European Data Protection Board
Rue Wiertz 60, B-1047 Brussels
edpb@edpb.europa.eu
Submitted via online form at https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en

20 Dec 2020

Dear Sir,

Re: Asia Cloud Computing Association's (ACCA) comments to the European Data Protection Board ("EDPB") on Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data ("Recommendations")

The Asia Cloud Computing Association (ACCA) applauds the EDPB for updating data regulations following the Court of Justice to the European Union (CJEU)'s judgement C311/18 ("Schrems II"),[1] and suggesting updates to supplement transfer tools to provide clarity on how data controllers and processors can be compliant with the EU level of protection of personal data. We appreciate the opportunity to provide feedback on the suggested approach.

As the apex industry association for Asia Pacific stakeholders in the cloud computing ecosystem, the ACCA represents a vendor-neutral voice of the private sector to government and other stakeholders. The ACCA's mission to accelerate the adoption of cloud computing throughout Asia Pacific by helping to create a trusted and compelling market environment, and a safe and consistent regulatory environment for cloud computing products and services. We are committed to enabling the continued free flow of data across borders, ensuring digital resilience, and developing a safe and secure ecosystem where data is protected by the best technology and regulatory frameworks, in support of a better world for all.

We strongly believe that a policy environment conducive to free flow of data will be key in allowing businesses to not only maintain key services to customers, but to also test new services and bring innovations to the market. Following discussions with our member companies, we are submitting our comments to the abovementioned Recommendations. We would be happy to arrange a videoconference call with you to discuss this further.

Thank you, and I look forward to hearing from you on the issues raised.

Yours sincerely,
Lim May-Ann
Executive Director
Asia Cloud Computing Association
mayann@asiacloudcomputing.org

[1] http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=9745404

Asia Cloud Computing Association's (ACCA) comments to the European Data Protection Board ("EDPB") on Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

1. International data flows may be impeded by an overly-restrictive interpretation of the Schrems II ruling

Significant practical and operational challenges will be presented for international data flows and management, if the *Recommendations* are adopted in their current form.

- Practically and operationally, it would create serious obstacles for any organisation that uses an online service to process and transfer personal data—including email, hosted applications, or any other online service—to transfers of personal data to and from the EU.
- Liability-wise, it would also potentially open these organisations to fines of up to 4% of its annual global turnover.
- Compliance cost-wise, EU organisations would be required to conduct their own costly analyses of the laws and practices of the respective non-EU jurisdictions. This is both unrealistic and disproportionate, in particular for small and medium-sized enterprises, research institutions, and others.

Negative impact on international data sharing and collaboration. As a result, the *Recommendations* will make it highly risky for EU companies to engage in commerce with non-EU customers or partners, for researchers to share information with foreign colleagues, for companies with non-EU offices or personnel to communicate with them online, or to engage in other routine operational tasks.

Increasing barrier to trade between EU and non-EU organisations. We are also concerned about the potential distortive effects for trade and competition between third country jurisdictions that have been deemed adequate under the GDPR and those jurisdictions where no such positive adequacy decision is in place. In the case of transacting with non-EU organisations, the Recommendations may end up creating a high barrier to trade between EU and non-EU organisations.

Particularly from the perspective of Asia-Pacific ("APAC"), only Japan and New Zealand have been recognized as adequate. This would create significant challenges, as the process by which a country is recognized as adequacy is a lengthy one – typically two to four years per country. We are therefore concerned that in the absence of an adequacy decision, companies in all other countries in APAC would have be expected to carry out costly and challenging assessments with no legal certainty that such processing of EU Resident data can be done so in compliance with the GDPR.

Contextual approach towards data transfers recommended. The *Recommendations* should instead allow for greater scope to apply a case-by-case basis contextual approach towards data transfers. This contextual circumstance was noted in the *Recommendations* itself; however, the *Recommendations* appear to preclude the possibility of providing such context. E.g. the data importer must use technical measures if they may fall within the scope of certain national security laws, notwithstanding any contextual factors; or even where there is a contextual low likelihood of the public authority accessing the data transferred.

