Ministry of Justice and Security

> Return address Postbus 20301 2500 EH The Hague

European Data Protection Board

Information Management and Procurement Department

Turfmarkt 147
2511 DP The Hague
Postbus 20301
2500 EH The Hague
www.rijksoverheid.nl/jenv

Contact
Paul van den Berg

T 070 370 79 11

Project name
EDP consultation

Our reference
3119592

Your reference
Public consultation reference R01/2020

Please quote date of letter and our ref. when replying. Do not raise more than one subject per letter.

Date 8 December 2020
Concerning Contribution to the consultation by EDPB on the measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

Introduction

The Dutch Ministry of Justice and Security/ Strategic Vendor Management Hyperscalers is grateful for the opportunity to contribute to the guidance given by the EDPB in its new *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*.[1] We would like to raise specific and practical questions regarding the application of the guidance to systematic transfers of personal data to globally operating cloud service providers headquartered in the USA.

We open with a summary of our recommendations to the EDPB. The proposals follow from our analysis whether current US law unjustifiably interferes with the data protection and privacy rights recognised by the Charter, based on the updated EDPB guidance on the European Essential Guarantees[2], and the *Schrems II* ruling.[3]

Subsequently, we describe our insights about the new EDPB guidance on technical measures on the systematic transfers of personal data to Microsoft in the USA. We hope the EDPB can use this analysis to make the guidance more easily applicable in the practice of ongoing data transfers to the USA.

[1] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Consultation version adopted on 10 November 2020, Consultation between 11 November and 21 December 2020, URL: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

[2] EDPB, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, Adopted on 10 November 2020, URL: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf

[3] CJEU judgment of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, case C-311/18, ECLI:EU:C:2020:559 (hereinafter: *Schrems II*)

Summary of recommendations

1. Provide a clear and specific assessment of the adequacy of the guarantees provided by the legal regime in the USA concerning both law enforcement powers and surveillance measures when data are transferred based on Article 46 of the GDPR (such as the (soon to be updated) SCC and Binding Corporate Rules).
2. Work with the European Commission to ensure that the burden of compliance with the essential European guarantees rests on the importing cloud providers in third countries, in particular in the USA. The EDPB now gives a soft organisational recommendation that importers should provide an overview of the applicable relevant surveillance laws and other sources of information about access by public authorities. These recommendations should be a legal requirement, for example, in the updated SCC from the European Commission.
3. Recognise other technical measures that may enormously reduce the impact of transfers of personal data to countries without an adequate data protection level. We suggest the following measures:
    - Enable users and admins to minimise the collection of Diagnostic Data and Website/Cookie Data;
    - Allow for the creation of pseudonymous accounts, where the data controller only holds the identifying data through, for example, Single Sign-On.
    - Ensure that data controllers can fulfil data subject access rights by granting full access to all personal data that cloud providers collect in their role as data processor through an Admin Console;
    - Minimise the retention periods of personal data, especially the pseudonymised data collected as Diagnostic and Website Data;
    - Organise independent annual privacy audits on specific compliance with the rules on access to the different categories of personal data within the recipient company and its subprocessors, and compliance with the contractually agreed purpose limitation rules
4. Issue pro-active, dynamic, up to date guidance to public and private sector organisations in the EU about the justifiability of transfers of personal data to the top-10 of most frequently used specific productivity, hosting/Virtual Machines and communication cloud services offered by US-based companies.
5. Ask the European Commission to create a new European supervisory body., based on a new separate Regulation, with its investigation and supervision powers, dedicated to the supervision of data protection compliance of the globally operating cloud service providers.
6. Promote long term structural compliance of the US cloud providers with the European data protection standards. Develop a strategy with the European Commission, the European Parliament, the Council of Ministers, and a representative group of globally operating cloud providers to create secure EU data havens.

