The Risk-Based Approach in the GDPR: Interpretation and Implications

By Gabriel Maldoff, CIPP/US, IAPP Westin Fellow

iapp

The Risk-Based Approach in the GDPR: Interpretation and Implications

By Gabriel Maldoff, CIPP/US, IAPP Westin Fellow

Europe's new General Data Protection Regulation, which will come into effect in the spring of 2018, embraces a risk-based approach to data protection. Throughout the GDPR, organizations that control the processing of personal data (known as "controllers") are encouraged to implement protective measures corresponding to the level of risk of their data processing activities.

High risk. The GDPR imposes heightened requirements on controllers that engage in "high-risk" activities. Specifically, before engaging in such an activity, an organization may be required to consult with a data protection authority and conduct a detailed privacy impact assessment. In the case of a data breach, it may be required to notify potentially affected individuals.

Risk. For activities that are not labelled "high risk," controllers still must adopt measures that are appropriate to the risk level of the activity. For example, controllers are required to "ensure a level of data security appropriate to the risk" and implement risk-based measures for ensuring compliance with the GDPR's general obligations.

Low risk. Where the risk to data subjects is minimal, a controller may be exempt from the requirement to notify authorities of a data breach and a foreign controller may be relieved from the requirement to appoint a representative in the EU.

Although the GDPR is silent on how organizations should assess and quantify risk, certain trends emerge from the sections where risk does appear that will guide organizations in implementing a risk based approach.

Heightened obligations for "high-risk" processing

The GDPR introduces stricter requirements for high-risk processing. Controllers that engage in processing that poses a high risk for data subjects face three additional obligations.

First, **Article 33** requires controllers to conduct a data protection impact assessment for high-risk processing activities. These are processing activities that rely on new technologies and are "likely to result in a high risk for the rights and freedoms of individuals." Three examples of high-risk activities are provided, including (1) "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 individual or similarly significantly affect the individual," (2) "processing on a large scale of special categories of data," and (3) "a systematic monitoring of a publicly accessible area on a large scale." The supervisory authority in each member state may promulgate a list of other processing activities that require data protection impact assessments as well as activities that are specifically exempt from the requirement.

Second, where a controller conducts a risk assessment and concludes that the activity may result in a high risk, **Article 34** requires the controller to consult the relevant supervisory authority before conducting the activity. The controller will be exempt from this requirement, however, if it takes measures to mitigate the risk. If the supervisory authority finds that the risk is unjustified, such as "where the controller has insufficiently identified or mitigated the risk," it is empowered to block the processing activity.

Finally, under **Article 32**, controllers are required to notify individuals *in addition* to the competent authorities of a security incident if "the personal data breach is likely to result in a high risk" to their rights and freedoms. A controller that engages in high-risk processing may avoid the individual notification requirement if (1) it "has implemented appropriate technical and organisational protection measures" (e.g. encryption), (2) the high risk "is no longer likely to materialize," or (3) notifying the affected individuals "would involve disproportionate effort."

GDPR encourages risk-based compliance

The concept of risk analysis most notably appears in the measures controllers should implement to assure adequate data security. However, controllers also are required to take risk into account as part of their "general obligations." Although not explicitly stated, risk-analysis concepts underlie the criteria set forth for authorities when assessing penalties to controllers for non-compliance. Thus, risk analysis may extend beyond the data security provisions, encouraging a risk-based compliance approach to many areas of the Regulation.

Processing with High Risk

Activities	Additional Obligations	Exemptions
• Systematic and extensive automated profiling • Large-scale processing of special categories of data • Large-scale, systematic monitoring of a publicly accessible area • Other activities that are "likely to result in a high risk for the rights and freedoms of individuals" • Member state law	Privacy impact assessments	Member state law exempts specific activities
	Prior consultation with DPA	Controller implements appropriate technical and organizational measures to mitigate the risk
	Notification of data breach to individuals	• Controller implements appropriate technical and organizational measures (e.g. encryption) • The high risk is no longer likely to materialize • Notifying affected individuals would involve disproportionate effort

Explicit risk-based measures

Similar to the Data Protection Directive 95/46/EC, **Article 30** of the GDPR requires controllers to "ensure a level of security appropriate to the risk." Controllers can comply with this requirement by implementing "technical and organisational measures" that mitigate the risk. These measures include pseudonymization and encryption as well as an ability to restore access to data if there is a security incident and "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing." One new way controllers can demonstrate compliance is by adhering to approved codes of conduct or certifications.

Unlike under the Directive, however, the GDPR introduces breach notification requirements. In the event of a data breach, **Article 31** specifies that controllers must notify the competent authorities "unless the personal data breach is *unlikely to result in a risk* for the rights and freedoms of individuals" (emphasis added).

The GDPR also extends the concept of risk to other areas. In Chapter IV, Section 1, devoted to "general obligations," **Article 22** instructs controllers to "implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation." These measures should reflect "the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of individuals."

Article 23, which sets out the principles of data protection by design and by default, requires controllers to implement privacy protective measures at the design stage of a product and ensure that, where users can select among different settings options, privacy-protective settings are the default. These measures, too, should reflect the risk and context of the controller's processing activities, as well as the available technology and cost of implementation. Controllers may adopt codes of conduct or approved certifications to meet the controller's general obligations, but only certifications may be used to meet the data protection by design requirement.

Controllers that are not based in the EU may be required to designate a representative in the EU if they process the data of EU residents. **Article 25** exempts controllers from this obligation if the processing is occasional, does not include the large-scale processing of "special categories of data," and is "unlikely to result in a risk for the rights and freedoms of individuals, taking into account the nature, context, scope and purposes of processing." Special categories of data are sensitive data that reveal racial or ethnic origin, political or religious beliefs, as well as genetic, biometric and health data.

