-state of Hamburg (Germany), https://datenschutz-hamburg.de/dsgvo-information/art-35-mussliste-nicht-oeffentlich/. For an overview about all Opinions of the EDPB about the proposals of the Member states (so far), see https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en.

53) It is laid down in Art. 63 ff. GDPR and Recital 135. For details Martini (2018), paragraphs 40–43.

54) Article 29 Data Protection Working Party (2017), p. 5.

55) See https://edpb.europa.eu/news/news/2018/press-release-third-plenary-session-eu-japan-draft-adequacy-decision-dpia-lists_en.

56) Article 29 Data Protection Working Party (2017). The EDPA has endorsed the Guidelines.

57) Article 29 Data Protection Working Party (2017), p. 9 ff.

58) Article 29 Data Protection Working Party (2017), p. 12 ff.

c) Specification by self-regulation

The GDPR follows the thought that controllers and processors may often know better than state authorities how to reduce the privacy risks of a software application. Additionally, legal obligations might be followed more likely, if the economic actors have already been involved in the process of law-making. In order to include the data industry in the quest to find the best ways to protect personal data, Art. 35(8) GDPR makes clear that codes of conduct (Art. 40 GDPR)[59] "shall be taken into due account (…) in particular for the purposes" of a DPIA.

The provision is the expression of a normative compromise. One the one hand, the GDPR declares methods of self-regulation as an important tool that it wants to strengthen (also in order to relieve the supervisory authorities from some of their burdens). On the other hand, the EU legislator doesn't want to transfer too much power to self-regulatory efforts of the industry: private actors are neither democratically legitimized to create binding law nor necessarily unbiased in their regulatory approach. Therefore, the GDPR leaves the final competence with the supervisory authorities while hoping that codes of conduct will complement the process of GDPR-specification.

5) When does the DPIA have to take place?

A DPIA generally has to take place prior to the processing. The EU legislator also had in mind to incentivize a recurrent system of risk management inside data processing companies and to restrict possibilities of circumvention. Therefore, Art. 35(11) GDPR makes clear that a DPIA also has to take place in case of a change of risk. It is "a continual process, not a one-time exercise".[60] Overall, the GDPIA follows the motto "check if it works, act if it changes".

59) Thus, the provision does not seem to include the possibility of certification mechanisms according to Art. 42 GDPR. A different view can be found in Article 29 Data Protection Working Party (2017), p. 16; it also states that Binding Corporate Rules (BCR) "should be taken into account as well".

60) Article 29 Data Protection Working Party (2017), p. 14.

6) How can a controller make a legally compliant DPIA?

With the DPIA, the legislator has introduced a potentially powerful tool in order to increase the privacy level in data-driven market segments. At the same time, there is the risk that the controller might either be subject to a costly and a time consuming burden or will make use of the instrument solely in a restrictive and limited way. With the danger of the DPIA being not more than paying a lip service to a worried public, Art. 35(7) GDPR establishes some ground work about how a compliant DPIA has to look like. It defines a minimum of content requirements.

On the one hand, Art. 35(7) GDPR gives some guidelines on how to implement the instrument in a running business process. But on the other hand, it does not specify a detailed and obligatory methodology. What seems to open room for circumvention at first glance, also serves to give space for the individual case in question. In the practical use, data controllers will have to derive their own methodology from the historical examples of impact assessments in other areas of society.[61] Also existing frameworks, such as Standard Data Protection Model in Germany[62] or the industry standard ISO/IEC 29134:2017, could play an important role in structuring the process. Last but not least, the Article 29 Data Protection Working Party has done some groundwork by collecting some common criteria.[63]

In short, the process of a DPIA can be defined as:

Establish context → assess the risk → treat the risk

To treat the risk, the controller has to choose technical and organizational measures "including safeguards, security measures and mechanisms to ensure the protection of personal data" (Art. 35(7)lit. d GDPR). Only if those measures are not suitable to reduce the danger and/or the likelihood of the process-

61) See above B. For the question of what makes a DPIA "good" and further research see Wright et. al. (2013), p. 163: They come up with three main criteria: "Be more than a compliance check; be a process; be reviewed, updated and on-going throughout the life a project". Furthermore they state "stakeholder consultation as a key issue" (p. 163).

62) For an overview Article 29 Data Protection Working Party (2017), p. 21 (Annex 1).

