WHY THE GDPR RISK-BASED APPROACH IS ABOUT COMPLIANCE RISK, AND WHY IT'S NOT A BAD THING

Raphaël Gellert

Researcher, Vrije Universiteit Brussel – Law, Science, Technology, and Society (LSTS)
Pleinlaan 2, 1050 Ixelles, BE
raphael.gellert@vub.ac.be

Keywords: ***Data protection, risk, GDPR, risk-based approach***

Abstract: *The topic of the risk-based approach to data protection has stirred quite some controversy, with the main criticism arguing that it goes directly counter the fundamental right nature of the right to personal data protection. Given the latter, and following the opinion of the Article 29 Working Party, the General Data Protection Regulation (GDPR) has adopted a risk-based approach that is limited to matters of compliance. This presentation explores what is exactly meant by such compliance oriented risk-based approach, and more in particular how it can nonetheless take into account the whole spectrum of the data subjects' fundamental rights and freedoms affected by data processing operations.*

1. Introduction

The goal of this contribution is to elucidate the notion of risk as it has been enshrined in the EU recently adopted General Data Protection Regulation (GDPR).[1] The GDPR has taken on board the so-called risk-based approach, which translates among others with the obligation to undertake so-called data protection impact assessments (DPIAs), enshrined in Art 35 of the GDPR.

This contribution investigates the notion of risk at the heart of DPIAs and of the risk-based approach more generally. It starts by showing that this notion of risk contains an important contradiction since it requires to take into account the possible (high) risks to the data subjects' rights and freedoms stemming from their data processing operations, and simultaneously to assess the latter's impact on the protection of personal data.

The hypothesis the present contribution puts forth is that this apparent contradiction in the GDPR can be solved if one considers that the risk at stake is a compliance risk, that is, a risk that the processing operation will (not be) compliant with data protection requirements.

The contribution goes on to explain the rationale of such notion of risk by paying heed to the debate between risk-based and rights-based approaches to data protection.[2] It shows that the notion of compliance risk appears as the only solution to an apparent catch. That of simultaneously shifting towards the risk management of data processing operations, whilst simultaneously respecting the rights-based nature of data protection as a fundamental right of the EU, which entails in particular to uphold its so-called data protection core principles (e.g., data minimisation, purpose limitation).

After having explained the rationale for such a notion of compliance risk, it goes on to show that it can actually do what it promises, that is, both managing the risks of non-compliance and go beyond said compliance by

[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), OJ L 119.

[2] For a summary of these debates, see Gellert 2016.

taking into account the broader spectrum of all the rights and freedoms potentially violated by a data processing operation. This is done by providing an in-depth analysis of how risk and risk management operate.

Finally, the contribution concludes with some reflexions on the level of protection afforded by the notion of risk enshrined in the GDPR, with a particular emphasis on the articulation between compliance and the data subjects' fundamental rights and freedoms.

2. The contradiction with the notion of risk in Art. 35 GDPR

The uncertainty surrounding the meaning of risk in the GDPR is probably best epitomised by Art. 35 itself. Art. 35(1) does indeed provide 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***.»[3]

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?

Quelle [2015, sec. 2.5] has duly noted this contradiction, and has perfectly summarised the situation, arguing that this might suggest that abidance by data protection principles, and mitigating the risks to the rights and freedoms of natural persons are two distinct things.[4] In which case, one must wonder what is exactly meant by such rights and freedoms and how mitigating the risks that concern them is different from protecting the data subjects' personal data. One can add the following issue: if these are two different things indeed, then what is exactly the role for the rights and freedoms of the data subject, and how is such impact assessment different from the traditional compliance approach?

Such contradiction is also apparent in Art. 35.7 GDPR, which provides for the minimum elements to be contained in a DPIA. It requires «an assessment of the necessity and proportionality of the processing operations in relation to the purposes» (Art. 35.7(b)), which can be seen as a minimal version of an assessment of the impacts on the protection of personal data. Yet it also requires «an assessment of the risks to the rights and freedoms of data subjects» (Art. 35.7(c)).

