arm

21 December 2020

European Data Protection Board

RESPONSE TO CONSULTATION ON DRAFT GUIDELINES 01/2020 BY ARM

Arm
110 Fulbourn Road
Cambridge, UK
CB1 9NJ

T +44 (1223) 400 400

E:
minsheng.lu@arm.com

arm.com

1. INTRODUCTION

On 10 November 2020, the European Data Protection Board ("**EDPB**") issued its Draft Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data ("**Recommendations**"). The Recommendations lists several supplementary measures with the aim of ensuring that protection granted to personal data processed in the EEA continues to apply irrespective of where the data is transferred to.[1] The Court of Justice of the EU found in July that to ensure the transfer of data was lawful, according to the GDPR, and consistent with the Charter of Fundamental Rights, it "might be necessary to supplement the guarantees contained"[2] in the standard contractual clauses. The court was silent on what type of supplementary measures controllers should implement.

ARM Limited ("**ARM**") is a large European tech company with establishments all over Europe; the central administration is in the UK. ARM designs microprocessors, physical intellectual property and related technology, software, cloud services and internet of things solutions. ARM was the first company producing chips small enough to fit in a pocket size mobile phone, and later, it created first processors to go into smart phones. To this day, ARM's chips power billions of smart phones and other devices sold around the world, and their innovations have been licenced by companies such as by Apple and Samsung.

ARM would like to submit that hardware-based solutions should be added as a category of supplementary measures. There has been a dramatic development on so-called Confidential Computing in the last years. This has been recognized not only by tech companies, but also by the United Nations[3] and the OECD[4]. Our proposal concerns the fourth step of the Recommendations, namely providing effective protection of personal data processed in a third country through additional measures.

This submission is divided into three parts: In **Section 2**, we will describe how hardware based supplementary

[1] See page 2 of the Recommendations.
[2] CJEU judgment of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, hereinafter C-311/18 (Schrems II), paragraph 132.
[3] Big Data UN Global Working Group, UN Handbook on Privacy-Preserving Computation Techniques (2019), page 41 seqq.
[4] See among others: OECD, Digital Opportunities for Better Agricultural Policies (2019), Chapter 11. Available at: https://www.oecd-ilibrary.org/sites/8e261f09-en/index.html?itemId=/content/component/8e261f09-en

measures work and how they can help to protect data processed in a third country. We will refer to hardware based supplementary measures as Confidential Computing. **Section 3** includes a proposal for an amendment. We conclude by way of a summary of our proposal in **Section 4**.

ARM is happy to answer any questions concerning Confidential Computing and to provide further background.

2. HOW CONFIDENTIAL COMPUTING CAN HELP TO PROTECT PERSONAL DATA

2.1 What is Confidential Computing?

Confidential Computing is the protection of data in use using hardware-based Trusted Execution Environments ("**TEE**"). In computing, data exists in three states: in transit, at rest, and in use.[5] Data is "in transit" if it is for example transferred from a European exporter of data to a non-EEA importer. It is "at rest" if it is stored for example in the third country and it is "in use" if it is processed. Typical technical and organisational measures, like encryption, address only two of the states, namely data at rest and data in transit. To address typical threats to data confidentiality in the third state (data in use), Confidential Computing establishes TEEs that allow a level of assurance of data integrity, data confidentiality and code integrity.

Hardware-based Confidential Computing ensures that unauthorized entities cannot view data while it is in use within the TEE. Naturally, this also prevents unauthorized entities from altering data or replacing data. This makes it an ideal technical measure to protect personal data. Confidential Computing implements fundamental requirements of Privacy by Design and Default such as data minimization and accountability.

2.2 What are the advantages of Confidential Computing?

Confidential Computing provides an additional layer of protection to any data processing. It does not make technical measures based on cryptography obsolete, but it can ensure – depending on the vendor specifications – that particularly sensitive data, for example encryption keys, (but also

[5] For those concepts, see: See: Confidential Computing: Hardware-based trusted execution for applications and data. A publication of the Confidential Computing Consortium. Available at: White Papers - Confidential Computing Foundation.

personal data, sensitive personal data, ML algorithms, or even applications) are protected. This is of relevance when the data at rest is situated in a country outside of the EEA. Confidential Computing can also provide attestation i.e. the ability for one party ("**Verifier**"), to gain confidence in the trustworthiness of the software and data state of another potentially untrusted party (the "**Attester**"). This trust is gained by obtaining an authentic, accurate and timely report of the security claims that guarantee the state of the data, software and hardware, to testify that data has not been tampered with. In a scenario involving international data transfers, European data exporters could demand such proof to ensure that the data was protected end-to-end.

