Comments on Recommendations 01/2020 of the European Data Protection Board (EDPB)

Duality, Inc. thanks the EDPB for the opportunity to contribute the following comments regarding the EDPB recommendations on measures that supplement data transfer tools to ensure compliance with the EU level of protection of personal data.

Our comments request a clarification to be inserted in Use Case 1, or in a new Use Case. This clarification would state that where personal data are processed in a third country by one or more entities while remaining in fully encrypted form, this too is a permissible data transfer, on condition that the encryption method meets all the encryption conditions in Use Case 1.

This clarification is important to recognize the robust data protection and data security protections afforded by homomorphic encryption technology platforms that are compliant with the homomorphic encryption standard.[1] The clarification would be fully consistent with the intent of draft Guidance.

Duality is a leading provider of Privacy Enhancing Technologies (PETs), enabling organisations to collaborate on personal data or other sensitive data without anyone but the providing controller having unencrypted access to the data. The Duality SecurePlus™ platform offers data science computations over PALISADE, an open source Homomorphic Encryption library. Duality's founding team is comprised from world renowned cryptographers, including Turing Award winner Prof. Shafi Goldwasser, and data science experts.

We enable sharing of data with one or more entities processing the data in a robustly encrypted, fully private manner that protects the data from access by the processors or any other party except for the data controller who encrypts the data.

1. How Homomorphic Encryption Works to Protect Data Robustly in the Context of International Data Transfers

We welcome recognition that supplementary measures may enhance the level of protection afforded to a transfer and that these measures may be of a contractual, technical, or organizational nature. It is also helpful to see the referenced examples in Annex 2.

However, we are concerned that the EDPB recommendation Use Cases present specific examples of compliant technical measures in an overly specific way. They appear to assume that robustly encrypted data can only be stored and that no processing can take place on data that are and remain robustly encrypted. This is not the case, in light of the significant progress

[1] That standard is defined by homomorphicencryption.org in this document: http://homomorphicencryption.org/wp-content/uploads/2018/11/HomomorphicEncryptionStandardv1.1.pdf.

on practical implementations of homomorphic encryption, adhering to the industry standard as defined by the industry standardization body, homomorphicencryption.org with participation of representatives of major corporations, such as Microsoft Intel, Samsung and many others.

Homomorphic encryption standards, as formulated by the HomomorphicEncryption.org industry consortium focus on 1) identifying homomorphic encryption protocols and specific security settings for those protocols so that 2) when those protocols are implemented in software or hardware and the implementations use recommended security settings, the implementations can be used to encrypt data with mathematical security hardness guarantees at least as strong as AES-128. The security parameters can be increased for even higher levels of security, if needed by the controller or the processor.

The standardized protocols adopted by HomomorphicEncryption.org have all been published and widely vetted in the open academic literature. The consortium considers only protocols based on the Ring-LWE hardness properties, which when used with the recommended parameters, makes the protocols quantum safe and resistant even to attacks from quantum computing devices.

Homomorphic encryption supports both processing by a single entity or by multiple entities without those entities *ever* having access to or visibility of personal data in the encrypted format.

Businesses routinely need to transfer personal data to cloud environments located across the Atlantic. In many cases, these transfers are very important for operations in multi-national organizations that operate excellence centers where they conduct data analysis to improve business operations or building or running machine-learning models. Small and Medium Enterprises (SMEs) often need to rely on external expertise in data analysis provided by 3rd parties operating a cloud-based service in another country.

In both the public and private sectors, healthcare research collaborations often need to collect data from medical centers located in EU and elsewhere in the world with the analysis being performed in the US. This research can be impeded by international data transfer restrictions, as has occurred in the context of diabetes and Alzheimer research. https://www.sciencemag.org/news/2019/11/european-data-law-impeding-studies-diabetes-and-alzheimer-s-researchers-warn. It is also true, for example, of transferring personal data regarding tracking long-term protection afforded by and long-term adverse effects of vaccines, such as Covid-19 vaccines.

There are substantial challenges for many controllers in adopting the measures set out in the current version of the recommendations. The last 10 years have seen a major shift in the business IT environment to reliance on externally hosted solutions, as well as the development of agile services delivered by sub-processors. A great many multi-national organizations and SMEs have adopted this infrastructure, which not only stores, but also processes personal data.

Homomorphic encryption enables processing personal data in these environments in a manner that is fully compliant with the *Schrems II* decision.

Recognizing this sub-use case for encrypted data would provide a helpful alternative in some cases that affords a very high level of data protection to personal data so transferred. It would also avoid creating legal uncertainty as to a promising method of data protection and innovation, supporting compliance with GDPR, and assisting small to medium sized EU-based controllers that lack the resources to invest in robust on-premises solutions.