63) For an overview of different frameworks from all over the EU, see Article 29 Data Protection Working Party (2017), p. 22 (Annex 2). It also "encourages the development of sector-specific DPIA frameworks" (p. 17).

ing risk under the threshold of a “high” one, the controller has to consult the supervisory authority (see Recital 84 sentence 4 GDPR and Art. 36 GDPR).

But the DPIA is not a static one-time scenario before a data processing is put into work. It rather forms an iterative process. In other words: It is a living and dynamic instrument.

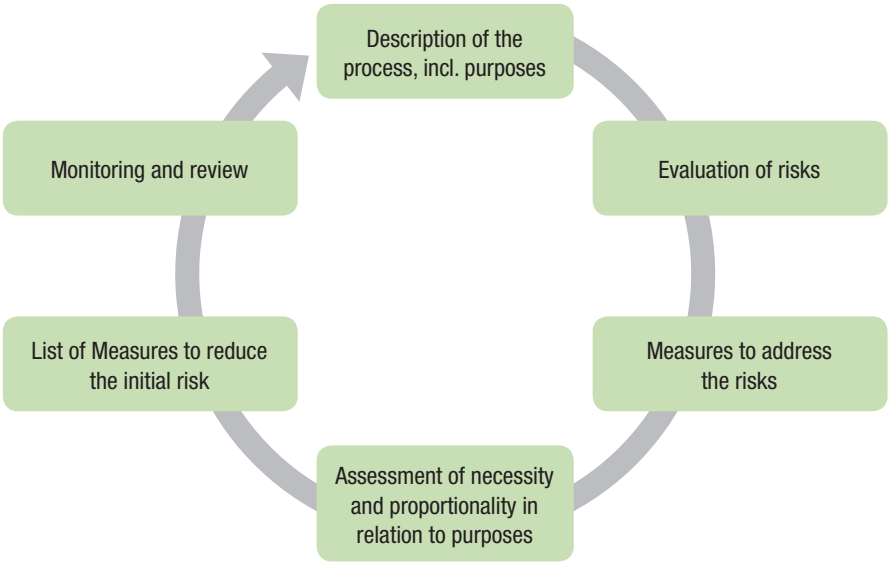

Figure 4: Iterative process of a DPIA[65)]

64) The figure is largely based on and inspired by Article 29 Data Protection Working Party (2017), p. 16.

Ⅱ. Limitations

The obligation to carry out a DPIA comes, firstly, as a burden for the economic freedom of every controller. It causes the need for additional managerial tasks, slows down the process of marketing a product and consumes time and resources to come up with a legally compliant DPIA. One could either criticize this as an unnecessary burden and a potential downfall for innovative processes – or regard a DPIA as a necessary reflection process that can only effectively be enforced into the data economy by binding law. However, the DPIA is not an entirely new instrument, but replaces the necessity of "prior checking" through the supervisory authority if processing operations are "likely to present specific risks to the rights and freedoms of data subjects" under the previous EU data protection law.[65] Thus, in some areas, the administrative burden of certain controllers has actually been reduced through Art. 35 GDPR, because they only need to consult the supervisory in case of a residual high risk (Art. 36 (1) GDPR). This is true at least in member states where the national legislation has chosen to implement and enforce a wide range for the previous concept of "prior checking".[66]

The legal term of "high risk" is vague and can only be fully effective through specification and interpretation. However, it doesn't seem impossible to bring the concept to life in a joint effort between legislator, supervisory authorities, EDPA, the industry and also the courts. As a first manifestation of a risk-based approach in EU data protection law, Art. 35 GDPR can serve as a sandbox and a trailblazer for a new

65) See Art. 20 of the EU-Directive 95/46/EG.

66) See the previous German law in Sec. 4d(5) and (6) BDSG (until May 2018): It was limited to "automated processes", was a responsibility of the DPO and didn't gain much significance (mostly due to a wide reservation of exemption). For more details, see Martini (2018), paragraphs 74, 75.

regulatory perspective on how to deal with the numerous dangers connected to the emergence of new data-driven technology. Whether it will slowly replace that current concept of a "general ban with a reservation of authorization" or rather develop into a supplementary extension of the scope of the GDPR will be subject of political debate. In any case, the basic idea to link certain (additional) regulatory measures to the risk-level that a specified application will presumably bring to the market, can (and should) constitute a central element of future legislation concerning algorithmic decision making, Artificial Intelligence and other innovative technologies.

