19 November 2020

"The Future of Encryption in the EU"

ISOC 2020 Webinar

Keynote Speech by European Data Protection Supervisor

Wojciech Wiewiórowski

Introduction

Ladies and Gentlemen,

The pandemic crisis not only makes our lives increasingly digital, but also accelerates the adoption of new technologies to support this digital transformation and the fight against COVID-19.

All of us rely on digital services in our lives and for work, consequently, an unprecedented amount of personal data processing activities and digital communication take place – around us and in our pockets.

This also comes at a price for the rights to data protection and privacy of individuals, which is already visible to us as we observe the number of cybersecurity incidents and personal data breaches increase.

The importance of encryption for data protection and privacy

Today I want to contribute to the debate by focusing on encryption from a data protection supervisory authority's point of view.

Thanks to the GDPR, encryption is officially part and parcel of effective data protection and privacy, for almost 2,5 years now.

Why? Because the GDPR explicitly refers to encryption in three of its 99 articles.

In the section on the security of processing, Article 32 lists encryption as a prominent security measure for personal data.

Another situation where encryption plays a role is in the assessment of personal data breaches in Article 34. A controller may not be obliged to communicate a breach to individuals concerned if encryption was applied to the data in question.

In both cases, the supervisory authority will have to assess not only the risk(s) related to data processing as such, but will also need to understand the effectiveness of the cryptographic measures.

In addition, Article 6 paragraph 4 on lawfulness of processing allows for the processing of data beyond its original purpose, when this purpose is "compatible". One of the elements to take into account in this assessment is the existence of appropriate safeguards, which may include encryption.

Although these three Articles 6, 32 and 34 explicitly mention encryption, there are of course other contexts in which the GDPR mandates appropriate technical and organisational measures, and these may include encryption, e.g. for data protection by design and by default.

While encryption as such is not always mandatory, the GDPR expresses a clear preference for such measures, therefore the EDPS (and other supervisory authorities) expects data controllers and processors to use them whenever possible.

The Schrems II Judgement

This is for example the case for international data transfers.

The European Data Protection Board (EDPB), of which the EDPS is a full member, has just last week issued its long-awaited practical guidance following the Court of Justice of the European Union's landmark Schrems II decision. The guidance is open for public consultation until 30 November. It outlines EU data protection authorities' expectations on how organisations should approach international data transfers of GDPR-covered personal data, including supplementary measures that companies can adopt to protect data from overreaching government surveillance outside of Europe.

As for encryption, the EDPB underlines that strong, state-of-the-art encryption in-transit and at-rest can help to provide an adequate level of data protection. This will apply in particular to scenarios where a data exporter uses a hosting service provider in a third country to store personal data (e.g., for backup purposes). The EDPB, however, stresses that encryption would only be an effective supplementary measure if the cryptographic keys are retained solely by the data exporter, or other entities entrusted with this task that reside in the EEA or a third country that the European Commission has found to provide an adequate level of data protection.

Here we clearly see the importance of having appropriate encryption mechanisms. They have the power to mitigate risks that otherwise might force processors to relocate huge datacentres, and controllers to move services to new compliant processors.

Challenges for strong encryption

There are certain challenges for strong encryption, such as:

- the need to maintain strong encryption algorithms and secure encryption products in the face of technological developments, e.g. quantum computing, as well as hardware and software vulnerabilities;

- how to deal with the metadata of encrypted digital exchanges, as personal data can be inferred using data mining and artificial intelligence.

From the perspective of individuals' whose data is processed and the viewpoint of a data protection supervisory authority, any weakening or circumvention of encryption constitutes a limitation of the rules designed to protect the fundamental rights to the protection of personal data and privacy.

We all know that one of the greatest disadvantages of IT backdoors in general - not just for encryption backdoors- is that they are open to manipulation not just by authorised persons but also by malicious actors.

Some argue that we need to circumvent encryption by introducing data processing at the points and times when data is in clear, for example before a file is actually encrypted, or before or after communication is encrypted end-to-end. The intention is clear: to inspect in real time data for different purposes such as the detection of criminal activities or the detection of attacks on IT infrastructure. A recent draft Council Resolution even speaks of "security despite encryption".

From my perspective, two aspects in this policy debate need to be stressed: the need to differentiate, and the need for clear legal framings.

Firstly, in my view, there is no *single* approach for requesting lawful access that can be applied to *every* technology or means of communication. Therefore it makes little sense to argue with absolutist positions, e.g. that "confidentiality of communications can *never* be restricted", or that "law enforcement will be unable to protect the public unless it can obtain access to *all* encrypted data".

Secondly, EU law and in particular the EU Charter of Fundamental Rights require any interferences with fundamental rights to be "provided for by law", in order to guarantee legal certainty and foreseeability, so that we can know who does what and for what reason.

In my recent EDPS Opinion on the EU Commission's proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online, I underlined that measures to detect, remove and report child sexual abuse online must be accompanied by a comprehensive legal framework which meets the requirements of Articles 7 and 8 of the EU Charter of Fundamental Rights. In order to satisfy the requirement of proportionality, the legislation must lay down clear and precise rules governing the scope and application of the measures in question and impose a minimum of safeguards, so that the persons whose personal data is affected have sufficient guarantees that their data will be effectively protected against the risk of abuse.

That legislation must be legally binding and, in particular, must indicate the circumstances and conditions under which the measures for processing such data may be adopted, thereby ensuring that interference is limited to what is strictly necessary. As clarified by the CJEU, the need for such safeguards is greater when personal data is subjected to automated processing

and when the protection of the particular category of personal data means that sensitive data is at stake. This equally applies to encryption-related measures.

I am looking forward to debating this topic during the discussion panel on encryption and effective law enforcement.

Conclusion

Encryption is a critical and irreplaceable technology for effective data protection and privacy. Encryption is as critical to the digital world, as is the physical lock to the physical world.

Privacy, data protection and encryption will help us to build the sort of open, dynamic, respectful digital environment we want for our children and grandchildren. This is even more important after the pandemic crisis.