February 1st, 2024

Finnish Energy's feedback for the report on General Data Protection Regulation

Finnish Energy represents approximately 290 companies that produce, acquire, transmit and sell electricity, district heating and cooling, and offer related services. Finnish Energy appreciates the opportunity to provide feedback on the application of the General Data Protection Regulation (GDPR).

In general terms, the benefits of the GDPR related to the harmonization of personal data protection across the EU area and cooperation among authorities are supported. However, it has been observed that there are relatively significant differences in the application and level of the regulation in different member states. Additionally, in cross-border situations, it has sometimes been unclear how the GDPR is applied simultaneously with the specific regulations of different countries (e.g., marketing or consumer protection regulations).

The most significant challenges in the application of the GDPR involve interpreting numerous provisions perceived as unclear and implementing detailed obligations at the company level. The regulation's text is so open to interpretation that its application is considered difficult, and ensuring the correctness of practices is still associated with significant legal uncertainty. Additionally, there are challenges related to guidance, which will be represented further below.

Guidance provided by EDPB and DPAs

Finnish Energy considers the guidelines provided by the European Data Protection Board (EDPB) useful in providing direction for application, and they somewhat facilitate the practical implementation of the regulation. However, Finnish Energy's view is that many existing guidelines have been perceived as too open to interpretation and general, thus not adequately assisting companies in the practical application of the provisions and decision-making.

Finnish Energy sees it is beneficial that the EDBP has provided practical examples in the guidelines. However, the current examples often do not provide suitable examples for real-life situations encountered by businesses. Despite the existing guidance, there are still uncertainties in certain areas, particularly regarding the assessment of the risk to the rights and freedoms of natural persons in the event of personal data breaches, i.e., whether a data breach should be reported or not. In addition, more clarification and detailed examples have been requested regarding Article 30 'Records of processing activities,' especially concerning the level at which the information mentioned in the article should be provided.

Furthermore, the regulatory guidance in national level related to the GDPR has not been deemed sufficient. Finnish Energy believes that there should be provided more concrete guidance from DPA to companies to ensure compliance with the regulation in the future as well.

International transfers and third countries

One area of uncertainty concerns the level of responsibility held by data controllers for the entire subcontracting chain's data transfers and how the assessment of the entire subcontracting chain should be practically verified, for instance, in impact assessments. Data controllers often find it quite challenging to assess the contractual relationships between their subcontractors and the subcontractors further down the chain, as well as to obtain information about the associated risks. Situations where personal data is transferred to third countries as part of international business operations are also perceived as challenging.

Many of the mechanisms required by the GDPR are seen as laborious within companies and involve a lot of uncertainties. Among these mechanisms, conducting Data Protection Impact Assessments (DPIAs) is particularly challenging and burdensome for companies in practice. For example, analyzing the legislation of the destination country requires resources that few companies have available.

It has been highlighted that it is not clear when a third-country company is required to comply with the GDPR and when it is not, as companies that do not comply with the regulation are not required to disclose this information. As a practical example, a subcontractor operating outside the EU, who would normally process personal data, may become bound by the GDPR through contracts. The same subcontractor operating outside the EU may offer its services (e.g., IT support) only to a company but request feedback from the company's employees about the service provided, acting in the role of a "controller". In this specific example, it is unclear under the regulation whether the GDPR should be applicable according to Article 3(2b), as the service is not directly offered to the employees.

General provisions and principles (Chapters I & II)

Several definitions according to Article 4 of the GDPR are considered unclear and difficult to interpret in practical application situations. For example, the concept of ‘health data’ is unclear, and there are differing interpretations among authorities regarding whether information about a person's sick leave constitutes health data.

The division of roles into data controllers and processors in Articles 4(7) and 4(8) of the regulation is perceived as straightforward, and the definitions are considered too abstract and general in relation to real-world application. In the practical business environment, data processors often also act as data controllers. This is evident, for example, in collecting feedback or log data and in product development.

Article 4(23) concerning cross-border processing discusses the activities of establishment of the data controller, although in practice, multinational corporations often have separate legal entities operating in different countries, which act both as data controllers and participate in the same processing activities (e.g., corporate HR systems). While a data controller is usually a single legal entity, in these situations, there are many legal entities involved. It is unclear whether cross-border processing also applies to these scenarios.

The burden of proof requirement included in Article 5(2) is quite heavy, and based on the text of the regulation, it is challenging to ascertain when the burden of proof has been fulfilled to a sufficient level. Finnish Energy sees that it would be important to receive guidance from the authorities on what constitutes the minimum level.

Furthermore, the legitimate interest as a legal basis according to Article 5(1f) has been found difficult to comprehend. Concerning legal bases for processing, it has also been unclear whether Article 6(1b) permits the use of a contract as the basis for processing personal data also in B2B situations. Based on the wording of the article, it can be interpreted that a contract may be used as a legal basis for processing only when the data subject is a party to the contract. However, in practice, processing personal data may be necessary to fulfill a contract even in B2B situations where the contract is with a company.

Rights of the data subject (Chapter III)

Businesses have found it unclear how and in what practical situations the notification obligation under Article 19 regarding the rectification or erasure of personal data, or the restriction of processing, should be applied.

Regarding the right to object under Article 21, concrete examples of what constitutes a 'reason relating to their particular situation' have been requested. This definition is open to interpretation, and it is also unclear how the collection of such information works in terms of the principle of data minimization. While the wording appears to be rooted in the context of search engines, its application has been challenging in other practical situations, such as human resources management. Finnish Energy see there is a need for clarification or guidance from the authorities, especially regarding the scope of the right to object, particularly concerning the 'reason relating to their particular situation.'

Controller and processor (Chapter IV)

Interpreting joint controllership under Article 26 has posed various challenges for businesses, especially for group companies. For group companies that share a common customer data system it is unclear, for example, when group companies should be considered independent separate joint controllers as opposed to joint controllers with regard to the personal data they process. Additionally, there is ambiguity regarding whether two controllers can process the same personal data without being joint controllers. Clarity is needed regarding when it is a transfer between controllers instead of joint controllership.

The data controller's responsibility could be seen overemphasized compared to the data processor, especially when the data processor is a market leader or provides platform services. The challenge arises from the fact that data processors often wield significant power in processing personal data compared to the data controller, even though the data controller has a greater responsibility for compliance with the GDPR. Data processors can significantly influence the implementation of data protection in services, as they often do not customize data protection features for each customer separately. For instance, some data processors' services often include ready-made solutions for fulfilling the obligations of the data controller, which, on one hand, assists the data controller but, on the other hand, gives disproportionate decision-making power to the processor while the responsibility remains with the data controller. For example, the terms of processing agreements and practices for implementing data subject information, obtaining consent, or retention periods may largely be dictated by data processors in a strong market position according to their own format.