3. The hypothesis put forth: compliance risk

3.1. Compliance risk: what is it and why it is not so bad?

The hypothesis put forward in this contribution is that the notion of risk which is at the heart of the GDPR is a compliance risk. Thus, instead of determining the chances that a given processing operation will violate the data subjects' fundamental rights and freedoms (and the severity thereof), its point is to determine the chances that a given processing operation will (not) comply with the GDPR (and the severity thereof).

Limiting impact assessment in the data protection field to issues of compliance has been criticised for not enabling the full potential of an impact assessment, and in particular, its ability to address all the privacy issues raised by the processing of data, but also issues of social acceptance and ethical concerns related thereto [e.g., Wright 2012; Wright/Mordini 2012].

However, the present contribution takes a different stance. It argues that limiting the GDPR risk to matter of compliance is not necessarily a bad thing. First, and as will be demonstrated, a compliance risk nonetheless allows to take into account potential violations of the data subjects' fundamental rights and freedoms stemming from processing operations. Second, a compliance risk is the only type of risk that manages to respect the

[3] Emphasis by the author.

[4] Quelle makes this point notably by paying heed to the differences between the respective GDPR proposals of the EU Commission, Parliament, and Council.

rights-based nature of data protection of the EU, and the ensuing need for a thorough and continuous application of its principles.

3.2. Why compliance risk? The debate between risk-based and rights based approaches and the conundrum of risk in the GDPR

This section shows that the GDPR adopted a notion of compliance risk because it needs to be in line with two seemingly opposed notions. On the one hand, the introduction of the risk-based approach in the GDPR and the transformation of data processing operations as a matter of risk management it entails. On the other hand, the need to respect the rights-based nature of data protection as a fundamental right of the EU.

This debate and contradiction has probably been best displayed by the Art. 29 WP in its statement on the risk-based approach in the GDPR.

For the Working Party it is clear that «the risk-based approach is being increasingly and wrongly presented as an alternative to well-established data protection rights and principles» [Art. 29 WP 2014b, p. 2]. It is indeed not acceptable to replace the traditional data protection principles with «a strong harm-based approach» [Art. 29 WP 2014b, pp. 2–3].

In doing so, the Art. 29 WP takes a firm stance and reaffirms the rights-based nature of the EU right to personal data protection. One can argue that the right to the protection of personal data is rights based in parts because it has acquired the status of fundamental right of the EU following the entry into force of the EU Charter of Fundamental Rights [see, González Fuster 2014]. This entails that it applies irrespective of the level of risk, and therefore provides for a «minimum and non-negotiable level of protection for all individuals» (Art. 29 WP 1998, p. 2].

The risk-based approach in the GDPR thus faces a conundrum. On the one hand it is risk-based, meaning that it will provide a level of protection directly dependent upon the level of risk at stake. On the other hand however, it must respect the rights-based nature of data protection as a fundamental right of the EU, which is its exact counterpart insofar as it provides for an even level of protection to all (thus irrespective of the level of risk).

As indicated, the solution to this conundrum is to conceive the notion of risk in the GDPR as a matter of compliance risk. The risk at stake is therefore not the risk that the processing operation will create harms for the data subjects, but the risk that the processing operations of the data controllers are not in compliance with the GDPR. In doing so, both the rights-based nature of the GDPR and the need to adopt a risk-based approach nonetheless are reconciled.

There is evidence that the risk in the GDPR is a compliance risk. This is clear from the Art. 29 WP itself, which argues that «the scalability of legal obligations based on risk addresses compliance mechanisms» [Art. 29 WP 2014b, p. 2]. Additional evidence that the risk-based approach in the GDPR is limited to compliance can also be found in a number of Recitals (see e.g., Recitals 78, 80, 81, 82, 84).[5]

3.3. How to articulate a compliance risk with the assessment of the risk to the rights and freedoms of the data subjects?

