FEEDBACK

Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

On November 11th, 2020, the EDPB published a recommendation which was supposed to help European data controllers understand how they could transfer personal data outside the European Union. However, this recommendation is not as pragmatic as we were hoping for.

We took two examples to illustrate this view, based on use cases described by the EDPB.

1. **Transfer of personal data that can directly identify an individual to the United States (US)**

According to the EDPB[1], it is only possible to transfer personal data to the US without breaching the GDPR if:

- The personal data is strongly encrypted, and
- The data importer does not have access to the encryption key

⇨ This practically prevents any access / processing / enrichment / analysis in the US by US actors.

Practical example: a data controller ("client") works with a software provider, whose responsibility it is to ensure that its software is always up and running for its client. In order to remedy any technical issue the client could encounter, the software provider installed its customer services in several countries, situated in different time zones, to ensure that clients' queries could be answered around the clock. Being able to benefit from customer support 24/7 is one of the criterions a company will take into account when choosing a software provider. Yet, in order to be able to respond to clients' requests, the customer services could need to have access to personal data.

Therefore, should European companies only use softwares for which customer services are based in Japan, Argentina or Uruguay, three countries deemed adequate by the European Commission?

According to the EDPB recommendation, only a "passive" data storage outside the EU, which does not require access to unencrypted data[2], seems possible. This seems neither practical nor conceivable in the "real world", especially for low-sensitivity data.

2. **Transfer of pseudonymised personal data to the US**

According to the EDPB[3], it is only possible to transfer pseudonymized personal data to the US without breaching the GDPR if:

- The personal data can no longer be attributed to, or single out a specific data subject without the use of additional information (even if the data was to be cross-referenced with information held by the third country's public authorities), and
- The data importer does not have access to the additional information

[1] EDPB - 1/2020_EN - Measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (§79).
[2] Id. The EDPB mentions access to data "in the clear".
[3] Id. (§80).

⇨ If we basically need to presume that public authorities in the US are likely to possess data concerning data subjects' use of information services[4], which could enable to identify them individually[5], then pseudonymisation can never provide an effective supplementary measure.

In conclusion, if our combined analysis of the CJEU *Schrems II* decision and the Board's recommendation is correct, then the transfer of personal data to the US (or any country with known surveillance practices by public authorities) is only possible if:

- The personal data is encrypted beforehand,
- The personal data is transferred to be processed in the US, but the processing does not require any access to unencrypted data.

In any other situation, there doesn't seem to be sufficient guarantees to ensure personal data is afforded a level of protection essentially equivalent to that guaranteed in the EEA[6].

⇨ **How can we consider that the recommendation takes a practical approach?**

As long as no European software or service can respond to companies' crucial needs, it is the role of the European Union to assume its responsibility, by:

- Publishing a list of countries which legislation would impinge the effectiveness of EU law's safeguards if personal data were to be transferred there, and
- Depending on the risk posed by each one, suggesting pragmatic security measures that data controllers could take in order to transfer personal data to these countries.

It is neither in the role, nor in the skills of each data controller to carry out this task, especially in a situation where the world was still "open" six months ago, enabling continual data flows between the EU and the US.

We do believe that the European Union should give itself the means to hold its position of defender of liberties, by taking a strict approach regarding data protection, in order to compel third countries such as the US to change their legislation and practices. However, on a shorter-term basis, it is necessary for the European Union to help companies find pragmatic solutions in order to enable them to transfer personal data safely.

Feedback written by Sébastien Gantou & Mathilde Tanon – DataSphere SAS / Digital DPO

[4] Id. (§§82, 83)
[5] Id. (§81)
[6] Id. (§88)