About SLM Microsoft Rijk

We, as Strategic Vendor Manager Microsoft for the Dutch government. SLM Microsoft Rijk fulfils a crucial role in the public procurement of software products and services for all approximately 300.000 civil servants employed by the central Dutch government and the agencies and organisations that are part of the central government. We started to commission DPIA reports in the summer of 2018. Although we are not a data controller ourselves, we commissioned those DPIAs to

ensure we procure GDPR-compliant products and services for the Dutch government organisations. In practice, this often requires negotiations about technical and legal improvements. Since the fall of 2018, we have published extensive DPIA reports on the main website of the Dutch government.[4] We have studied the role of Microsoft as the provider of the Enterprise versions of Microsoft Office (locally installed and as cloud software), of Microsoft Windows, of Microsoft Intune, and the role of Microsoft as the provider of data transfer and storage services (Microsoft Exchange Online, SharePoint, OneDrive and Azure). Our role as a procurement department is not limited to Microsoft. We have also commissioned DPIA reports on G Suite Enterprise and G Suite Enterprise for Education, Amazon Web Services VM and database services, and the Zoom videoconferencing services. Besides, we are closely involved with the DPIA conducted by our colleagues from the Ministry of Economic Affairs on Oracle cloud services.

Guidance on the European Essential Guarantees

In its recent *Recommendations on the European Essential Guarantees for surveillance measures,*[5] the EDPB provides an updated explanation of the four European essential guarantees that make limitations to the data protection and privacy rights as recognised by the Charter justifiable. These four guarantees are:

1. Processing should be based on clear, precise, and accessible rules
2. Necessity and proportionality concerning the legitimate objectives pursued need to be demonstrated
3. An independent oversight mechanism should exist
4. Effective remedies need to be available to the individual

Data controllers and Data Protection Authorities should equally apply these criteria to test whether the surveillance measures in a third country can be regarded as justifiable interference. These criteria are essential guarantees, the EDPB adds, but not sufficient by itself to determine whether the legal regime of the third country offers an essentially equivalent level of protection.

We do not underestimate the difficulty of assessing the legal regime in countries like, for example, India, China, Philippines, South Africa, or the Ukraine where a cloud provider may operate a service desk. However, in this contribution, we only focus on the US American legal regime. It follows from the *Schrems II* ruling from the European Court of Justice[6] and the explanation of the EDPB that the current legal regime in the USA does not meet these four criteria, for the following reasons:

[4] See: https://www.rijksoverheid.nl/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise and https://www.rijksoverheid.nl/documenten/publicaties/2018/11/12/strategisch-leveranciersmanagement-microsoft-rijk-slm-microsoft

[5] EDPB, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

[6] CJEU judgment of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, case C-311/18, ECLI:EU:C:2020:559 (hereinafter: *Schrems II*)

1. FISA Section 702 and EOP 12333 do not indicate limitations on the powers they confer to implement surveillance programmes for the purposes of foreign intelligence.[7]
2. US laws permit public authorities to have access on a generalised basis to the content of electronic communications. This must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.[8]
3. The scope of the supervisory role of the oversight mechanism by the US Ombudsman does not cover the individual surveillance measures.[9] It is doubtful whether the US Ombudsman meets the other elements for independence defined by the European Court of Human Rights in its jurisprudence about surveillance measures, such as independence from the executive, being vested with sufficient powers and competence and whether its activities are open to public scrutiny.[10]
4. Closely related to the third guarantee, data subjects from the EU whose data are transferred to the USA cannot bring legal action before an independent and impartial court in order to have access to their personal data, or to obtain the rectification or erasure of such data.[11]

Additional measures to ensure compliance with the EU level of protection of personal data

Many data controllers in the EU use the services of USA-based cloud providers for daily productivity and communication tasks. Though data controllers in the EU frequently have the option to store the so-called Customer Content Data in datacentres in the EU, not all cloud providers offer such an option. Where available, such geolocation choices only apply to *data at rest*, not to *data in transit*. More importantly, most globally operating cloud providers systematically process other categories of personal data on their own servers in the USA, or in other third countries in the case of 24/7 Support Services. Such other categories of data are: Account Data, Contact Data, Authentication/License verification Data, Financial Data, Support Data, Diagnostic Data (including telemetry data) and Website/Cookie Data. For a better understanding of these terms, we refer to our contribution to the consultation by the EDPB on the concepts of controller and processor in the GDPR. [12]

As the EDPB writes, quoting the CJEU in *Schrems II*, data exporters in the EU must verify, on a case-by-case basis and, where appropriate, in collaboration with the importer of the data, whether the law of the third country of destination ensures an essentially equivalent level of protection, under EU law, of personal data transferred according to standard data protection clauses, by providing,

[7] EDPB Recommendations on the European Essential Guarantees, par. 36. *Schrems II*, par. 180.