The rationale for a risk limited to compliance has been explained. Yet, it remains to be seen what is in practice the added value of such type of risk. Can it nonetheless allow for the taking into account of the whole spectrum of the data subject's fundamental rights that are potentially affected by the processing of their personal data? The present section will show that even though it is limited to compliance, this risk can nonetheless allow for

[5] Recital 84 in particular provides that «In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk.»

the taking into account of the different rights and freedoms affected by a processing operation. This requires an in-depth analysis of the notion of risk.

A risk can be defined as an event that has a certain severity, has a number of probabilities of occurrence, as well as a number of consequences.[6] The whole point of risk management (or risk analysis) is to take decisions concerning risk, i.e., whether or not to take the risk at stake.

Risk analysis is usually divided into 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 [Warner 1992, p. 5]. 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 [ISO 2009, p. 6].

The key in understanding the articulation between compliance issues and the violation of the data subjects' broader spectrum of fundamental rights can be found in the risk management step.

It is indeed widely accepted that the decision of whether or not to take a risk takes the form of a cost-benefit analysis,[7] that is, a balancing of the consequences of the risk, which can be positive or negative. Negative consequences are referred to as harms, whereas positive consequences are referred to as benefits [see, e.g., de Sadeleer 2014, p. 91].

In the present case it is argued that the negative consequences of the non-compliance risk precisely consist in the violation of the data subject's fundamental rights and freedoms.

In other words, not-complying with data protection law has a number of negative consequences, which amount to the violation of the data subjects' fundamental rights and freedoms. It is precisely these violations that the data controller will need to take into account when deciding whether or not to pursue a processing operation.

This actually makes a lot of sense. For instance, not minimising the data may result with violations of the data subject's fundamental rights. The same goes true if the data are processed for further incompatible purposes. As a matter of fact, in its opinion on the purpose limitation principle, the Art. 29 WP has made the link between the violation of said principle and the harms to the data subjects this may lead to [Art. 29 WP 2013, 2014a]. Thus, the lower the compliance, the higher the potential violations of the data subjects fundamental rights.

4. Conclusion: what protection to be expected from the risk-based approach?

As a way of concluding this piece, one may ask what exact type of protection the GDPR risk-based approach will achieve, and in particular, what is the role of the data subjects' rights and freedoms in this regard.

The bottom line is that compliance is transformed into a matter of risk taking. Contrary to the traditional understanding of compliance, which frames it as a matter of «yes or no», i.e., «complying or not complying», the risk-based approach shows that in practice compliance is more granular than it seems to admit.

As indicated, a risk has a certain level, which is measured in terms of likelihood (or probability) and severity. This is explicit in the GDPR (e.g., Recitals 75, 90).[8] Such likelihood and severity is measured by having regard to so-called risk factors.[9] In terms of risk factors for the probability one can take the example of the CNIL's 2012 methodology, which takes the case of employee training: the less trained the employees, the higher the

[6] See for instance Bernstein 1996, p. 100: «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 lost, by the decision».

[7] See Hood et al. 1992, p. 137: ‹‹risk management› has been commonly used to refer to an analytic technique for evaluating risks against likely benefits».

[8] See Recital 90: «a data protection impact assessment should be carried out by the controller in order to assess the particular likelihood and severity of the high risk».

[9] The CNIL refers to risk factors as threats [CNIL 2012b, p. 6], and the ISO defines them as «elements, which, alone or in combination has the intrinsic potential to give rise to risk» [ISO 2009, p. 4].

likelihood that non-compliance will occur [CNIL 2012b]. In terms of risk factors for the severity, many can actually be found in the GDPR, which refers to the context, scope, purposes of the processing (e.g., Recital 90); or the extent of the processing, the type of data at stake, and or the type of processing, as in the case of Art. 35.3 which refers to «a systematic and extensive evaluation of personal aspects relating to natural persons» (Art. 35.3(a)); or to the «processing on a large scale of special categories of data» (Art. 35.3(a)) among others.

