Spring 2020

ihl

The In-House Lawyer

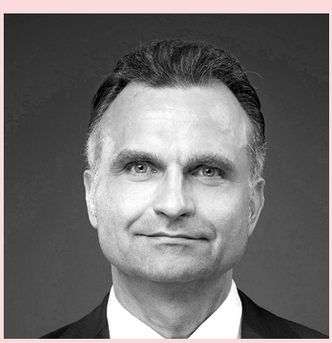
BRAND AND REPUTATION MANAGEMENT • CYBERSECURITY • INSURANCE • COVID-19 RESPONSE

Eye of the storm

Insurance GCs brace for impact amid global crisis

The risk-based approach under the GDPR and Swiss data protection laws

Clara-Ann Gordon, partner and Dr. András Gurovits, partner, Niederer Kraft Frey



Clara-Ann Gordon
Partner, Niederer Kraft Frey
clara-ann.gordon@nkf.ch

Dr. András Gurovits
Partner, Niederer Kraft Frey
andras.gurovits@nkf.ch

The General Data Protection Regulation (GDPR) and the Revised Swiss Data Protection Act (revised FADP) embrace a risk-based approach to data protection. Organisations that control the processing of personal data (controllers) are encouraged to implement protective measures corresponding to the level of risk of their data processing activities.

Direct applicability of the GDPR to Swiss companies

Due to the so-called 'marketplace principle' Swiss companies with a branch in the EU are subject to the GDPR when processing their data. In addition, Swiss companies that offer goods and services to data subjects in the EU are also subject to the provisions of the GDPR, if they process their data in this context. The same applies to those data processors who observe the behaviour of persons in the EU, for example by using cookies.

Revision of FADP – alignment with the provisions of the GDPR

As a non-EU country, Switzerland enjoys great sovereignty in the revision of its data protection legislation and would not have to implement the provisions of the GDPR. With regard to the significance of the effects of the GDPR on Switzerland, the 'adequacy decision' of the EU Commission is of primary importance. If the revised FADP were not regarded as 'adequate' in comparison with the EU, today's simple cross-border data traffic would be endangered. Also from the point of view of the Swiss economy, an adaptation to the GDPR is necessary. Under the marketplace principle, GDPR is directly applicable to many Swiss companies and accordingly the FADP should therefore be designed analogously to the GDPR in order to avoid duplication.

Need for action on the part of Swiss companies and controllers

Swiss companies or controllers must comply with both the GDPR and the FADP. If these new regulations are not complied with, very high fines may be imposed. Under the GDPR this is known to be 4% of global turnover or €20m, whichever is higher, or 2% of global turnover or €10m for minor infringements, whichever is higher. Under the revised FADP fines are lower at CHF 250,000, but they are imposed on the private individual and not on the company.

Broad list of duties – is compliance possible at all?

The GDPR and the revised FADP contain a broad catalogue of obligations for controllers which must be fulfilled. In view of the wealth of these new obligations, many companies are wondering whether they can fulfil them at all.

In order to cushion this somewhat, the GDPR and also the revised FADP have introduced the risk-based approach, which is intended to provide

> **The GDPR and the revised FADP contain a broad catalogue of obligations for controllers which must be fulfilled. Many companies are wondering whether they can fulfil them at all.**

the controller with a certain degree of relief and leeway for implementation.

Differentiation of the controller's obligations

In view of the very broad scope of application of the GDPR and the very far-reaching measures which the controller has to take, the risk-based approach is intended to achieve a differentiation of the controller's obligations. This is based on the idea that the data protection instruments should only be used depending on the risk that the data processing poses to the data subject in each individual case in order to establish a reasonable cost-benefit ratio. With structured risk assessments, complexity can be made manageable and weighing decisions can be made in a comprehensible manner.

What are the risk areas?

Pursuant to Article 24 in conjunction with Article 32 GDPR, the severity of the risk to the rights and freedoms of the data subjects must be taken into account when selecting technical and organisational measures. Furthermore, according to Article 33 GDPR, the question of whether the controller must submit a report to the supervisory authority in the event of a breach of data protection is decisive as to whether the breach leads to a risk for the rights and freedoms of the data subjects. The GDPR also orders the implementation of certain special measures in the event of a 'presumably high risk' for the personal rights and freedoms of data subjects. Examples include the data protection impact assessment pursuant to Article 35 GDPR and the notification of data subjects in the event of data protection violations pursuant to Article 34 GDPR.

According to Recital 75, possible data protection risks that result from data processing and can lead to physical, material or immaterial damage are, for example: discrimination, identity theft or financial loss. Examples of high-risk processing operations are given in Recital 89, including processing operations using new technologies and novel processing operations that have not previously been subject to a data protection impact assessment.

How is the risk-based approach applied in practice?

The risk-based approach in the GDPR leads to the following requirements for the controller:

- Identification of risks associated with processing.
- Risk analysis taking into account the probability of occurrence and the severity of the consequences.
- Classification of whether the risk is low or high.
- Risk treatment through appropriate measures.

Risk-based approach in the revised FADP?

The revised FADP does not contain a definition of the term 'risk-based approach'. The white paper to the revised FADP sets out in various sections what 'risk-based approach' means: 'The risk associated with processing must be related to the technical possibilities to reduce it. The higher the risk, the greater the probability of occurrence and the more extensive the data processing, the higher the requirements on the technical precautions have to be, so that they can be considered appropriate'.

Conclusion: risk analysis and risk-measured responses

The GDPR and the revised FADP embrace a risk-based framework that encourages controllers to engage in risk analysis and to adopt risk-measured responses. 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. ■