FiCom | Asko Metsola
18.12.2020

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

Finnish Federation for Communications and Teleinformatics FiCom is a lobbying organization for the ICT industry in Finland and looks after its interests. FiCom's members (Cinia Oy, Cisco Systems Finland Oy, Digita Oy, DNA Oyj, Elisa Oyj, Oy L M Ericsson Ab, Finnet Association, Geomatikk Finland Oy, Google Finland Oy, HP Finland Oy, Maxisat concern, Microsoft Oy, Nestor Cables Oy, Rejlers Oy, Suomen Erillisverkot Oy, Teleste Oyj, and Telia Finland Oyj) are companies and other entities that operate in the ICT sector in Finland.

FiCom thanks for the opportunity to comment on the Recommendations and states the following:

2.1. Step 1: Know your transfers

The following two use cases are created as examples in order to ask for further clarification from the EDPB in relation to finding effective supplementary measures or whether GDPR Article 49 (1) (a) or (b) could be used:

> Case 1: Considering the footnote 22 in the Recommendations which states that remote access by an entity from third country to data located in the EEA is also considered a transfer it would be appreciated to get a further clarification in regard to how third level support should be addressed in such cases? The question relates to situations where a supplier's support is needed in the technical environment to solve an incident, where first- and second-line support has not been able to solve the matter. These cases can be done in a very controlled manner without any access to personal data and if data needs to be accessed, it is done in a strictly monitored way, etc.
>
> Case 2: Telecommunication service provider is acting as a processor in B2B relationship and an incident has occurred to the platform of that telecommunication service provider. The supplier providing third level support may process the incident ticket in the third country (usually United States). The data processed by the supplier are the data in the incident support ticket sent by telecommunication service provider to the supplier who provides a platform.

Is it possible for EDPB to clarify whether such use cases could be considered as scenarios for which effective supplementary measures could be found?

In addition, is it possible for EDPB to give its assessment whether GDPR Article 49 (1) (b) could be used for such third level support cases? The aim is to understand whether it is acceptable for the EDPB that controller could use GDPR Article 49 (1) (b) for the third level support cases as such cases are by nature impossible to predict and control in advance.

If Article 49 (1) (b) is not applicable in such context, could that be considered an acceptable approach for the EDPB that for such use cases consent would be acquired based on Article 49 (1) (a) instead (following all applicable conditions to acquisition of valid consent based on GDPR)?

According the Recommendations data exporter should know the transfers and suppliers till the very last supplier. It is important to highlight the big challenges related to that recommendation. In reality, there are cloud service providers to whose clouds hundreds of other cloud service providers can join and it is impossible to investigate all suppliers in the cloud services. This also relates to SaaS (software as a service) – the buyer of the service has no control over how the service is provided as vendors are constantly changing, etc. Therefore, further guidance would be appreciated in relation to the data exporter's responsibility to investigate the supply chain of cloud service providers, especially in SaaS cases.

2.3. Step 3: Assess whether the Article 46 GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer

Is it possible to get further clarification whether there are any other requirements for documenting the assessments, besides written documentation?

Where appropriate, it is stated that one's data importer should provide data exporter with the relevant sources and information relating to the third country in which it is established and the laws applicable to the transfer. Considering that the data exporter needs to be able to rely on supplier's information, is it possible to get further guidance on how should the liability be divided in these cases?

Third countries like United States, India and Sri Lanka are common countries for IT and support and customer care related collaboration for the European companies. Therefore, it would be highly beneficial if the EDPB provides guidance regarding those countries' data protection adequacy level, so that companies do not have to do such assessments one by one? The guidance is specifically requested for telecommunication service providers which are subject to additional scrutiny due to Schrems II decision.

Alternatively, the Recommendations could explicitly acknowledge that, in determining whether and what safeguards to apply, data exporters can and should consider the specific circumstances of the transfer —including the likelihood, based on documented expert analysis, that third-country national security authorities will in fact access the data, the scale and frequency of the transfers, the type of recipient, the purpose of processing, the nature of the personal data transferred, and other relevant factors.

