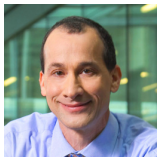
Risk and high risk: Walking the GDPR tightrope



Paul Schwartz

Privacy Perspectives | Mar 29, 2016

One of the most important developments in privacy and security law over the last decade has been the increased focus on risk as a touchstone for regulation. The "risk principle" is the idea that organizations that process and use personal data should devote more resources to the activities that raise the most significant threats, and that the law should promote a nuanced approach rather than imposing one-size-fits-all regulation.

The EU's General Data Protection Regulation adopts the risk principle, but takes two different approaches to the concept. First, the GDPR sees risk as a continuum and expects companies to do more as their data processing poses increased possibilities of harm. Second, it divides risk into a category with two steps, "risk" and "high risk." This distinction is highly significant because the "high risk" level triggers distinct obligations. As a result, the identification of the amount of risk and the question of whether the "high risk" category is reached are matters of crucial importance.

A further issue is present, moreover, for American companies seeking to comply with the GDPR. Transatlantic concepts of privacy harms are frequently different. If these two legal systems have separate approaches to this issue, there is a great potential for differing assessments of the significance of

the given threat. As a result, U.S. companies face uncertainty in judging the risks of their data processing and whether it qualifies as a risk or a high risk.

Category one: Risk-as-continuum

Like the Directive, the GDPR requires a legal basis for any processing of personal data. To a far greater extent than the Directive, however, the GDPR seeks to tailor its legal obligations to the risk that the data processing poses. The Directive makes only sparing use of the risk concept and does so for its security requirements. Article 17 requires "appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access." The Directive's requirement of data security is to "ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."

The GDPR goes further; the risk principle is one of its cornerstones. In particular, Article 22 calls for data controllers to assess "the risks of varying likelihood and severity for the rights and freedom of individuals." Following this assessment, controllers are to implement "technical and organizational measures" commensurate to the identified threat.

Data protection by design, which Article 23 sets out, also reflects the risk principle. The relevant language regarding the building-in of privacy is parallel to that found in Article 22; in both sections, the focus is on different kinds of risks and their impact on "rights and freedom."

In another use of the risk principle, the GDPR views it as functioning as part of an off-on switch for the GDPR's recordkeeping duty. Specifically, Article 28 frees an enterprise or organization with fewer than 250 employees from an obligation to maintain records regarding data processing when such activities are not likely to result in "a risk for the rights and freedom" of the individual. Thus, risk in this context provides a threshold below which a small company need not maintain records of data processing.

Finally, like the Directive, the GDPR uses risk to organize its security principle. Article 30 calls for "appropriate technical and organisational measures, to ensure a level of security appropriate to the risk." Article 30(1a) calls for heightened attention to a special group of security risks; these are ones that flow from "accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

In sum, these examples show that the GDPR generally conceives risk as a quality that increases sequentially. A company must respond to risk with commensurate technical and organizational measures. In addition, the GDPR uses the risk principle in its requirements for data protection by design, recordkeeping, and security.

Category two: Risk-as-disjunctive

In contrast to a threat model based on a continuum, the GDPR sometimes views risk as falling into two mutually exclusive categories: risk or high risk. Here is risk as a disjunctive: data processing activities fall into one category or the other. The recordkeeping requirement, discussed above, suggests there is a "low-risk" or "no-risk" category as well. The risk versus high-risk distinction matters, however, because once a threat falls into the high-risk category, the GDPR imposes new requirements on the organization that processes personal data.

The high-risk category was absent from the Commission's original proposal of January 25, 2012. The European Parliament's amendments of March 12, 2014, introduced these terms at two junctures, none of which survived subsequent negotiations. In its draft of June 11, 2015, the Council made copious use of the high-risk concept and played a great influence on the fashion in which the GDPR adopted the concept. As a

consequence, the Council is responsible for the important future role of this this idea in EU data protection law.