[8] Idem, par. 37, with reference to the CJEU judgment of 6 October 2015, Maximillian Schrems v Data Protection Commissioner, Case C-362/14, EU:C:2015:650 (*Schrems I*), par. 94.

[9] Idem, par.40. *Schrems II* par. 179.

[10] Idem, par. 42.

[11] Idem, par. 47. *Schrems I*, par. 194. Schrems II, par. 196.

[12] Dutch Ministry of Justice and Security, Contribution to consultation by EDPB on the concepts of controller and processor in the GDPR, 13 October 2020, URL: https://edpb.europa.eu/sites/edpb/files/webform/public_consultation_reply/input_slm_on_public_consultation_07-2020_edpb_-_controller_vs_processor.pdf

where necessary, supplementary measures to those offered by those clauses.[13] According to the EDPB, data controllers must perform this verification repeatedly. This puts an even higher burden on controllers, while it is unclear how frequent this exercise has to be completed.

The draft EDPB guidance provides the following measures and steps.

Document what personal data are transferred, based on what transfer tools. This is a self-evident step. Assess the circumstances of the transfer. We recommend the EDPB adds that this analysis must focus on the role of the cloud provider as a data processor. To mitigate possible risks of further processing of personal data for unauthorised purposes, the cloud provider may only

1. Process the personal data for a few specific and legitimate purposes defined the data controllers assess the impact of rules of a general nature on the fundamental rights of individuals.

This step is problematic. As analysed by the European Court of Justice, in the USA there is no, or only a minimal right of redress for the data subject whose personal data are accessed by public authorities, if the data subject is ever made aware at all.

2. Assess the impact of specific laws with requirements to disclose personal data to public authorities or to grant such public authorities powers of access to personal data.

As noted above, such problematic laws in the USA apply to many globally operating cloud service providers, specifically Section 702 of the US FISA and EOP 12 333.

3. Assess other relevant aspects of the legal system in the recipient country. These circumstances are:
    a. Effective mechanisms for individuals from the EU to obtain (judicial) redress against unlawful government access to personal data
    b. The existence of a comprehensive data protection law or an independent data protection authority
    c. Adherence to international instruments providing for data protection safeguards.

On the foot of the *Schrems II* ruling, the USA currently does not meet these three mitigating circumstances. There are only sectoral and regional laws, and there is no dedicated omnibus data protection authority. The USA are a member of the Organization for Economic Co-operation and Development (OECD). The OECD Privacy Guidelines, last updated in 2013, constitute a non-binding (voluntary compliance) international privacy framework.

[13] EDPB, EDPB Recommendations on the European Essential Guarantees, consideration 5 and par. 5.

d. Identify supplementary technical measures. The EDPB specifically mentions five technical measures:

1. Strong encryption of *data at rest*, with the keys retained solely under the control of the data exporter.

However logical this seems; this solution is not available in practice. Most cloud providers offer encryption services for the *data at rest*, but they still have access to the encryption keys, by virtue of their hosting of the keys created by the customer. Many personal data fall outside of the protection offered by encryption with a customer key, such as User-Account Data, log files and remote telemetry data collected as Diagnostic Data. Microsoft, for example, offers encryption tools such as *Customer Lockbox* and *Customer Key*. *Customer Lockbox* is a feature that helps to explicitly regulate access to document contents by Microsoft support engineers in Office 365. The customer can authorise access for limited time frames and specific purposes. *Customer Key* is a feature for Office 365 that allows customers to control encryption keys for the encryption of data at rest. Microsoft still has access to the key when processing data. This feature reduces the opportunities Microsoft must access customer data but does not eliminate them. In response to Schrems II and the EDPB guidance, Microsoft will update its encryption offer with a double key. The requirement mentioned by the EDPB in use case 3, under 10, for a data exporter to rule out the existence of backdoors in hardware or software seems to create an insurmountable hurdle. To comply with this requirement, a data controller must evaluate the hardware used by the cloud-provider, attest remotely that no deviating hardware is used and audit every single software update in the cloud environment and *on premises* (own hardware, including backdoors in any mobile apps). Specific analysis from the EDPB is urgently needed whether this new Microsoft solution and encryption solutions adopted by other cloud providers would meet this threshold from the EDPB for key ownership.