Underscoring the granular dimension of compliance and transforming it as a matter of risk-taking is in line with the role and added value of the risk-based approach as it was envisaged in early documents laying the ground for the adoption of the GDPR. These documents underlined indeed the need for «real protection on the ground», as opposed to compliance understood as protection on paper, which is often reduced to box-ticking exercises [Art. 29 WP 2010; Art. 29 WP/Working Party on Police and Justice 2009]. By inquiring which concrete risk factors lead to higher levels of compliance risks, this is exactly what the present risk-based approach does. Similarly, it provides for the calibration of the data controller's obligation, allowing them to allocate resources where they are more needed. Hence, the Art. 29 WP's notion of scalable approach to compliance discussed *supra*.

One may however ask what is the role of the data subjects' rights and freedoms in all this. The answer put forth in the present contribution is that addressing the potential violations of the data subjects' rights and freedoms contribute to the compliance of the data processing operations. In this sense, they are an integral part of the «protection on the ground» aspect of the risk-based approach, since they contribute to determining «in practice» what it means to be compliant.

Indeed, just as a low level of compliance signals the likely infringement of the data subject's rights and freedoms, ensuring in turn that the rights and freedoms are not violated by the processing operation contributes to higher levels of compliance. As a matter of fact, this is exactly the approach followed by the CNIL in its 2012 guidance document [see, CNIL 2012a].

Thus, and as a way to conclude one can indeed see that the GDPR has enshrined a notion of compliance risk. Such compliance risk manages to reconcile both the rights-based dimension of the EU fundamental right to the protection of personal data as well as the fact that data controllers are now explicitly tasked with managing the risks created by their processing operations.[10] The potential violations of the data subjects' rights and freedoms stemming from processing activities can be factored in such compliance risk by bearing in mind that they are the consequences of low levels of compliance. In doing so, compliance risk ensures that in conformity with the rights-based approach the data protection principles remain upheld in all situations, and simultaneously allows for the taking into account of the broader dimension of data processing activities.

5. Bibliography

Art. 29 WP, Opinion 1/98 Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS), 1998.

Art. 29 WP, Opinion 3/2010 on the principle of accountability, 2010.

Art. 29 WP, Opinion 03/2013 on purpose limitation, 2013.

Art. 29 WP, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 2014a.

Art. 29 WP, Statement on the role of a risk-based approach in data protection legal frameworks, 2014b.

Art. 29 WP/Working Party on Police and Justice, The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to the protection of personal data, 2009.

Bernstein, P. L., Against The Gods – The Remarkable Story of Risk. New York: John Wiley & Sons, Inc 1996.

[10] This is for example very clear with Art. 24.1 enshrining the accountability principle, and which provides that data controllers should take into account «the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons».

CNIL, Measures For The Pirvacy Risk Treatment, 2012a.

CNIL, Methodology For Privacy Risk Management: How to implement the Data Protection Act, 2012b.

de Sadeleer, N., EU Environmental Law and the Internal Market. Oxford: Oxford University Press 2014.

Gellert, R., We Have Always Managed Risks in Data Protection Law: European Data Protection Law Review 2016, 4(2), pp. 481–492.

González Fuster, G., The Emergence of Personal Data Protection as a Fundamental Right of the EU. Dordrecht: Springer 2014.

Hood, C. et al., Risk Management, in: The Royal Society (ed.), Risk: Analysis, Perception and Management – A Report of a Royal Society Study Group, London: The Royal Society 1992, pp. 135–201.

ISO, ISO: 31000 Risk management – Principles and guidelines, 2009.

Quelle, C., The data protection impact assessment: What can it contribute to data protection?, 2015.

Warner, F., Introduction, in: The Royal Society (ed.), Risk: Analysis, Perception and Management – A Report of a Royal Society Study Group, London: The Royal Society 1992, pp. 1–12.

Wright, D., The state of the art in privacy impact assessment. Computer Law & Security Review 2012, 28(1), pp. 54–61. http://doi.org/10.1016/j.clsr.2011.11.007.

Wright, D./Mordini, E., Privacy and Ethical Impact Assessment, in Wright, D./De Hert, P. (eds.), Privacy Impact Assessment, Dordrecht, Heidelberg, London, New York: Springer 2012, pp. 397–417.