2.4. Step 4: Adopt supplementary measures

In the Recommendations it is stated that if you transfer personal data to third countries, regions or sectors covered by a Commission adequacy decision (to the extent applicable), you do not need to take any further steps as described in these recommendations. However later in the Recommendations it is stated that controllers may have to apply some or all of the measures described in use cases irrespective of the level of protection provided for by the laws applicable to the data importer because they are needed to comply with

Articles 25 and 32 GDPR in the concrete circumstances of the transfer. Is it possible to ask for additional clarification on how these two statements should be understood together?

The GDPR establishes a risk-based framework to protect personal data. The SCCs and other Article 46 transfer mechanisms are similarly risk-based; they contemplate that data exporters will choose "appropriate safeguards" for a transfer based on the level of risk involved (GDPR Art. 46(1)). The CJEU's Schrems II decision also recognizes that exporters must make "case-by-case" assessments, and that "all the circumstances of the transfer" must be considered when determining whether a transfer can proceed (e.g., paras. 121, 126, 134). When assessing supplementary measures, GDPR's risk-based approach is not reflected in the Recommendations. It can for example be noted that it´s only briefly mentioned in the Recommendations that a factor that can be considered when assessing supplementary measures is the nature of the data. Isn´t that circumstance quite important to decide the risk level of the transfer and what kind of supplementary measures should be put in place?

The Recommendations could be read to take a formalistic, "one-sized-fits-all" approach—suggesting that technical measures are always required where there is the mere theoretical possibility of government access, regardless of the context of the transfer, and providing "Use Cases" that do not acknowledge that technical safeguards may not be necessary for some transfers, or that in some cases, contractual and organizational safeguards alone may suffice. As a matter of fact, in some cases, technical safeguards can be the most effective additional safeguard, for example to avoid covert surveillance under authorities such as the U.S. Executive Order 12333. In other cases, organisational safeguards can be effective, such as to challenge orders. And contractual safeguards can buttress these measures by imposing liability on data importers to comply. To the extent that the Draft Recommendations can be read to conflict with such an approach, they should be revised.

In the use cases provided by the Recommendations it´s not visible that the nature of the data is a part of the assessment and something to be considered. Therefore, one could interpret that transferring email address abroad is posing equal risk to a data subject as transferring traffic data or sensitive data for example. Could it be clarified how much weight should be put on the nature of the data? Recommendations should identify a list of potential safeguards, but be clear that data exporters should be free to choose whatever safeguards they deem most appropriate based on the context of the transfer.

In the Recommendations, under section 60, it´s highlighted that it is the responsibility of the data exporter and the data importer to assess whether the level of protection required by EU law is respected in the third country concerned in order to determine if the guarantees provided by the SCCs or the BCRs can be complied with in practice. However, other parts of the Recommendations states that it´s the data exporter that is responsible for the assessment of the need of supplementary measures. Could the EDPB clarify if there is legally a joint responsibility for the assessment or rather not? Can contractual guarantees by the processor replace the investigation obligations of the controller?

2.6. Step 6: Re-evaluate at appropriate intervals

How often should reassessment be done? In cases where there are no additional triggers for re-assessment (e.g. data breaches, other alerting events), is there any specific interval of time the EDPB is having in mind for re-evaluation?

General notions

Are the parties in general free to contractually put the responsibility on one of the parties (the one with the best control over the circumstance at hand)?

