Technology Industries of Finland

12/21/2020

Technology Industries of Finland comments to EDPB Recommendations 01/2020 on Supplementary Protection Measures on Data Transfers

Technology Industries of Finland (TIF) is a national trade organisation, representing more than 1,600 technology companies active in Finland. The technology industry is Finland's most important export sector. Technology companies operate in international export markets and ability to process data efficiently and based on one data policy is of utmost importance to our member companies.

The European Data Protection Board (EDPB) has invited public consultation on its Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, published on November 11, 2020. On the same date, the EDPB published Recommendation to European Essential Guarantees for Surveillance Measures. In addition to the comments provided by Confederation of Finnish Industries ("EK"), TIF would like to draw attention of the board to the following remarks:

Key Messages

- European (technology) companies operate in global export market
- ECJ Case Law and EDPB Recommendations place everyday data-functions of companies under threat
- Everyday functions of companies, information tools, Email, Customer Relations Management Systems and Human Resources systems are data driven. Ability to access data company-wide and ability to use data for sales, analysis, HR development and customer management are of key importance to companies' competitiveness.
- Generally, data processed in everyday business transactions is very unlikely to be subject to intervention from surveillance bodies or other intervention from third countries.
- EDPB should place more weight on nature of data and develop more risk-based approach to transfers and measures needed to protect data from interventions of governments.

Detailed Remarks

In the Schrems II ruling, the ECJ explicitly referred to the possibility to carry on data transfers if the controller implements "additional safeguards" or "supplementary measures", in the case that the destination country does not offer equivalent or adequate level of protection. Further, the Court stated that the transfers should be assessed "in the light of all the circumstances of that transfer", "on a case-by-case basis".

Data transfer out of the EU should not automatically and per se be considered as high-risk processing, even in absence of an adequacy decision. In the light of the Schrems II ruling, transfers should be assessed in context. There is no apparent reason to derogate from the general GDPR risk-based approach.

Ability to effectively process data is a key pre-requisite for successful running of every global company, no matter of what size. On a Schrems II Impact Survey Report[1], commissioned by

[1] https://www.digitaleurope.org/wp/wp-content/uploads/2020/11/DIGITALEUROPE_Schrems-II-Impact-Survey_November-2020.pdf

DIGITALEUROPE and other European business associations, 9% of surveyed companies stated that they are not transferring data outside Europe and 85 % of surveyed companies were estimated to use standard contractual clauses as legal base for transfers. Furthermore, only 8% of surveyed companies estimated the cost of reassessment of their SCC practice to be negligible and 92 % estimated cost to be high or moderate.

At such an hour, when companies' means to survive depend heavily on their ability to run their businesses digitally, recommendations that would force huge and expensive changes to existing data transfers to carry on their businesses, would deliver quite a blow to European companies.

Recommendations should be re-thought to better balance real-life threats to privacy and reasonable operating environment of companies.

Firstly, the board should allow more weight in recommendations for nature and type of data. On para 33, categories of data is listed as one of the factors to be considered in the analysis, but relevance of category is not elaborated further.

Secondly, the board should allow more weight for likelihood of intervention of surveillance authorities of third countries. Usually, data processed in course of business is linked to business transactions, account management, HR operations or normal office solutions. Ability to effectively process this kind of data on daily basis, throughout the organisation is a key requirement for successful running of any international organisation.

This kind of information is likely not to call attention of surveillance authorities, but ability to process it is strictly necessary to run day-to-day business. Para 42 of the recommendation divides the assessment of third country's practices to subjective and objective factors. This division rules out the role of assessment of likelihood of data being accessed by surveillance authorities. Additionally, the depth and effect of access by surveillance authorities may vary significantly and that will also affect on how it affects privacy of individuals as well. This is not reflected on the recommendations neither.

The use cases n:o 6 and 7 provided in the recommendations for which no supplementary measures can be envisioned, are the ones that are used on daily basis in global business operations and used by great number of companies to make data available where it is needed.

By addressing the issues above, the board would be able to allow European companies to maintain competitive edge and carry on their daily operations without massive restructuring of their data practices.

Inquiries:

Jussi Mäkinen, Head of Digital Regulation, Jussi.makinen@techind.fi, +358 40 900 3066