2. The *Recommendations* suggest high technical standards which may not be fit-for-purpose

While illustrative examples, case studies and use cases can be highly instructive, we are concerned that some of these use-cases are confusing, misleading and inaccurate. They draw extreme conclusions from narrow assessments and unhelpfully exclude what could otherwise be considered viable and effective data protection controls:

- Extreme encryption requirements that are too complex to be workable, likely to result in unnecessary cost and increased security risk for EU governments and businesses. [Use Cases 1,3]

- Technical requirements on key mangement that are inconsistent with the normal operation of the internet. [Use Cases 1,3]

- C. Overly restrictive use of encryption as a silver bullet while disregarding alternative technical and organizational controls, and which are misleading and inconsistent with established EDPB guidance. [Use Cases 1,3,6]

- D. Statements that the EDPB "is incapable of envisioning an effective technical measure" highlights the inadequate survey of available technical and organizational methods undertaken in developing the guidance. [Use Case 6,7]

Please see Appendix A where there are selected examples where we have identified technical inaccuracies, to illustrate our broader position on this.

Representing cloud service providers who may be instrumental to ensuring that data can flow between EU and APAC, **our recommendation is that the entirety of the Use Case section be removed from the Guidelines and a forum is established for meaningful consultation, collaboration and co-design of effective guidance while deferring to existing European security assurance schemes for technical aspects relevant specifically to encryption.** Instead, the *Recommendations* should allow space for EU organisations to protect their data with technical solutions which are fit-for-purpose.

Appendix A

A. Extreme encryption requirements that are too complex to be workable, likely to result in unnecessary cost and increased security risk for EU governments and businesses. [Use Cases 1,3]

Issue: The requirements described in Use Case 1 and 3 call for the use of strong encryption technologies to protect data in transmission and at rest. Encryption is an effective mechanism for data protection and appropriate use of encryption is consistent with industry practice, international standards (ISO27001) and European certification schemes (including German C5 and the proposed ENISA CCCS). All of these assurance approaches require the use of appropriate encryption mechanisms that are fit-for-purpose and include mechanisms to verify their integrity.

However, the EDPB guidelines expand the requirement for encryption to a highly specific, narrow and extreme statement of requirement.

- Firstly, Use Case 1 states that "*the encryption algorithm and its parameterisation (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 states*".
- Use Case 3 expands this to include "*effective protection against active and passive attacks*". Both of the Use Cases describe how the encryption must be "*flawlessly implemented and validated* ".

Both use cases describe how "encryption *keys must be managed (generated, administered, stored, if relevant, linked to the identity of an intended recipient, and revoked), and the keys are retained solely under the control of the data exporter, or other entities entrusted with this task which reside in the European Economic Area (EEA) or a third country* ". These are extremely narrow and explicit implementation requirements.

Consequence: Although encryption is a very effective protective control for the security of personal data, the specificity and impracticality of the recommendations could result in significant cost while actually creating the risk of reduced privacy and security protection through unnecessary complexity:

1. Every small enterprise in Europe may need to develop the deep cryptographic expertise to not only understand the interception capabilities of other countries, but then design their applications to apply that expertise to a 'flawless implementation'. The information to perform such an analysis is not readily available, much less the technical expertise in such a highly specialised market. The architecture proposed by the EDPB is only one possible architecture and equally protective security can be achieved in more practical designs.
2. Every small enterprise in Europe may need to acquire and deploy their own on-premise key management hardware, ensure that it is flawlessly implemented and maintained, then ensure that it is securely accessible over the internet.
3. Every small enterprise in Europe may need to replace their encryption technology if at any point a vulnerability is found in the encryption algorithm or protocol, no matter how theoretical or speculative that may be. Such is the consequence of a requirement to be 'flawless' and capable of withstanding unquantifiable nation state capabilities for decryption.
4. As every small enterprise in Europe devotes money and people to these 'flawless' encryption implementations, errors due to poor configuration, lack of expertise or inadequate focus on more pressing areas of information security may lead to heightened real security and privacy risk.

Such a restrictive and explicitly narrow implementation is inconsistent with GDPR Article 32 : “measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected.”

Better Approach: Current best practice is to validate encryption technologies and implementations through industry expertise and information sharing, international standards and the validation practices of schemes including the German C5, ISO audit and the proposed European ENISA Candidate Cybersecurity Certification Scheme (CCCS). Risk assessment is the best way to inform the most appropriate choice for key management and custody, including the right decisions for key generation, control and management. Sole control of key management is one of a range of options, but it comes with a burden of restriction, cost and complexity so the correct choice must always be made for a specific scenario.

Recommendation: We recommend EDPB remove the specific details outlined in Use Case 1 and 3 regarding encryption implementation and replace them with a reference to selecting appropriate encryption approaches validated through risk assessment and schemes like ISO, German C5 and the proposed ENISA CCCS.

