# Feedbacks on EDPB Recommendations 01/2020

As a programmer, a hacker and a software architect specialized in legal and financial software, I have to admit that by seriously following the Recommendations EDPB wrote, data controllers and data processors would do a great job to protect the long term freedom and privacy of European citizens on the global Internet.

Despite several careful readings, I've been able to find very few attack vectors that could allow their legal or technical circumvention and let me say this is actually unusual.

Yet some important improvements are needed to reduce the probability of misbehaving entities that could ignore or circumvent the supplementary measures required by the GDPR, weakening the effective data protections of Europeans and thwarting their fundamental rights.

## Automatic data transfer through software proxy

Let's start by saying that I really appreciated the recommendation at chapter 2.1, paragraph 13: any remote access to the data from a third country to data stored in European Union must be considered as a data transfer, even if done for technical or support reasons.

However European organizations that store personal data into local data centres but use software controlled by entities outside the EEA, could allow such entities to easily access such data through the software itself.

For example the automated (or otherwise independent) control of any software that can access the protected data, e.g. through a centralized configuration automatically consumed by the software itself or through any form of automatic updates, should be considered as a data transfer in and of itself.

Consider the following use case:

> A European data controller sells to data subjects raw storage on its own data centres. To increase security and minimize management costs, it adopts an operating system (or any another software that could gain access to the data) that automatically applies its own security updates, published by a third party located outside the EEA. Despite not having any right to access to the data, such third party could easily access them by publishing a version of the software that accidentally includes instrumentation for remote debugging left behind during development or even a full blown backdoor.
>
> If such third party could be forced by its local legislation to do so, the data breach would pass completely unnoticed as it could remove all the evidences of the access just as easily.

It's not easy to design effective supplementary measures to protect personal data against such kind of access, and even just detecting them could be very expensive.

If the software is published in source form and provides for reproducible builds, the data controller could compile the software locally, from scratch, after a careful code review of each new version by an independent team of European InfoSec experts. But to ensure proper and verifiable application of such operational measures, the data controller should also publish a cryptographically signed hashchain of the sources and the binaries executed after each update along with the signed security

report and a trusted timestamp from a European TSA. Furthermore each version of the sources and the binaries deployed in production should be safely archived for an appropriate number of years, as a condition to prove proper compliance in case of inspection or litigation.

Yet, depending on the role of the software, the kind of privileges it gets at runtime, the architecture of the data centre and several other technical factors, such procedure could impose a dangerous delay to the application of critical security updates, reducing the data protection provided against other kinds of attack. Moreover technical measures adopted to secure the access to the data by the software may fail, after the discovery of certain vulnerabilities, thanks to the local access to the hardware and the runtime permissions of the software. Think for example to vulnerabilities such Hearthbleed, Meltdown and Spectre or the very recent flaw discovered in Intel SGX, allowing a local software to steal crypto keys stored in the memory enclaves through a technique called Load Value Injection that could be very easy to exploit with such kind of administrative access to the servers.

In such cases, the execution of software provided by the third party from outside the EU could severely reduce the protection granted to the fundamental rights of European citizens.

So my suggestion is to recommend data controllers and data processors to

1. carefully document the usage and the whole administrative control chain of any software that could gain access to the personal data and is developed, distributed or otherwise controlled by entities outside the EEA
2. detail the security measures, the technical procedures and the technologies adopted to avoid and/or detect such kind of data breaches
3. stop running the software if no supplementary measure could effectively protect the data from such kind of attacks without reducing the overall security
4. stop running the software if the supplementary measures adopted become vulnerable to locally exploitable attacks and until they are fixed or replaced with better alternatives

My 20 years experience with large corporations and their legal teams reassures me that such deeply technical assessments, measures and procedures will be actually put in place if (and only if) explicitly recommended by the EDPB, but their lack would completely cancel the kind of data protection that the EJC recognised to European citizens with the Schrems II sentence.

# Shoaling

Another simple and powerful attack vector to the GDPR is the ability to hide in the shoal: like fishes that avoid predators, each member of large number of small entities that share similar business practices, dilutes the chance of individual "capture" by the competent Supervisory Authority in case of misbehaviour.

Many organizations transferring data outside the EEA would accept a small risk of ignoring these Recommendation, since the accountability depends on the resources of the competent Supervisor Authority, which might constitute a serious bottle neck to enforcement (see paragraph 7 of the Recommendations). Moreover such bottleneck would create an individual and collective incentive to setup delay tactics, producing a distributed denial of service that could practically disrupt data protection on a national scale.

