Adjudicating personal data protection in the European Union: what to expect from impact assessments?

Vazquez Maymir, Sergi; Ioannidis, Nikolaos

Publication date:
2019

Document Version:
Final published version

Brussels Laboratory for Data Protection & Privacy Impact Assessments (d.pia.lab)
Research Group on Law, Science, Technology & Society (LSTS)
Vrije Universiteit Brussel (VUB)

Adjudicating personal data protection in the European Union: what to expect from impact assessments?

Monday 20 May 2019
14:00 – 16:30
Brussels, Belgium

Public report from the workshop
by Sergi VAZQUEZ MAYMIR and Nikolaos IOANNIDIS

Vrije Universiteit Brussel
Faculty of Law and Criminology

Pleinlaan 2
1050 Elsene (Brussel)
room **4C306**

dpialab.org/events

Adjudicating personal data protection in the European Union: what to expect from impact assessments?

Public report by Sergi VAZQUEZ MAYMIR[1] and Nikolaos IOANNIDIS[2]

Introduction

The European Union (EU)'s General Data Protection Regulation (GDPR) brings to the fore a plethora of novel solutions aiming at, *inter alia*, better safeguarding interests of individuals whenever their personal data are being handled. Amongst these novelties is an obligation, imposed on data controllers, to carry out – before these data are handled – a process of data protection impact assessment (DPIA). This process is required to be conducted for data handlings capable of presenting "high risk" to the "rights and freedoms of natural persons" in order to "ensure the protection of personal data and to demonstrate compliance" with the law (Article 35 GDPR).

However, DPIA as such has seldom been an object of any judicial or extra-judicial proceedings. Due to the minimalistic contents of its main provisions, occasional vagueness of its terminology and rather high fines for non-compliance and malpractice, it already provokes a number of legal questions, further magnified by the relative novelty of this requirement.

Therefore, the aim of this workshop was to map and subsequently analyse possible legal questions concerning DPIA that might emerge in a set-up of legal proceedings, at both national- and EU level. Some of them might be answered by looking at the experience of impact assessment in other areas and jurisdictions, while others, exclusive to the DPIA, need further clarification (e.g., assessing "high risk" to the "rights and freedoms of natural persons").

The workshop was held under the Chatham House Rule, which reads: "When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed."[3]

Questions

Q1: Outcome rather than method: Is it possible to fine a data controller for having poorly performed the process of DPIA? Can the negligence of a data controller be proven, beyond the mere fact of not having carried out a DPIA?

Q2: Purpose of the DPIA: Is the process of DPIA a purpose by itself, or is its purpose to support responsible and informed decision making? Is it better to evaluate the responsibilities of data controllers based on the results obtained rather than the method used?

Q3: The risk to a right: What is or should be an *acceptable level* of risks to rights and freedoms?

Q4: DPIA as a proof of due diligence: Can or should the process of DPIA account as evidence for the benefit of the data controller or as a proof of due diligence?

[1] E-mail: Sergi.Vazquez.Maymir@vub.be.
[2] E-mail: Nikolaos.Ioannidis@vub.be.
[3] Cf. https://www.chathamhouse.org/about-us/chatham-house-rule.

Q5: Dealing with moderate or medium level risks: How tolerant should the supervising authorities of data controllers be towards *moderate or medium* level of risks?[4]

Q6: Balancing benefits: How far should the process of DPIA go in distinguishing, on the one hand, between the *benefit obtained* as a result of a processing activity by private entities and society in the case of legislative measures, and on the other hand, the *impact* towards the data subject?

Q7: Assessing data processing: Does necessity and proportionality extend beyond the concepts of risk and its likelihood? Can processing still be disproportionate regardless of the risk source? Could a data controller still proceed to the envisaged processing, when, after having conducted a DPIA, only medium or low risks are identified or when the interference remains disproportionate?[5]

Q8: The good the bad and the objective DPIA: What does it mean to perform a DPIA correctly and appropriately? Taking into account Recital 76 GDPR,[6] how do we define an "objective risk assessment" in the context of data protection law? Should "objectivity" become one of the criteria used to assess whether a DPIA has been correctly performed? [7]

a. If the answer is positive, then, should data controllers performing a "non-objective" assessment be fined?[8]

b. How does objectivity interplay during the analysis of risk thresholds? Is it important as a data controller to objectively justify the decision not to perform a DPIA even though any of the exempting criteria of Article 35 would apply?

