SVENSKT NÄRINGSLIV

European Data Protection Board

2020-12-18

Feedback: The EDBP draft Recommendations 01/2020 on measures that supplement transfer tools and Recommendations 02/2020 on the European Essential Guarantees for surveillance measures

Due to the fact that the European Commission has published new versions of the Standard Contractual Clauses, SCCs, as well as newly suggested Article 28 Clauses for Data Processing Agreements, SCCs are still considered as a viable transfer tool by the European Commission. The Schrems II ruling impacts every personal data transfer where different transfer tools are used (i.e. not exclusively Standard Contractual Clauses) and onward transfers are included in the scope and affected as such.

Identify and access third country jurisdiction

Despite the EDPB Recommendations provided, the core challenge for any company will continue to be how to reasonably identify and assess the jurisdiction of a third country data protection and surveillance laws. There will be inconsistent conclusions if the laws are compliant with the principles of necessity and proportionality and the presence of an impartial oversight mechanism offered by a judicial body or independent organisation, especially with reference to the level of analysis that is required by the EDPB in step 3 and the fact that many companies do not have the competence or resources to do this kind of assessments. This is reinforced by the experience of the EU commission whose decisions often took years to conduct similar exercises. It also raises questions on how local DPAs will have the scope and resources to assist organisations review and/or review assessments as the issues will cover national security issues across a range of jurisdictions, legal systems and cultural norms.

Risk-based approach

Not having a risk based approach where assessing the sensitivity of the data and the likelihood of it being of interest to foreign surveillance puts unnecessary constraints on companies to implement security measures where it in practice may not be needed.

We believe it is reasonable to take into consideration (i) the categories of personal data, (ii) the likelihood of surveillance measures based on the identity of the actual importer and exporter and (iii) the categories of data subjects. The realistic risk of being subject to access

Svenskt Näringsliv Confederation of Swedish Enterprise
Postadress/Address: SE-114 82 Stockholm Besök/Visitors: Storgatan 19 Telefon/Phone: +46 (0)8 553 430 00
www.svensktnaringsliv.se Org. Nr: 802000-1858

requests of public authorities varies significantly based on the business model of the exporter and importer (data transfers for business purposes vs. social networks), and the data category (business data vs. private information). The level of extra protections afforded to data transferred internationally should be proportionate to the level of risk it poses.

EDPB should add to paragraph 33 that the likelihood of public authorities' access in the specific case of a transfer scenario can complement the other factors for assessing the risk of the transfer. EDPB could also clarify paragraph 42 to set forth that, when legislations in third country may be lacking there should be flexibility to determine if case law or codes of practices provide sufficient information The likelihood of access cannot be used as the sole criteria to determine the risk in the assessment.

Also, the importance of contractual and organisational measures should not be overlooked. While contract verbiage does not bind third countries' authorities by nature, any importer's commitment to challenge, redirect or pushing back a government request, as well as and transparency measures to inform the exporter / controller of any such request, is of paramount importance to determine whether interference will effectively take place. Thus, not only technical, but also a combination of contractual and organisational measures can ensure an essentially equivalent level of protection for data subjects in practice. Particularly in combination with a more proportionate and risk-based approach to data flows less at risk of interference and surveillance.

Organisational measures such as ISO certifications are also certified mechanisms under GDPR and the global nature of these standards can efficiently help global businesses assess and comply with relevant privacy laws, particularly if the standard is updated to address specific issues such as local surveillance laws. EDPB should amend paragraph 48 taking into consideration that a holistic view and a risk assessment can lead to the result that contractual and organizational measures alone can sufficiently protect the data subject. Further, EDPB could include a reference to contractual and organizational measures in paragraph 33.

The recommendations go beyond the requirements of the GPDR resulting in severe disadvantages for EU companies' competitiveness and digital innovation. We note that the EDPB does not consider the requirements in GDPR and the Schrems II judgment to have a risk-based approach when determining if and what supplementary measures that may be required. Therefore, we request that the EDPB clarifies that the transfer tool under Article 46 alone, depending on the processing of personal data, could satisfy the requirement of an "essentially equivalent level of data protection".

Use cases

We welcome the EDPB's approach to introducing "Use Cases" as a way of providing examples of situations where a transfer, with appropriate supplemental measures, would be considered as providing an adequate level of protection. It reflects an enormous effort to provide concrete examples and options for companies to address a nearly impossible task; finding a way to maintain EU data protection standards in an inherently global and multicultural world in which norms and laws diverge.

Unfortunately, the use cases in the current recommendations are too general. We would like to ask the EDPB to describe the different supplementary measures in relation to actual

services that are used by millions of data controllers around the EU, for example email services, analytic tools, marketing services and using a cloud provider not only for backups but rather for storing active data.

Swedish companies are relying on the biggest search engines to be visible and relevant for consumers and B2B-customers all over the world. Removing US tools would be like remove the possibility of EU companies to be reachable in the global market. The effect would be that EU companies lose the competitiveness on the market due to lack of visibility.

Security and Encryption

Restricting data flows is detrimental to the security of data. Global cloud service providers offer cutting-edge security services not based on location but by the policies and technology used. The EDPB Recommendations could incentivize data controllers to prefer less secure service providers only because of local processing, over those which process data also in third countries to avoid complex risk assessments and monitoring obligations, which would be especially challenging for SMEs. The EDPB Recommendations would considerably lower security standards.

While encryption can provide strong protection against access to data, including bulk data collection by governments, it can only serve as one of several potential measures to protect personal data in transition and “at rest” (i.e. when stored on a cloud provider’s servers). The reason is that encryption might impact certain processing activities, e.g. certain operations in the course of a SaaS offering, when datasets are analysed, or other computations are carried out, to render a specific service to the client.

Moreover, the general requirement to apply comprehensive encryption to all stages of the data processing would result in companies having to implement very costly encryption methods even cases where the risk (taking into account all factors, including the likelihood of access) is very low. Such encryption measures would be disproportionate, and particularly burdensome for SMEs.

Most importantly, strict prohibitions of decryption at any point in the processing undermines IT security as technologies such as packet inspection hinder the transfer of malicious traffic and to absorb DDoS attacks. Decryption of the packets is necessary to do this analysis. If this measure is prohibited, many businesses would struggle to maintain a high level of IT security, significantly damaging the resilience and security IT network and critical infrastructure.

The EDPB Recommendations should take into account that the access to industry-standard IT security measures is essential for any business processing data. The access to state-of-the art security services must be factored into any risk assessment of transferring data to a third country.

THE CONFEDERATION OF SWEDISH ENTERPRISE

Carolina Brånby