So my suggestion is twofold:

1. explicitly clarify that, according to the Article 12 of the GDPR, the data subjects has the right to receive (or at least to request) the whole documentation about the assessments and supplementary measures adopted for data transfers outside EEA,
2. clarify the maximum delay allowed to comply to such access requests (from the data subject or competent Supervisor Authority), and recommend the definition of effective day-fines for each day of delay afterwards, designed according to Article 84 and Recitals 150 and 151 of the GDPR

By recognising to the data subject the right to receive (or at least to obtain) the whole documentation about the transfers, you reduce the ability to hide bad behaviours behind the large number of data controllers to monitor, increasing the probability of being caught on misbehaviour. Moreover data-subjects might ask for support to independent lawyers and technicians to understand the effectiveness of the supplementary measures adopted, without overwhelming the Supervisor Authority with misguided complaints.

The day-fines after a reasonable wait would encourage corporations to actually be proactive into implementing and documenting their assessments and the supplementary measures.
To maximize this virtuous effect, wherever the local legislation allows for this, EDPB may recommend that part of such fine should be turned into a damage repair for the requesting data subjects, so that people would get an economical incentive to go after bad actors and protect the privacy of their fellow citizens.

# Sharksuckers

The remora (also known as “sharksucker”) is a small fish whose front dorsal fins evolved into an organ that works like a suction cup to attach to a shark, usually on the shark's belly or underside. Remoras eat parasites from the shark’s skin and mouth, while the shark protect remoras from predators and give them free transportation throughout the oceans.

A similar strategy has been adopted by many small data controllers to effectively dissuade data subjects to engage in data protection litigations despite blatant data transfers towards the USA were occurring after the invalidation of the Privacy Shield.

The trick was to take a safe bet by choosing (and imposing to the data subjects) a platform provided by a Big Tech firm, and then declare that such firm was in fact acting as an autonomous data controller on its own, even refusing to acknowledge any joint-controllership (and despite explicitly signing Data PROCESSING Agreements).

Such strategy has been successfully applied, for example, by most Italian schools during the first and the second waves of the SARS-CoV-2 pandemic: feeling threatened by the legal strength of these large corporations, most parents waived the rights granted to their children by the GDPR. Many Italian DPOs actually endorsed such behavior, without even requiring from the data controllers simple and obvious data minimization techniques, such as using temporary pseudonyms for students or providing VPNs and proxy servers to hide their IPs, user agents and location.

The net effect of such "sharks' fellowship" has been a severe reduction of the data protection of millions of children and young Europeans, with a huge potential for long term effects on the freedom and autonomy of a whole generation of Italians.

To prevent such concrete privation of fundamental rights to happen again, it should be clarified

1. what conditions can led to a joint-controllership
2. to what extent the data controller who chooses to adopt the services of a third party (either as data processor or as joint-controller) remains accountable for the choice itself, if such third party was unable to grant complete and effective protection to the data subjects from the very beginning or if such service agreement was not ceased after the Schrems II decision
3. how supplementary measures should be put in place to reduce the data transferred outside EEA to the bare minimum technically required to provide the services (even in case of a joint-controllership), and who will be held accountable in case of their lack.

# Lying

In section 2.4 it should be explicitly stated that any supplementary measure, either technical or operational, should allow independent verification of their effectiveness and their proper application, by design.

In fact, given the information asymmetry between data subject on one hand and data controllers and processors on the other, it's very easy for the stronger parties to misrepresent or simply lie in the documentation provided about the supplementary measures adopted. Thus it would be wise to clarify that any supplementary measure whose effectiveness and proper application cannot be concretely verified by an independent third party, has to be considered inadequate to protect the data subjects.

Moreover, since it would be impossible for the competent Supervisor Authority to actually verify the proper application of all the measures declared by all controllers and processors, it would be wise to allow independent third parties to audit their application on behalf of requesting data subjects (which would obviously bear the cost).

Such form of transparency of data controllers and data processor would facilitate the exercise of data subjects' rights under Articles 15 (2) of the GDPR, as established by Article 12 (2) and at the same time it would reduce the load on competent Supervisory Authority, as data exporter would have a huge incentive to be proactive in data protection.

# In conclusion

The EDPB "Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" look clear, coherent and well designed.

By closing the few loopholes detected here, the Board would spread a robust set of practices to effectively protect our fundamental rights, raising the rational trust in data management and protection all over the European Union.

Your fellow citizen,

Giacomo Tesio