B. Technical requirements that are inconsistent with the normal operation of the Internet. [Use Cases 1,3]

Problem: Use Cases 1 and 3 include a requirement that “*the keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of an intended recipient, and revoked), and the 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*”. By corollary, if the United States is not deemed to provide an adequate level of protection, then the generation, administration or storage of keys could not be performed by a US entity.

The majority of encryption keys and digital certificates (a form of key) that are currently in use on the internet, including those that power the secure communication of global and European businesses are generated and administered by a small number of highly trusted providers such as Symantec, Comodo, Let's Encrypt, GlobalSign, DigiCert and Entrust. All of these are US based, but that fact carries no security implication as to their use. The requirement as stated by EDPB would prevent such certificates being generated or used by a European customer.

Transport Layer Security (TLS) encryption in the browser requires a certificate owned by the application provider and issued by a certification authority. The TLS certificate is firstly used to confirm the authenticity of the website. Secondly, session keys are created on the server side (by the company operating the website) and client side (in the browser) to enable encrypted transmission of data. If neither the TLS certificate could be generated by a US-based company nor the session keys could be generated by the application or cloud service provider outside the EEA, then the majority of existing applications on the internet would presently be incapable of meeting the EDPB requirements.

Consequence: Implementing this requirement would require many global and European companies and websites to change their digital certificate provider. This is a costly exercise that could introduce operational disruption and limit the range of certificate providers in use. It would be a complex, costly exercise that provides no security or privacy value, very much contradictory to the balanced guidance of GDPR Article 32.

Better Approach: Key management methodologies and approaches are already addressed within national assurance frameworks like C5 and European frameworks like ENISA CCCS. International standards and practices for key management are also well established and effective. It would be advisable for the EDPB to consult with more thorough consideration to the technical practicalities of these recommendations, or defer to the customers and application/cloud providers with the expertise to implement workable designs.

Recommendation: Requirements for keys to be generated, administered, stored and retained solely under the control of the data exporter should be removed.

C. Overly restrictive use of encryption as a silver bullet while disregarding alternative technical and organizational controls. This is misleading and inconsistent with established EDPB guidance. [Use Cases 1,3,6]

Problem: Use Case 1 describes a scenario whereby private data is stored by a hosting provider in a third country, and identifies the use of strong encryption of the data prior to processing and sole control of the keys to be an effective supplementary control. But Use Case 1 is the only use case in which such a conclusion is reached. Use Case 6 and 7 along with the absence of any other use cases in which any other mechanism of protection suffices, leaves the reader to conclude that the only effective technical control for transfer of data to a third country is for the data to be encrypted before transmission.

The most appropriate approach to use of encryption should be determined from solution architecture and risk assessment rather than arbitrary specification. Indeed, the Privacy-by-Design guidelines published by the EDPB (Guidelines 4/2019 on Article 25 Data Protection by Design and by Default)[2] describe how such an appropriate selection and assessment of controls should be achieved:

> *"Technical and organizational measures and necessary safeguards can be understood in a broad sense as any method or means that a controller may employ in the processing. Being appropriate means that the measures and necessary safeguards should be suited to achieve the intended purpose, i.e. they must implement the data protection principles effectively."*

The technical controls recommended in Use Cases 1 and 3 and lack of other relevant controls in Use Case 6 and 7 in particular demonstrate how the EDPB has not taken into account its own guidance. The inadequate survey of the available technical controls and mechanisms, disregarding for example alternative mechanisms of encryption, access control and obfuscation, is overly simplistic and misleading.

Consequence: By narrowing the consideration of available controls to almost exclusively focus on encryption, the EDPB has disregarded more effective controls. The requirement for example in Use Case 1 to encrypt data prior to transmission and retain sole custody of keys places severe functional limitations on any service that may be used, If all data is encrypted then the ability to index, search or automatically process data is not possible. it would result in additional complexity and cost for the data exporter and as a result even introduce additional security risk.

Better Approach: Access control restrictions can prevent cloud service operators from even accessing data, even if it is processed by systems within secure enclaves. Obfuscation techniques such as masking can ensure data can be safely masked prior to transmission and processing -

[2] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en

encryption as described in Use Case 1 is not the only mechanism for masking. Transparent data encryption approaches can effectively create a secure mechanism for a data exporter to expose unencrypted data on demand to applications only under their control, while the data is maintained in encrypted form to any external party. There are numerous other controls and design approaches that can be applied based on the specific use case and architecture, each of which can provide effective risk mitigations but there is no indication in the Guidelines that these have been considered.