Furthermore, the aspect of "engaging stakeholders, including the public"[67] that Art. 35(9) GDPR addresses briefly, stays relatively vague and is not mandatory ("where appropriate"; "shall"). Also, dangers which do not stem from the processing of personal data are not covered by Art. 35 GDPR, even though the possible dangers are not limited to privacy breaches (see Art. 1 (2) GDPR and Recitals 75 and 85 GDPR).[68]

Another main point of criticism against Art. 35 DSGVO has been addressed by Mario Martini:[69] He points his finger at the fact, that a DPIA has to be documented internally by the controller, but not published for a wider audience.[70] Thus, the EU-legislator has missed to guarantee a sufficient level of transparency of potentially risky data processes and has weakened the control mechanisms against faulty impact assessments. In the worst case, controllers can classify applications with an actual high risk as not risky without the public or the supervisory bodies even taking notice. Especially for consumer organizations it could be an important tool to be able to take a closer look at the DPIA in order to find out about the general architecture and potential impact of an application.

67) Wright et. al. (2013), p. 174.
68) See above C.IV.2.
69) Martini (2017), p. 1022.
70) See also Article 29 Data Protection Working Party (2017), p. 18: "Publishing a DPIA is not a legal requirement of the GDPR."

Ⅲ. Reform proposals

Even though the instrument of a DPIA still has to pass the practical test in the EU, some reforms have been proposed. They are based on the limitations of Art. 35 GDPR in its current form.

First of all, the transparency of the DPIA could be improved by establishing a legal obligation to publish its results, instead of treating it as a mostly internal review mechanism.[71] Every consumer could thus gain more insight in the risks of a data processing that he is subject of as well as in the countermeasures a controller has taken into account. As a result, the degree of public supervision over potentially risky data processes could be raised to a high level. Also, there would be a higher incentive for data controllers to take the DPIA more seriously if they have to expect attentive actors (such as consumer organizations or media outlets) to take a closer look at their results.[72]

To institutionalize the obligation to publish, the EU could establish a registry for DPIAs:[73] It could then become much easier for the public to access the DPIA of different controllers instead of having to browse the website of each application in question. Also the supervisory authorities would gain a better overview about the impact assessments conducted by controllers.

71) Martini (2017), p. 1022. Further thoughts will be found in Martini (2019).

72) However, the scope of the obligation to publish might be limited in certain cases. See Wright et. al. (2013), p. 175: "If there are security, commercial-in-confidence or other competitive reasons for not making a PIA public in full or in part, the organisation should publish a redacted version or, as a minimum, a summary."

73) This demand is shared by Wright et. al. (2013), p. 174.

Secondly, the assessment of whether a data processing contains a "high risk" (or not) could be complemented by mechanisms of an external auditing.[74] If independent organizations or external service providers review the DPIA, it potentially becomes less likely that the internal process of the controller is erroneous or intentionally curtailed. A step towards that goal would be to widen the advisory role of the DPO in Art. 35(2) GDPR by making his involvement compulsory ("must" instead of "shall"). An obligation to implement an external audit could also be laid down for specific cases – for example all data processes that are not subject of the white list in Art. 35(5) GDPR. Another possibility would be to make use of the certification mechanisms laid down in Art. 42 GDPR to cover at least some aspects of the process that leads to a DPIA.

Thirdly, the EU legislator should think about how to bring the aspect of participation of different stakeholders to full blossoming. Art. 35(9) GDPA should only be seen as a first step of a way "of gathering fresh input on the perceptions of the severity of each risk and on possible measures to mitigate these risks"[75]. To give more guidance to those who carry out a DPIA, the supervisory authorities should gather and give access to more information (incl. questionnaires, checklists and methodological approaches).[76]

Lastly, the scope of the DPIA might fall short of the needs of a widespread control mechanism for software applications. In times of growing digitalization of many areas in consumer's daily life, not only the dangers for privacy (or privacy related fields) should be taken into account: An impact assessment could also include risks that are not connected purely to the processing of personal data, but stem from other parts of an IT-system.[77] However, the GDPR is limited by Art. 16 TFEU[78]: Its scope only covers "the protection of individuals with regard to the processing of personal data". As a result, without fundamental changes

74) See also Wright et. al. (2013), p. 176.

75) Wright et. al. (2013), p. 174.

76) See also Wright et. al. (2013), p. 175. A good example for an explanation (incl. a template) is given by the ICO in the UK and can be found here https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/.