Risk-based approach to compliance

Article 79 sets out the factors authorities must consider when imposing penalties for violations of the GDPR. In all circumstances, the remedy should be "effective, proportionate and dissuasive." When deciding whether to impose a fine and in what amount, the supervisory authority must consider "the degree of responsibility of the controller or processor having regard to technical and organisational measures implemented pursuant to Articles 23 and 30." Recall that these articles outline the data protection by design and data security requirements, which require controllers to tailor protective measures to the risk of a processing activity.

Additionally, the supervisory authority must consider "the nature, gravity and duration of the infringement having regard to the nature, scope or purpose of processing" as well as "the intentional or negligent character of the infringement." Controllers can reduce their exposure to penalties by demonstrating their adherence to approved codes of conduct or certification mechanisms. Taken together, these factors suggest that fines should be imposed in accordance with the risk profile of the operation and the extent to which the controller appropriately addressed the risk. It follows that a controller may face reduced fines or avoid fines altogether by addressing the risk of its activities, even if such measures fail to prevent a data breach.

Even where there is no data breach, risk-based compliance may provide a defense to violations of other provisions of the GDPR. Recital 60a instructs controllers to take into account the risk that "data subjects might be deprived of their rights and freedoms or from exercising control over their personal data." Since the GDPR's provisions on consent for processing and data subject rights are designed to "strengthen the control over their own data," the risk-based approach may similarly apply to consent and data subject rights provisions. Thus, a controller that fails to obtain consent or fails to provide a data subject access to her personal data may escape liability if it implemented procedures for appropriately addressing the risk of such events. For example, if a controller processes a child's personal data without parental consent, the controller might argue that it should not be held liable because it had in place systems to mitigate the risk that a child would try to evade the parental consent requirement.

Processing with Risk

Activities	Additional Obligations	Exemptions
Examples • Data subjects deprived of control • Processing sensitive data • Profiling • Vulnerable individuals • Large-scale processing Potential Harms • Discrimination • Identity theft or fraud • Financial loss • Damage to the reputation • Loss of confidentiality • Reversal of pseudonymization • Significant economic or social disadvantage	Notification of data breach to DPA	Data breach is "unlikely to result in a risk for the rights and freedoms of individuals"
	Foreign controllers appoint EU representative	Processing is occasional, does not include large-scale processing of sensitive data, *and* is "unlikely to result in a risk for the rights and freedoms of individuals."
	Data security: Controllers must implement (and choose processors that implement) "technical and organizational measures" appropriate to the risk of a data breach	Controller processes only "anonymous data" not subject to regulation
	Risk-based compliance with GDPR's "general obligations"	Controller processes only "anonymous data" not subject to regulation

Deconstructing “risk”

Risk analysis is contextual. Where the concept of risk appears in the GDPR, it is defined by reference to the “likelihood and severity” of a negative impact on data subject rights. Controllers should account for “the nature, scope, context and purposes of the processing.” When conducting a risk analysis, the French data protection authority, CNIL, has advised controllers to first identify the potential harm associated with a processing activity. Next, controllers should evaluate the severity of harm that could result. Finally, controllers should assess the likelihood of the event by analyzing the vulnerabilities of their systems and operations as well as the nature of the threats.

Potential harm under the GDPR

Recital 60a provides insight into the nature of the harms that the GDPR seeks to avoid. The GDPR defines harm as “physical, material or moral damage.” It is particularly concerned with processing activities that could lead to “discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy, unauthorized reversal of pseudonymization, or any other significant economic or social disadvantage.”

Assessing an activity’s risk level

Although the recital does not speak directly to the relative severity of each type of harm, Article 33 provides three examples of high-risk activities: (1) “systematic and extensive” automated profiling that “significantly affects” individuals, (2) large-scale processing of special categories of data, and (3) large-scale, “systematic monitoring of a publicly accessible area.” These “high-risk” activities provide insight into the types of harm that may be considered especially severe under the GDPR. First, where many individuals are affected, the harm is more likely to be severe. Second, the GDPR is especially concerned with processing activities that could lead to discrimination as well as economic or social disadvantage. Finally, financial loss is not singled out and may in fact be considered a less significant harm than events that reveal intimate and personal details about individuals.

Recital 60a identifies other activities that also pose a risk – although perhaps a lower risk – to data subjects. These are processing activities “where data subjects might be deprived of their rights and freedoms or 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 or data concerning health or sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or prediction of 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 individuals, in particular of children, are processed; where processing involves a large amount of personal data and affects a large number of data subjects.”

It is important to note that these risky activities are not exclusive. Supervisory authorities in the member states and the European Data Protection Board will have the power to identify other activities that are either likely or unlikely to result in a “high risk” for the rights and freedoms of data subjects. The EDPB may also issue guidance on the measures controllers can take to address risky processing activities.

Conclusion

The GDPR embraces a risk-based framework that encourages controllers to engage in risk analysis and to adopt risk-measured responses. The GDPR imposes additional obligations for data processing activities that pose a high risk to individuals, while requiring controllers to account for risk in complying with many provisions of the Regulation.

Controllers that engage in low-risk processing activities, or that adequately address risk, may avoid specific requirements to notify a data protection authority of a data breach and, for foreign controllers, to appoint a representative in the EU. The GDPR also requires the supervisory authorities to consider the risk level of the activity when deciding whether to impose fines for a purported violation.

Risk is not clearly defined but the recitals provide examples of harms and instruct controllers to assess the probability of such harms in light of the nature of the threat. Activities that involve large-scale processing and automated evaluation of the personal characteristics of data subjects are more likely to be considered high risk.