Q9: A legal and technical endeavour: How does the role of software developers and technology manufacturers influence the responsibility of data controllers over their control on the processing activities? Considering the fundamental role of technological partners, should we consider the "actual control" of controllers over the data processing operations?

Q10: Transparency and DPIA: Considering Articles 12, 13 and 14 GDPR (including transparency and compliance with the data protection principles), how could the obligation to provide information to the data subject be framed? Is listing the information enough or should the data controller take additional steps?[9]

---

[4] While the threshold is clear with regard to risks which are considered high, there is less consistency in the treatment of low and residual risks.

[5] We should question whether Article 24, 35 and 36 GDPR be interpreted as controllers being loosely able to undertake any processing activity which is not or no longer likely result in a risk to individuals regardless of the underlying purpose, given the presence of measures to mitigate risks and provide that remaining obligations of the GDPR have been complied with.

[6] Recital (76) GDPR: "The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk".

[7] When assessing risks during the threshold analysis, you need to objectively justify your decision to perform or not a DPIA. If we do not understand what "objective assessment" means, it could be the case that we will face huge fines wrongly.

[8] This is also relevant with regard to the role of the DPIA as evidence.

[9] Cf. Article 29 Working Party 'Guidelines on transparency'.

Q11: To inform or not to inform: From the perspective of the GDPR and taking its human-centric approach, when would it be appropriate to seek the views of the data subject? When is not appropriate to involve the data subject?[10]

Q12: Practicalities of consultation and representativeness: Who qualifies as data subject in the case of groups or communities? Who is considered to be their representative? How many of them would need to be surveyed? What do we mean by "large scale processing operations", and how many data subjects would need to be consulted and actively take part in the survey? What are the consequences of not performing this kind of consultation?

Q13: The difference between (actual) infringement and a probable infringement: What is likely to result in a "high risk to rights and freedoms of natural persons"? Given that, in practice, you either have an infringement of rights or you do not, having a "high risk" involves the embracement of risk management doctrines, how is that to be considered in the context of a DPIA?

Q14: Semantics of the proportionality test: What does "adequate and proportionate" mean in the context of data processing operations?

Q15: Lessons from environmental law: How should data protection embrace the concepts that have been coming up in the field of environmental law regarding grades/thresholds/levels of protection, such as foresight, precaution, threats of harm?

Q16: How much justification is enough: If the quality and empirical basis of justification should be directly proportional to the level of a foreseen harm and the consequences of being wrong, how should we justify the appropriateness of a processing operation and the safeguards adopted to mitigate its impact?[11]

Q17: How should harm be defined? Following the environmental law approach, if harm always surpasses our expectations regarding who could be potentially affected by a determinate activity, what are the criteria to define "harm" when performing a DPIA? [12]

Q18: Distinguishing between risk management and risk assessment: What is the difference (if any) between risk management and risk assessment?[13]

[10] It difficult to assess the limits of the duty to consult in those cases where there are both organizations representing individuals and then also separately individuals acting on their own. How to weight the relevance of these actors in the consultancy process is not clear.

[11] To justify a governmental interference on the freedoms of individuals such as in the case of public policy on smoking or healthy food, a high level of evidence would be required. The choice of stringent evidence is relevant to any particular scenario and depends on the consequences of being wrong rather than the consequences of acting or not acting. This poses an ethical question to the assessor who must weight the consequences of assessing wrongly.

[12] One of the lessons learned from impact assessments in environmental law is that "we always underestimate risks", both the nature of harm and the extent of harm, "we never ever go in the other way".

[13] There is a serious danger of causing confusion when separating risk assessment from risk management, arguably a "nonsense" to one of the participants.