77) About this regulatory idea in the context of an extensive legal analysis of the regulation of algorithmic decision-making and Artificial Intelligence, Martini (2019), forthcoming.

78) Treaty on European Union and the Treaty on the Functioning of the European Union, 2012/C 326/01. See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT.

to the legal doctrine of data protection law and its groundwork in the TFEU, the GDPR cannot widen the scope of a DPIA without interfering with other fields of regulation (such as anti-discrimination law, food safety, health regulation etc.). Even though the impact assessment can consider different fundamental rights (see also Art.1 (2) GDPR: “in particular”), the processing of personal data has to stay at its center.

IV. Conclusion

The DPIA is one of the most interesting legal innovations in the GDPR.[79] Art. 35 GDPR is based on the vast experiences connected to the instrument of impact assessments worldwide – and can be seen as a major step towards a more sustainable and privacy-friendly way of developing and marketing digital products. It specifies the idea of Privacy by Design into an institutionalizable process.

At the same time, the DPIA serves as a trial balloon for the concept of a risk-based approach in data protection law and beyond. It bears the chance that every processing gets the (legal and factual) handling that fits its risk. Even though the regulatory concept of Art. 35 GDPR is complex, it succeeds in distributing the task to specify the legal terminology to different players, including modes of self-regulation. As a result, it might serve as a reference model for the legal handling of new technologies.

Whether the DPIA turns out as a success doesn't only depend on the data industry and their willingness to embrace the ideal of developing ethical and privacy-friendly IT-products. It will vastly be up the supervisory authorities and their EU-wide collaboration to keep highly profitable data-driven market segments at bay and establish a healthy balance between economical and societal interests. For that, the member states have to equip them with sufficient resources – only then will they be able to fulfill their various duties.

Additionally, the supervisory authorities should pay close attention to guide (especially small and medium size) companies through the new bureaucratic burdens, thus fulfilling their advisory role. At the same

79) Martini (2018), paragraph 1.

time, they should observe closely whether the self-assessment about a potential initial and residual high risk has been rightly placed solely in the hands of the controller.

Despite all positive expectations, the practical test of the DPIA still has to pass its field test – as does the GDPR as a whole. But as the “California Consumer Privacy Act" from 2018 shows, the European approach to privacy regulation has already inspired other legislative bodies – notably reaching closer to the highly innovative and profitable data companies in the Silicon Valley. In the end, only time will reveal if the GDPR will turn out as a small or a giant leap for mankind.

Literature

Article 29 Data Protection Working Party (2017): “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”, wp248rev.01, adopted on 4 April 2017, retrieved from http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

Bamberger, K., Mulligan, D. (2013), “Privacy in Europe: Initial Data on Governance Choices and Corporate Practices”, The George Washington Law Review, Vol. 81, 2013, pp. 1529–1664.

Edwards, L., McAuley, D. and Diver, L. (2016): "From Privacy Impact Assessment to Social Impact Assessment", 2016 IEEE Security and Privacy Workshops (SPW), San Jose, pp. 53–57, doi:10.1109/SPW.2016.19.

de Hert, P., Kloza, D., Wright, D. (2012): “Recommendations for a privacy impact assessment framework for the European Union”, Brussels – London, retrieved from https://piafproject.files.wordpress.com/2018/03/piaf_d3_final.pdf.

Martini, M. (2017): “Algorithmen als Herausforderung für die Rechtsordnung”, Juristen Zeitung (JZ) 2017, pp. 1017–1025.

Martini, M., Wagner, D., Wenzel, M. (2018): “Das neue Sanktionsregime der DSGVO – ein scharfes Schwert ohne legislativen Feinschliff. Teil 1”, Verwaltungsarchiv (VerwArch) 2018, pp. 296-335.

Martini, M. (2018): Commentary on Art. 35 DSGVO, in: Paal/Pauly, Datenschutz-Grundverordnung / Bundesdatenschutzgesetz, München, 2nd edition, 2018.

Martini, M. (2019): “Herrschaft der Algorithmen – Ohnmacht des Rechts?”, Springer, Wiesbaden, forthcoming (approx. 350 pages).

Morgan, R. (2012): “Environmental impact assessment: the state of the art”, Impact Assessment and Project Appraisal, 30:1, pp. 5–14, DOI: 10.1080/14615517.2012.661557.

