ohpen

European Data Protection Board
Rue Wiertz 60
B – 1047 BRUSSELS
Belgium

Subject: Public Consultation on Guidelines 05/2021 Date: 2022-01-20

Dear Sir/Madam,

Introduction

On 18 November 2021 the European Data Protection Board (**"EDPB"**) released Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR (**"Guidelines"**) for consultation. Ohpen welcomes the opportunity to share its views on the Guidelines.

Ohpen is a cloud-native core-banking platform that powers savings, investment, mortgage, loan, and pension products for its clients. We are headquartered in Amsterdam with offices in Barcelona, London, Antwerp, Bratislava and Zilina. We were the first cloud service provider (**"CSP"**) in the world to utilise cloud technology for banking services, providing us with over ten years of first-hand experience with delivering cloud services. As a business-to-business CSP working in the financial services sector, data protection is a key focus for us and our clients. We recognise the importance of data protection in building and maintaining trust with clients and the individuals whose personal data we process, including our clients' customers and third party providers. As part of ensuring our compliance programme is effectively meeting the needs of our clients and compliant with applicable data protection laws, we regularly turn to the latest EDPB guidelines and recommendations as a useful source of additional guidance on the practical application of certain GDPR requirements.

In reviewing the Guidelines, we welcome the clarifications the EDPB has sought to make with respect to the interpretation of "transfer of personal data to a third country or to an international organisation". However, as currently drafted, the Guidelines suggest an interpretation that does not align with the text of the GDPR, the underlying policy rationale for the introduction of those provisions, or the interpretation of those provisions by the Courts. This risks introducing additional ambiguity regarding the interpretation and application of those provisions that doesn't exist today.

Background

CSPs based in the European Economic Area (**"EEA"**) frequently utilise the services of US-owned cloud infrastructure providers (**"CIPs"**) such as Amazon Web Services (**"AWS"**), Microsoft and Google Cloud to deliver their services. To assist their clients with ensuring data is not transferred outside the EU, many US-owned CIPs offer to ring-fence data to EEA availability zones. This offering is commonly adopted by EU-based CSPs as a way of keeping personal data within the EEA so as to avoid a transfer of personal data to a third

Ohpen Services B.V. | Rokin 111 | 1012 KN Amsterdam | The Netherlands | + 31 (0)20 722 1000
info@ohpen.com | www.ohpen.com | CoC Amsterdam 54158311 | IBAN NL72 INGB 0653 1626 77 | VAT NL8511.98.284.B.01

country. We view this processing activity as falling outside the scope of the international transfer obligations set out in Chapter V of the GDPR as there is no transfer of data outside of the EEA. This view is shared by data protection professionals around the globe and aligns with the interpretation of Conseil d'État in their recent ruling on the use of AWS by a service provider engaged by the French Ministry of Health[1].

However, the "criteria to qualify a processing as a transfer of personal data to a third country or to an international organisation" set out in paragraph 7 of the Guidelines is drafted in such a way that may reasonably be interpreted to include processing in the EEA within the scope of an international transfer by virtue of a CIP being established in a third country.

The criteria that qualify a processing as a transfer set out in paragraph 7 of the Guidelines are (emphasis added):

1. A controller or a processor is subject to the GDPR for the given processing.
2. This controller or processor ("exporter") discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor ("importer").
3. **The importer is in a third country** or is an international organisation, irrespective of whether or not this importer is subject to the GDPR in respect of the given processing in accordance with Article 3.

In the situation of an EEA-based CSP engaging a US-owned CIP, each of the cumulative criteria set out above can be read to be satisfied if you take a plain language reading of the emboldened section of point 3 (i.e. the EEA-based CSP has transferred data to a US-owned CIP, who is in a third country). This criteria would suggest that an international transfer may occur in a situation in which personal data never leaves the EEA and cannot be accessed from outside the EEA.

We do not think the Guidelines are intended to treat the example of an EEA-based CSP transferring personal data to a US-owned CIP as an international transfer when the personal data remains within the EEA. This does not align with the intent of the provision, the European Commission's interpretation of what constitutes an international transfer[2] or with the recent post-*Schrems ii* ruling of the Conseil d'État[3].

This outcome would also lead to absurdities when the controller sought to undertake a Transfer Impact Assessment to assess the risks of the proposed "international transfer" given consideration of many of the local requirements in the third country would be irrelevant in light of the fact the data would never leave the EEA.

As highlighted within the Guidelines, in the example set out above the controller would still be subject to Article 32 of the GDPR, requiring it to ensure appropriate safeguards are in place to protect the personal data. This would include consideration of, among other things, the fact that the processor is US-owned and may be subject to laws on government access to personal data that go beyond what is necessary and proportionate

[1] https://www.conseil-etat.fr/en/news/the-urgent-applications-judge-does-not-suspend-the-partnership-between-the-ministry-of-health-and-doctolib-for-the-management-of-covid-19-vaccinati

[2] "When personal data is transferred outside the European Economic Area, special safeguards are foreseen to ensure that **the protection travels with the data**." (emphasis added). https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_en

[3] https://www.conseil-etat.fr/en/news/the-urgent-applications-judge-does-not-suspend-the-partnership-between-the-ministry-of-health-and-doctolib-for-the-management-of-covid-19-vaccinati

in a democratic society. This is an appropriate mechanism for ensuring the personal data is adequately protected in the context of these types of controller/processor relationships.

Recommendation

We recommend that the EDPB amends the criteria set out in paragraph 7 of the Guidelines to clarify that data must leave the EEA to be considered an international transfer.

This amendment will avoid the ambiguity the current Guidelines are likely to introduce, whereby CSPs that have made a concerted decision to store personal data within the EEA may be deemed to have undertaken an international data transfer solely by virtue of the fact that the CIP providing those EEA-based hosting services happens to be located in a third country.

Best regards,

Jan Verberne
Data Protection Officer