Q19: Assessment needs understanding: How can we ensure that the necessity and proportionality assessment will meet the quality expected from the DPA?[14]

Q20: The resources dedicated by the controllers: Are guidelines available to provide SMEs or economically weak entities with tools to perform the process of DPIA, taking into account that not everyone has the resources that big tech companies have?

Q21: Criteria to perform or not perform: The WP 29 guidelines identify a number of criteria, which determine whether a DPIA should be performed or not. What is the meaning and nature of these "criteria" to the interpretation of a DPIA in practice?

Q22: The consequences of misinterpretation: What are the consequences of misinterpreting a basic actor/element of the assessment (i.e., who is the data subject)?

Q23: New and old technology and the scope of DPIA: What does "new technology" mean, and how will it narrow or broaden the scope of the DPIA process? Is there a need for a DPIA for "old technology", such as Facebook or automated decision-making?

Q24: Privacy by design and by default: What is the relation between the DPIA and the concepts of privacy by design and by default (Article 25), when read in conjunction with the GDPR, as a whole?

Q25: Data subject and the need-to-know approach: As a data controller, what is the appropriate format to use in order to reach the data subject? Which is the level of information to be granted to the data subject? How can we ensure that the information provided to the data subject is not biased by the data controller?

Q26: Level of transparency: Is there a possibility to request access to DPIA in order to mitigate possible complaints? The GDPR creates a series of criteria under which a DPIA needs to be conducted, but then, we also need to consider how national and regional authorities will add norms and rules. In that respect, how do we ensure harmonization?

Q27: Territorial scope of the data protection obligations: What if a data controller, registered in Belgium, based on the list of national exemptions is not required to perform a DPIA in Belgium, but the same data controller provides services in another Member State where that same activity is regarded as requiring a DPIA?

Q28: *Ex ante* or *ex post*, the less intrusive assessment: Should we consider the DPIA as a s a tool to reach an ex-post justification to a processing operation? How does the GDPR and the DPIA encourage the assessment and adoption of the "less intrusive option" with respect to the interference of individual rights?[15]

Q29: Public authorities and DPIA: Where the processing carried by a public authority is based on enacted legislation and there is no obligation foreseen to perform such DPIA process in such legislation, is there an exemption to perform the process of DPIA?

[14] Considering that DPIA includes an assessment of the necessity and proportionality of the processing operations, this implies that the data controllers understand what the processing is about and what it can do. From a procedural practical point of view (Article 36(2) GDPR), the DPA has the power to reject the assessment on necessity and proportionality.

[15] The example of loyalty cards and fingerprints and how that was in compliance with the data protection obligation to carry out the "less intrusive option" when processing data (Article 5 GDPR).

Q30: The liability of public authorities: Can public authorities/legislators be held liable for not performing or wrongly performing a DPIA? Which is the competent authority to attest and rule on such cases? How would the consultation procedure, foreseen in Article 35(9), been done in the public context?

Q31: The evidential value of DPIA in courts: What could be the added value of a DPIA in courts?[16] Would the DPIA be assessed as a positive circumstance, even if not explicitly required by law?

Q32: The assessment of DPIA by the courts: To what extent will courts assess the DPIA? How will they scrutinize it? Will they merely check the formal compliance, or will they also examine its content?

Q33: Liability generated from DPIA publishing: To what extent assessors might be held liable for publishing a DPIA? Can this be used as a basis for damage claims against the data controller who published the DPIA?

Q34: Challenging European Data Protection Board (EDPB) opinions: How to challenge a decision of the EDPB, if this is possible? Where do we challenge a decision/opinion of the EDPB?

Q35: Legality of national legislation on DPIA duties: Are national legislators allowed to enact laws, requiring DPIA to be carried out? An example is Belgium, where it is mandatory to carry out a DPIA process on CCTV. Would the CCTV Belgian requirement be contrary to EU law?

The workshop was organised within the framework of the research project **PERSONA** (*Privacy, ethical, regulatory and social no-gate crossing point solutions acceptance*), funded by the European Union's Horizon 2020 Research and Innovation Programme under grant agreement No. 787123

[16] This particularly refers to those cases where the data controllers do not fall under Article 35, but have carried out the process of DPIA nevertheless.