Morrison-Saunders, A., Pope, J., Gunn, J., Bond, A., Retief, F. (2014): “Strengthening impact assessment: a call for integration and focus”, Impact Assessment and Project Appraisal, 32:1, pp. 2–8, DOI: 10.1080/14615517.2013.872841.

Clarke, R. (2009): “Privacy impact assessment: Its origins and development”, Computer Law & Security Review, Volume 25, Issue 2, 2009, pp. 123–135, retrieved from http://www.rogerclarke.com/DV/PIAHist-08.html.

Hamidovic, H. (2010): “An Introduction to the Privacy Impact Assessment Based on ISO 22307”, ISACA JOURNAL VOLUME 4, 2010, pp. 1–5.

Strauß, S. (2017): “Privacy Analysis – Privacy Impact Assessment”, in: Hansson, S. O. (ed.), The Ethics of Technology – Methods and Approaches, London and New York, pp. 143–156.

Webler, T., Kastenholz, H., Renn, O. (1995): “Public Participation in Impact Assessment: A Social Learning Perspective”, Environmental Impact Assessment Review, Volume 15, Issue 5, September 1995, pp. 443–463.

Wirth, C. / Kolain, M. (2018): “Privacy by BlockChain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data”, in: Prinz/Hoschka (Eds.), Proceedings of the 1st ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies, Amsterdam 2018, DOI: 10.18420/blockchain2018_03.

Wright, D., Finn, R. and Rodrigues, R. (2013): “A Comparative Analysis of Privacy Impact Assessment in Six Countries”, Journal of Contemporary European Research. 9 (1), pp. 160–180.

Wright, D., de Hert, P. (2012): “Privacy Impact Assessment”, Springer, Dordrecht.

Annex: Relevant provisions and recitals of the GDPR

Art. 35 GDPR
Data protection impact assessment

1. [1]Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. [2]A single assessment may address a set of similar processing operations that present similar high risks.

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

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

    1. 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;

    2. 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

    3. a systematic monitoring of a publicly accessible area on a large scale.

4. [1]The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. [2]The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. [1]The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. [2]The supervisory authority shall communicate those lists to the Board.

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

7. The assessment shall contain at least:

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

    2. an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

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

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

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

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

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

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

Art. 36 GDPR
Prior consultation

1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment 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.

2. [1]Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. [2]That period may be extended by six weeks, taking into account the complexity of the intended processing. [3]The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. [4]Those periods may be

suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:

    1. where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

    2. the purposes and means of the intended processing;

    3. the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;

    4. where applicable, the contact details of the data protection officer;

    5. the data protection impact assessment provided for in Article 35; and

    6. any other information requested by the supervisory authority.

4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

Recital 75

The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the

reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

Recital 84

[1]In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. [2]The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. [3]Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.

Recital 89

[1]Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. [2]While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. [3]Such indiscriminate general notification

obligations should therefore be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. [4]Such types of processing operations may be those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing.

Recital 90

[1]In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. [2]That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.

Recital 91

[1]This should in particular apply to 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 example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. [2]A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. [3]A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic

devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. [4]The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. [5]In such cases, a data protection impact assessment should not be mandatory.

Recital 92

There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

Recital 93

In the context of the adoption of the Member State law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question, Member States may deem it necessary to carry out such assessment prior to the processing activities.

Recital 94

[1]Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory

authority should be consulted prior to the start of processing activities. [2]Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person. [3]The supervisory authority should respond to the request for consultation within a specified period. [4]However, the absence of a reaction of the supervisory authority within that period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. [5]As part of that consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.

Recital 95

The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.

입법평가 Issue Paper 18-15-⑤

Data Protection Impact Assessment
(Art. 35 GDPR) as a Tool of Privacy Regulation

발 행 일　2018년 11월 15일
발 행 인　이익현
발 행 처　한국법제연구원

세종특별자치시 국책연구원로 15 (반곡동, 한국법제연구원)
T.044)861-0300　F.044)868-9913
등록번호　1981.8.11. 제2014-000009호
http://www.klri.re.kr

ISBN 978-89-6684-893-5　93360

Data Protection Impact Assessment (Art. 35 GDPR) as a Tool of Privacy Regulation

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE
세종특별자치시 국책연구원로 15 (반곡동, 한국법제연구원)
T.044)861-0300 F.044)868-9913 http://www.klri.re.kr

9 788966 848935 93360
ISBN 978-89-6684-893-5
값 5,500원