COMPUTER LAW & SECURITY REVIEW ■■ (2017) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Understanding the notion of risk in the General Data Protection Regulation

Raphaël Gellert *

Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, The Netherlands

Keywords:
Risk
GDPR
Data protection and privacy impact assessments

ABSTRACT

The goal of this contribution is to understand the notion of risk as it is enshrined in the General Data Protection Regulation (GDPR), with a particular on Art. 35 providing for the obligation to carry out data protection impact assessments (DPIAs), the first risk management tool to be enshrined in EU data protection law, and which therefore contains a number of key elements in order to grasp the notion. The adoption of this risk-based approach has not come without a number of debates and controversies, notably on the scope and meaning of the risk-based approach. Yet, what has remained up to date out of the debate is the very notion of risk itself, which underpins the whole risk-based approach. The contribution uses the notions of risk and risk analysis as tools for describing and understanding risk in the GDPR. One of the main findings is that the GDPR risk is about "compliance risk" (i.e., the lower the compliance the higher the consequences upon the data subjects' rights). This stance is in direct contradiction with a number of positions arguing for a strict separation between compliance and risk issues. This contribution sees instead issues of compliance and risk to the data subjects rights and freedoms as deeply interconnected. The conclusion will use these discussions as a basis to address the long-standing debate on the differences between privacy impact assessments (PIAs) and DPIAs. They will also warn against the fact that ultimately the way risk is defined in the GDPR is somewhat irrelevant: what matters most is the methodology used and the type of risk at work therein.

1. Introduction

The goal of this contribution is to understand the notion of risk as it is enshrined in the General Data Protection Regulation (GDPR).[1] It puts a particular focus upon Art. 35 insofar as it provides for the obligation to carry out data protection impact assessments (DPIAs) – the first risk management tool to be enshrined in EU data protection law – and therefore contains a number of key elements in order to grasp the notion.

The notion of risk is of increasing importance in the GDPR, among others because it incorporates a so-called risk-based approach. The adoption of this risk-based approach has not come without a number of debates and controversies,[2] notably

* Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, The Netherlands.
E-mail address: rgellert@uvt.nl.

[1] 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), [2016], *OJ L 119/1*.

[2] See (Council of the European Union, 2013); and (DigitalEurope, 2013, p. 1): "The risk-based approach as a means to improve the data protection Regulation has been widely debated in the Council."

https://doi.org/10.1016/j.clsr.2017.12.003

Please cite this article in press as: Raphaël Gellert, Understanding the notion of risk in the General Data Protection Regulation, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.12.003

on the scope and meaning of the risk-based approach.[3] The Article 29 Working Party has itself weighed in on the debate, clarifying the scope of the risk-based approach (Art. 29 WP, 2013b, 2014), and more recently with revised Guidelines on DPIAs (Art. 29 WP, 2017).

Yet, what has remained so far out of the debate is the very notion of risk itself, which underpins the whole risk-based approach.

The uncertainty surrounding the meaning of risk in the GDPR is probably best epitomised by Art. 35 itself. Art. 35(1) provides that:

> *"Where a type of 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 (. . .) on the protection of personal data."*[4]

As one can see, there seems to be a contradiction concerning what the object of impact assessment is in the first place. What should be assessed? The likely high risk to the data subject's rights and freedoms, or the impact on the protection of personal data?[5] And how is it that both seem to be connected in the definition of an impact assessment?

This lack of clarity surrounding the notion of risk can also be visible in a number of impact assessment methodologies that will be examined throughout the present piece, and which mobilise diverging notions of risk.

In order to do so it starts by defining the notion of risk, of risk analysis (as the process to concretely use the notion of risk), and their respective constitutive elements. These will in turn be used as tools of description of the notion of risk enshrined into the GDPR.

Of particular importance, is the fact that risk is composed of both an event and its consequences. This property of risk will be critical in shedding some light on the notion of GDPR risk. By framing risk as composed of both an event and its consequences, one can understand the GDPR risk as being about "compliance risk", with the lack of compliance being the "event", and the risks to the data subjects' rights and freedoms being the consequence (i.e., the lower the compliance the higher the consequences upon the data subjects' rights). This stance is in direct contradiction with a number of DPIA methodologies as well as Art. 29 WP documents,[6] which argue for a strict separation between compliance and risk issues: risk calculations can only come on top of fulfilled compliance obligations. It will argue in favour of integrating compliance within the risk assessment process (i.e., compliance is itself already a matter of risk) by paying heed to the other objectives of the risk-based approach (scalable protection on the ground), and by the fact that the other elements of risk contained in Art. 35 GDPR (namely so-called risk criteria) also seem to point towards this solution.[7]

The conclusion will use these discussions as a basis to address the long-standing debate on the differences between privacy impact assessments (PIAs) and DPIAs. They will also warn against the fact that ultimately the way risk is defined in the GDPR is somewhat irrelevant: what matters most is the methodology used and the type of risk at work therein.

2. Definition of risk and of its constitutive elements

2.1. *Definition of risk*

In a nutshell, one can argue that risk can be given two meanings – a vernacular one and a more technical one. In the vernacular sense, risk is usually referred to as future, possible danger, i.e., as "an eventual danger that can be foreseen only to some extent" (Godard et al., 2002, p. 12). In a technical sense however, risk can be seen as a two-fold notion. It is used for decision-making based on the assessment of future events. Its constitutive elements are two distinct yet joined operations: forecasting future events (both negative and positive) and making decisions on the basis thereof.[8] One can therefore argue that 'any decision relating to risk involves two distinct and yet inseparable elements: the objective facts and a subjective view about the desirability of what is to be gained, or lose, by the decision'.[9]

2.2. *Risk and risk analysis*

Nonetheless, risk remains an abstract notion in need of methodologies, templates, and processes that concretely implement it.[10] This is the role of risk analysis (also sometimes referred to as risk management).[11] Mirroring the two-fold dimension of risk, risk analysis is composed of two steps: risk assessment and risk management. Risk assessment measures the level of risk (in terms of likelihood and severity), while the point of risk management is to decide whether or not to take the risk.[12] The decision at risk management level is usually accompanied by measures aiming at reducing the level of risk: sometimes the risk level is too high, but it can be reduced to an acceptable level. These measures can be referred to as risk reduction, risk control, risk response, or more generally, risk mitigation measures.[13] It is commonly accepted that it is impossible to reduce risks to a zero level.[14] So the whole point

[3] On these discussions, see (Gellert, 2016; Macenaite, 2017).
[4] Emphasis by the author.
[5] For a similar line of reasoning, see (Quelle, 2015, sec. 2.5).
[6] These documents will be discussed *infra*, see others (Art. 29 WP, 2014; Art. 29 WP, 2017).
[7] Concerning the objectives of the risk-based approach, see *infra*, section 3.3.2.
[8] (Bernstein, 1996, p. 3). On the fact that a risk can refer both to positive and negative events occurring, see (Douglas and Wildavsky, 1983).
[9] (Bernstein, 1996, p. 100). Note that the ISO defines risk as the "effect of uncertainty on objectives" (2009, p. 1). See also the definition provided by the Art. 29 WP and defining risk as "a scenario describing an event and its consequences, estimated in terms of severity and likelihood" (Art. 29 WP, 2017, p. 6).
[10] (Power, 2007, p. 12).
[11] Not to be confused with the risk management step as such, see herein below.
[12] (Warner, 1992, p. 5).
[13] (ISO, 2009, p. 6).
[14] See, e.g., (Gellert, 2015, p. 15).

Please cite this article in press as: Raphaël Gellert, Understanding the notion of risk in the General Data Protection Regulation, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.12.003