Public Consultation

Comments to the guidelines 07/2020 on the concepts of controller and processor in the GDPR

Swedish Trade Federation

Swedish Trade Federation is a trade and retail organization that represent 9,000 small, medium and large companies with approximately 300,000 employees. Below you will find our contribution to the consultation.

Standardized services

As set forth in paragraph 38, when determining the means, a distinction can be made between essential and non-essential means where "essential means" are closely linked to the purpose and the scope of the processing and are traditionally and inherently reserved to the controller. In many cases, IT and online services are standardized services where the essential means are already predefined. In addition, alterations to the services are either not possible or associated with high costs for the buyer. It would be helpful to have further clarifications on how to assess these types of standardized services where the "essential means" already are predefined and if there can be situations where a "processor" in fact is to be regarded a controller when offering a standardized service.

The Swedish Trade Federation also welcomes clarifications and practical examples on the level of detail that must be met in the instructions to the processor, see section 1.3.1. If possible, it would be beneficial if the EDPB could provide a standardized template to be used in data processor agreements.

Assessment of security measures

The controller is responsible for ensuring and demonstrating compliance with the GDPR according to Article 24. This includes responsibility for implementing appropriate technical and organizational measures. In addition, according to Article 28.1, the controller can only use processors who can provide sufficient guarantees to implement technical and organizational measures. Moreover, the processor must be able to demonstrate compliance to

Regeringsgatan 60
11143 Stockholm
Tel 010-47 18 500
svenskhandel.se

the satisfaction of the controller, se paragraph 93. In many cases, the service provider has the sole responsibility of implementing security measures appropriate to the risk and the controller has an obligation to conduct audits and inspections to assure that the security measures are sufficient, see Articles 28.3 (f) and (h). According to Article 24.3, approved certification mechanisms referred to in Article 42 could be used as an element to demonstrate compliance.

In light of the above, the Swedish Trade Federation wants to bring the EDPB's attention to existing information security standards, such as the SOC 1, SOC 2, and SOC 3[1], that can be used to assess whether a service provider satisfies "good information security practices". As there is already a mechanism for auditing information security measures and obtaining reasonable assurance through these reports, it would be beneficial if data controllers could demonstrate compliance also under the GDPR by relying on existing standards regarding information security measures implemented by their processors. Indeed, by using existing standards the controllers would have better tools to assess information security measures as part of their obligations under the GDPR, and the processors would have a clear framework on how to create a high level of information security in their services. Consequently, this is something that would benefit the protection of data subjects' rights. The Swedish Trade Federation welcomes a statement from EDPB that certain existing standards indeed could serve to demonstrate compliance, e.g. regarding implemented information security measures, under the GDPR.

The rapporteur has been policy expert and lawyer Sofia Stigmar and Linda Leffler Olsson.

[1] AICPA, SOC for Service Organizations: Information for Service Organizations, https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganization-smanagement.html (2020-10-13 14:39).