In the Recommendations it´s stated that if you decide to continue with a transfer notwithstanding the fact that the importer is unable to comply with the commitments taken in the Article 46 GDPR transfer tool, you should notify the competent supervisory authority in accordance with the specific provisions inserted in the relevant Article 46 GDPR transfer tool. The competent supervisory authority will suspend or prohibit data transfers in those cases where it finds that an essentially equivalent level of protection cannot be ensured. According to the Finnish DPA it will send all notified transfers to the EDPB to decide on since those decisions cannot be made country by country. Considering that it would be appreciated if the EDPB could clarify the procedure for notifications, the process and handling times for these notifications. What is expected from the data controller during the time the case is pending in the EDPB regarding the transfer, shall controller continue as-is until the resolution is given? When the controller has concluded that they need to notify the DPA and reaches out to the DPA, what is the scope of the assessment local DPA will be doing compared to what the EDPB will be doing? Who will be the one deciding on the penalties?

It seems that the responsibility to assess compliance to transfer mechanism (e.g. SCCs) is mainly placed on the data exporter. Shouldn´t it be on the data importer (contracting party signing the agreement)? Signature of a contract constitutes a civil law act, which the signatory becomes legally bound by. If a party signs a contract it may perhaps not be able to comply with, this entails risk for a breach of the contract. It is possible to argue that legally it would be more correct to put the liability on the contracting party that is not able to follow the contract. However, the assessment of supplementary measures could be joint if the contracting party brings up flaws in the ability to be compliant to the contract.

In general, the spirit in the Recommendation is that data transfers outside EU/EEA are undesirable. It is important to highlight the fact that companies cannot work only in EU/EEA without connection outside EU/EEA since most companies are fully dependent on service providers outside EU/EEA. In addition, telecommunication service providers are obliged to transmit communications throughout the world, and it is vital that data is also transferred outside EU/EEA to make that happen. Telecommunication service provider has an obligation to provide secure and functioning services and service providers are needed to provide incident and maintenance support 24/7 in accordance with “follow the sun principle”. Also, companies shall have the freedom to choose their service providers and structure their business in a way that supports their business and operations in the best possible way. Any further clarification from the EDPB on that matter would be highly appreciated.

Use cases

The whole concept of "*supplementary measures*" is problematic as building supplementary measures for Use Case 6 would mean that solutions and information technology could be built at the European end which would make it impossible for the foreign authority to get their hands on the original data. This kind of assignment is not possible and would put unrealistic expectations on European companies.

The EDPB states essentially the same in the following, regarding the Use Case 6:

> *EDPB is, considering the current state of the art, incapable of envisioning an effective technical measure to prevent that access from infringing on data subject rights. (88., p. 27)*

Based on the abovementioned, supervisory authorities should not be setting such unrealistic expectations on the companies, but instead try to provide "white-listed" or approved cloud service providers list to the EU/EEA companies, if possible.

It is a reality in many situations, that maintenance of an IT system has been outsourced to other geographies. It is also a reality and a real repeating case that IT incidents happen. Sometimes, the best resources of an international service provider may well be situated out-of-EU. Professional maintenance does not always necessitate constant always-on-access to all of the system but can rely on controlled when-needed access. It would be highly appreciated if the EDPB could clarify how to provide such limited access to non-EU geographies without a data exporter immediately finding itself in a situation which could be considered a GDPR breach. For exemplifying the case, this access could be called 'targeted access':

Characteristic to this would be:

- this access is in principle different compared to a constant 'always on' access
- it is controlled by the data exporter
- targeted access is given when-needed (limited in time)
- targeted access is given to what-needed (limited in scope)
- data operations done are logged hence giving the extra control of what is happening to the data

The present Recommendation could give more input on if this type of access could be granted without it being a violation of GDPR and the Recommendations.

Further clarification would be highly appreciated on use cases 6 and 7. Do these use cases mean that personal data storage, maintenance and access (i.e. any and all processing) must be in EU/EEA and no supplementary measures help for those cases whatsoever (i.e. full data and related services localization to EU/EEA is the only option)?

Is that the goal with the Recommendations that cloud vendors with headquarters in third countries shall establish cloud servers in EU/EEA and ensure 24/7 support also only from EU/EEA despite that support could be provided in a better and more efficient way from third countries during the European night hours?