The leading example of an obligation triggered by high-risk concerns data breach notification. The GDPR generally requires that controllers notify the responsible supervisory authority within 72 hours of a data breach. In cases of high-risk data breaches, there is an additional obligation. Where such a threat exists to "the rights and freedoms" of individuals, the controller must disclose the personal data breach to the data subject. Such notifications must be made "without undue delay" and provide relevant details in clear language about the nature of the breach.

Another instance of a special obligation concerns the "data protection impact assessment." Here is an attempt to replace the Directive's heavier hand with regulatory flexibility. The Directive contains a general obligation for controllers to notify member state's supervisory authorities of personal data processing. To justify its new approach, the GDPR engages in a bit of data protection self-criticism. It notes in Recital 70 that the Directive's "indiscriminate general notification obligations" failed to "contribute to improving the protection of personal data" in all instances.

In place of the old regime of general notification of processing, the GDPR has a more limited obligation, which is developed through its data protection impact assessment. A controller is now required to seek formal advice from the responsible supervisory authority, but only before processing personal data in high risk cases. The impact assessment requires a consultation between the controller and the supervisory authority. Within eight weeks, the supervisory authority is to decide whether or not the processing is in compliance with the GDPR.

What constitutes risk or high risk?

Thus, the GDPR contains two different approaches to risk. Both approaches require organizations to assess the extent of the threat that different processing operations raise to "rights and freedoms." Three points should be made regarding the required assessments.

First, the GDPR provides general guidelines and broad suggestions regarding its approach to risk and high risk alike. For example, Recital 70 states that high risks follow from data processing that use "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." More generally, the GDPR observes in Recital 60(b): "Risk should be evaluated based on an objective assessment, by which it is established whether data processing operations involve a risk or a high risk."

Second, the GDPR provides a process-oriented approach to risk and high risk. As part of its focus on procedures, it enumerates steps to be taken, including the necessary consultations. The resulting process is highly diffuse. It requires development of guidelines, best practices, and the building of categories of risk threats. As an example, Recital 60(c) addresses the need for "guidance for the implementation of appropriate measures, and for demonstrating the compliance by the controller or processor, especially as regards the identification of the risk … and the identification of best practices to mitigate the risk." Guidance can come from approved codes of conduct, approved certifications, and guidelines from the European Data Protection Board.

Regarding the data protection impact assessment and data breach notification, here too, there is attention to required procedures; many of these will be developed by EU governmental agencies and authorities once the GDPR is finally enacted. These guidelines will require years to finalize, which will lead to a period of uncertainty for companies. For example, the supervisory authority is to develop a public list of the kinds of processing operations for which the controller must carry out data protection impact assessments. Different supervisory authorities may incorporate different elements on these lists. The GDPR also requires the European Data Protection Board to issue "guidelines, recommendations and best practices" concerning the

types of personal data breaches that create high risk (Art. 66 subs. 1 [b], [c]). The extent to which a data controller or processor complies with these procedures will be an important factor for the supervisory authority when assessing fines for violations of the GDPR (Article 79, subs. 2a [d], [j]).

Third, the U.S. and EU differ fundamentally in how they assess privacy risks. U.S. law has long struggled in its approach to privacy harms. U.S. courts have grappled, for example, with whether a data breach leading to a risk of identity theft provides adequate standing for a lawsuit. In the EU, by contrast, there is a firm and well-developed law regarding privacy harms. With the establishment of the European Union Charter of Human Rights, moreover, data protection is now a legally guaranteed fundamental interest in the EU.

The result is a considerable challenge for U.S. companies that fall under the GDPR's jurisdiction. These entities must learn to view risk and high risk alike through an EU perspective. The high fines the GDPR permits, make the assessment of risk and compliance with EU-mandated procedures all the more imperative.

photo credit: Piccadilly Circus Circus via photopin (license)

Written By

Paul Schwartz

https://iapp.org/news/a/risk-and-high-risk-walking-the-gdpr-tightrope/