2. Including Any of the Suggested Clarifications Would Advance Data Protection

The EDPB recommendations should not constrain transfers by prescribing the adoption of certain technical measures when other, equally secure measures provide the very same, appropriate level of protection.

By way of example, if an importer can demonstrate to the exporter that the encryption conditions of Use Case 1 are satisfied, then that should permit the data transfer to safely proceed for **processing** in the third country with technical measures in place that ensure full encryption at all time while in the third country. Functionally, the personal data remains fully and robustly encrypted meeting the Use Case 1 conditions. At the same time, the robustly encrypted personal data should also be allowed to be processed, not simply stored.

Homomorphic encryption already works for a range of types of processing, such as various statistical functions and machine learning models. If the processor and the controller agree that the processing can work on homomorphically encrypted data that remains securely encrypted in the third country, the final EDPB Guidance should allow its use. When it is practical, this form of processing addresses fully the data protection concerns that animate both the *Schrems II* decision and the EDPB guidance. It unquestionably deserves recognition in the final guidance as a useful privacy-enhancing technology in the specific context of international transfers.

Similar to multi-party computing, homomorphic encryption supports a broad range of computations without exposing the data during analysis (whether by joint processors or a single processor). However, both methods are not yet a one-size-fits-all solution or a “silver bullet” that solve all practical issues raised by international data transfer restrictions. Nonetheless, there are more than enough use cases to merit recognition of fully encrypted processing as part of the Use Cases in the final guidance.

3. Proposed Clarifications to Recognise Processing of Homomorphically Encrypted Data

Specifically, Duality requests that the final guidance allow processing of robustly encrypted personal data in third countries either by:

(1) expanding Use Case 1 to allow processing as well as storage by encryption that meets the encryption requirements set forth in that use case; or

(2) creating an additional use case 1A or 5A to address processing of robustly encrypted data.

The Specific Amendments that we recommend to the text are as follows:

A. Use Case 1: Data storage for backup, data processing –, and other purposes that do not require access to data in the clear

Amended Use case 1

A data exporter uses a hosting service provider in a third country to store personal data, e.g., for backup purposes or to support processing of personal data.

If

1. the personal data is processed using strong encryption before transmission,

2. the encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis performed by the public authorities in the recipient country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them,

3. the strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved,

4. the encryption algorithm is flawlessly implemented by properly maintained software the conformity of which to the specification of the algorithm chosen has been verified, e.g., by certification -by a recognized expert in cryptography

5. the keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of an intended recipient, and revoked), and

6. the decryption keys are retained solely under the control of the data exporter, or other entities entrusted with this task which reside in the EEA or a third country, territory or one or more specified sectors within a third country, or at an international organisation for which the Commission has established in accordance with Article 45 GDPR that an adequate level of protection is ensured, then the EDPB considers that the encryption performed provides an effective supplementary measure.

B. Alternative: Use Case 1A or 5A

Processing of encrypted data.

The data exporter wishes personal data to be processed by one or more processors without disclosing the content of the data to the processors. Prior to transmission, the data exporter encrypts the data in a robust way such that none of the processors, acting separately or jointly, can access or reconstruct the

personal data. The processors never have access to the decryption keys and must at all times process data while it is encrypted. The data exporter receives the result of the processing from the processors and may decrypt it to arrive at the final result which may constitute personal or aggregated data.

1. the personal data is processed using strong encryption before transmission,

2. the encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis performed by the public authorities in the recipient country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them,

3. the strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved,

4. the encryption algorithm is flawlessly implemented by properly maintained software the conformity of which to the specification of the algorithm chosen has been verified, e.g., by certification by a recognized expert in cryptography,

4. the encryption algorithm is flawlessly implemented by properly maintained software the conformity of which to the specification of the algorithm chosen has been verified, e.g., by certification by a recognized expert in cryptography

an expert,

5. the decryption keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of an intended recipient, and revoked) and are at no time accessible to the processors, and

6. the algorithms used for the computation on encrypted data conform to the state-of-the-art and can be considered secure against active adversaries; The encrypted data remains secure even if all transformed data is collected by a specific adversary

7. the decryption keys are retained solely under the control of the data exporter, or other entities entrusted with this task which reside in the EEA or a third country, territory or one or more specified sectors within a third country, or at an international organisation for which the Commission has established in accordance with Article 45 GDPR that an adequate level of protection is ensured, then the EDPB considers that the encryption performed provides an effective supplementary measure.