Having the technical measures on a hard-ware level excludes several parties who otherwise might have access to the data, such as operating system providers, device platform operators, peripheral vendors and application and service providers building on top of the product. The less parties with access, the more secure the data . Confidential Computing has been designed for privacy.

2.3 Transfers under Chapter V GDPR: how can Confidential Computing help to ensure an appropriate level of protection of the personal data?

There are many use cases for Confidential Computing. A typical case is cloud computing. In Section 3, we will provide requirements regarding this use case according to the model that the EDPB uses in the Recommendations.

To understand the advantages of Confidential Computing, it is important to know that in a typical cloud scenario, there are many layers which may be targeted for attack: the hardware, the firmware for devices, the OS of the host that operates the system, the hypervisor and also the cloud provider's orchestration system.[6] In a non-adequate country, it is advisable to reduce the number of actors that have access to the data via hardware, privileged administrator access or the hypervisor.

While it is currently not possible on a commercial scale to process encrypted data, i.e. change data fields, add and remove information etc., it is possible to provide a Confidential Computing Environment where the data's

[6] See: Confidential Computing: Hardware-based trusted execution for applications and data. A publication of the Confidential Computing Consortium. Available at: White Papers - Confidential Computing Foundation.

confidentiality is protected even though the data is physically in a public cloud. Confidential Computing aims to allow the removal of even the cloud provider from the chain of trust. It is beneficial for the Cloud provider in this case to be able to use Confidential Computing technology to remove itself and its employees from possibility of coercion and therefore liability.

Other use cases involve processing with multiple parties computing or token storage.

2.4 Is this a technology that can be deployed now?

Confidential Computing is already available and implemented widely in personal devices like smart phones and to some degree also in data centres. There are several vendors such as IBM, Microsoft, Google Cloud Platform and many others that provide such technologies. Confidential Computing and TEEs are mentioned as one privacy-preserving computation technique in the UN Handbook on Privacy-Preserving Computation Techniques[7].

3. PROPOSAL FOR AN AMENDMENT OF THE RECOMMENDATIONS

ARM proposes to add Confidential Computing as one of the Use Cases in Annex 2 of the Recommendations.[8]

Text proposal:

Use Case: Data transfers with Confidential Computing.

A data exporter based in the EU uses a cloud service provider in a third country. The country has not been declared adequate by the Commission. The data of the EU data exporter is hosted in that country.

If

1. The data is encrypted in transition and storage according to use cases 1[9] *and 3*[10]*,*

[7] UN Handbook on Privacy-Preserving Computation Techniques, page 41 seqq.
[8] Recommendations para 69 seqq. and in particular 72-86.
[9] Recommendations para 79.
[10] Recommendations para 84.

*2. The data is brought into a Trusted Execution Environment or other hardware-based measure ensuring confidentiality of processing in use ("**TEE**"),*

3. The vendor provides an audit trail that shows that the data was encrypted entering the TEE,

4. The data is only de-crypted and processed in the TEE and subsequently again encrypted such that it does not exist in a de-crypted form outside of the TEE,

5. Evidence or audit trail shows that the Cloud Service provider cannot access the data in plaintext, nor the key material used for the encryption/decryption;

We also propose adding Confidential Computing in the text of the Recommendations as one of the technical measures employed. This would provide the opportunity to explain the technology, which has multiple use cases and can be used to implement Privacy by Design in the context of international data transfers.

4. CONCLUSION

With the proposed addition of Confidential Computing, the EDPB would recognize a technology neutral measure that completes the trinity of data states: data at rest, in transit and in use. Paired with other privacy-preserving measures, Confidential Computing can protect Personal data from unauthorized access and can provide assurance that the data has not been altered.

Given that contractual measures only provide additional protection, not the protection needed to achieve essentially equivalent guarantees,[11] we are convinced that more guidance on technical measures will be highly appreciated by controllers based in the EU. It is easy for controllers to find guidance on appropriate contractual safeguards, but harder to know which technical measures are appropriate to protect data in the eyes of the regulators. Confidential Computing provides for the "continuity of the high level of protection"[12] under the GDPR to personal data transferred to a third country that the CJEU demanded.

[11] Recommendations, para 93.

[12] Schrems II para 93.

Sincerely,

Michael Lu

Michael Lu
Dir Software Strat. (Security & Privacy)
minsheng.lu@arm.com