Recommendation: The EDPB should remove the narrow and specific technical implementation details in Use Case 1, 6 and 7 and engage in a structured consultation with experts in cloud computing services to develop guidance that is both consistent with existing guidance (such as EDPB Guidelines 4/2019) and enable fit-for-purpose choice by data exporters.

D. Statements that the EDPB "is incapable of envisioning an effective technical measure" highlights the inadequate survey of available technical and organizational methods undertaken in developing the guidance. [Use Case 6,7]

Problem: Use Case 6 is written in the context of potential access to unencrypted data in a third country indicating that the "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. The EDPB does not rule out that further technological development may offer measures that achieve the intended business purposes, without requiring access in the clear.

In the given scenarios, where unencrypted personal data is technically necessary for the provision of the service by the processor, transport encryption and data-at-rest encryption even taken together, do not constitute a supplementary measure that ensures an essentially equivalent level of protection if the data importer is in possession of the cryptographic key". Processing of unencrypted data is not the same as access to unencrypted data, and although computer science is advancing on approaches to enable processing of encrypted data, it is not yet state-of-the-art.

It is however unclear from the guidelines if the EDPB has undertaken any substantive assessment of technical and operational controls that could prove appropriate and effective. A singularly narrow focus on encryption is not an adequate assessment. For example, EDPB do not appear to have considered a number of existing viable and proven practices that include:

- Use of administrative pre-authorisation controls, whereby a customer's explicit authorisation is required by an administrator before any administrative access is performed;
- Use of automated scripts to perform administrative action on customer data, whereby the scripts can perform restricted actions without any actual human access;
- Use of cryptographic techniques with Cloud Hardware Security Modules whereby access is granted by the customer to a process that decrypts and acts on the customer data, but only under their control;
- Use of split-key or dual-key encryption approaches whereby a key managed by the cloud provider and a key managed by the customer need to be simultaneously provided to enable processing of data;
- Use of transparent data encryption techniques on database systems whereby administration and management of the database configuration can be performed by an administrator, but specific content can remain encrypted and only available to the customer in a decrypted form.
- Use of automated auditing and reporting of operations on customer data as a detective control

- Use of hardware separation to systematically limit administrative access and segregate virtualisation from the underlying hardware platform
- Use of hardware-enforced secure enclaves for segmentation of encrypted and unencrypted processing.

Consequence: By exclusively focusing on a very narrowly defined encryption approach and disregarding all other viable mechanisms of technical and organizational control, the EDPB have reached an incorrect and misleading conclusion. The consequence of this error could be far-reaching for European enterprises and governments severely restricting their ability to innovate, introducing significant cost and risk. Protection of private data is achieved through a range of controls selected for both appropriateness and effectiveness, fit-for-purpose.

Better Approach: The EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (DPbDD) state:

> *The core obligation is the implementation of appropriate measures and necessary safeguards that provide effective implementation of the data protection principles and, consequentially, data subjects' rights and freedoms by design and by default. Article 25 prescribes both design and default elements that should be taken into account. Those elements, will be further elaborated in these Guidelines.*
>
> *Article 25(1) stipulates that controllers should consider DPbDD early on when they plan a new processing operation. Controllers shall implement DPbDD before processing, and also continually at the time of processing, by regularly reviewing the effectiveness of the chosen measures and safeguards. DPbDD also applies to existing systems that are processing personal data.*
>
> *The Guidelines also contain guidance on how to effectively implement the data protection principles in Article 5, listing key design and default elements as well as practical cases for illustration. The controller should consider the appropriateness of the suggested measures in the context of the particular processing in question"*

Yet this identification of appropriate, necessary and effective controls has been narrowed in the proposed recommendations to a single control: data encryption with the data exporter as the sole controller of keys. All other controls appear to have been disregarded. A better approach would be to comprehensively survey and understand the broad range of effective technical and organizational controls available in consulting with industry leading customers.

Recommendation: We recommend Use Case 6 is removed from the Guidelines as a misleading and inadequate survey of available controls. Instead, we would recommend the EDPB survey and consult in a more comprehensive manner to identify and evaluate the range of controls that do offer appropriate protections and are already incorporated in such approaches as the CISPE Code of Conduct.[3]

[3] https://cispe.cloud/code-of-conduct/