2. Pseudonymisation, with the identifying data held exclusively by the data exporter.

Again, this seems to be a theoretical measure, as most cloud providers will process Account Data, Contact Data and License Verification Data on their servers in the USA. Therefore, even if they only process pseudonymised data when they transfer Diagnostic Data to the USA, they can never meet this threshold of not being able to identify or single out the individuals. As the EDPB also correctly remarks, this division of data is even more unlikely if the cloud provider also engages in behavioural advertising. It follows from the Snowden revelations that secret services have used unique, pseudonymous, identifiers from tracking cookies to single out and trace individuals.[14]

3. Encryption of *data in transit* through third countries

Since the Snowden revelations, this type of encryption should be universally applied by the globally operating cloud providers, and thus, this technical measure should be easy to comply with.

[14] See for example The Washington Post, NSA uses Google cookies to pinpoint targets for hacking, 11 December 2013, URL: https://www.washingtonpost.com/news/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/

4. Export to a recipient with professional privilege

This is not an option for data controllers when they use any of the globally operating providers of productivity, communication, and data hosting services. Realistically, a data controller in the EU can only determine (by organisational measure), that cloud providers may not process certain kinds of classified or sensitive data without additional encryption.

5. Splitting the data into non-identifiable elements for two or more recipients

This is not an option when using common cloud productivity, communication, and hosting services, because such a data splitting service is not offered by any of the top 10 globally operating cloud service providers headquartered in the USA that are commonly used by most private and public sector organisations in the EU.

e. Identify organisational supplementary measures.

The EDPB provides a long list of organisational measures that the contract could contain. Based on our contracting practice, we particularly value the transparency requirements and look for a track record of legal resistance against orders to hand-over personal data. We think some of the measures now listed as 'organisational', should, be qualified as 'hard' technical measures, specifically data minimisation and audits. In our opinion, cloud providers in the USA should commit to the following technical measures to minimise the impact of possible unauthorised access to the data for surveillance or law enforcement purposes. These additional measures are:

- Enable users and admins to minimise the collection of Diagnostic Data and Website/Cookie Data;
- Allow for the creation of pseudonymous accounts, where the data controller only holds the identifying data through for example Single Sign-On
- Ensure the data controllers can fulfil data subject access rights by granting full access to all personal data the cloud providers collect in their role as data processor through an Admin Console;
- Minimise the retention periods of pseudonymised data;
- Organise independent annual privacy audits on specific compliance with the rules on access to the different categories of personal data within the recipient company and its sub processors and compliance with the contractually agreed purpose limitation rules.

Recommendations

1. **Provide a clear and specific assessment of the adequacy of the guarantees provided by the legal regime in the USA concerning both law enforcement powers and surveillance measures when data are transferred based on Article 46 of the GDPR.** The EDPB should perform this task. It is not realistic and disproportionate to require such a highly complex analysis from all individual data controllers in the EU. The conclusion that data controllers should stop the transfer if they conclude the legislation in the recipient country does not offer the required level of protection is not very realistic in practice either. Often, there are no realistically deployable, non-cloud, equivalents for most

widely used productivity and communication services, including the tools for videoconferencing software which is highly in demand since the outbreak of the Covid pandemic.

2. Work with the European Commission to **ensure that the burden of compliance with the essential European guarantees rests on the importing cloud providers in third countries**, in particular in the USA. Recital 108 of the GDPR and the CJEU put the burden on exporters to verify, on a case-by-case basis and, where appropriate, in collaboration with the importer in the third country, if the law or practice of the third country impinges on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools. But it is unrealistic to ask public and private sector organisations to each make their own analysis of the complicated legal surveillance rules in the (many) recipient countries outside of the EU. Surveillance legislation is notoriously undocumented and often untested in public court cases, even in the best-case scenario that jurisprudence is made publicly available in a searchable format. The EDPB now recommends that importers should provide an overview of the applicable relevant surveillance laws and other sources of information about access by public authorities. This should be a hard legal requirement, for example, in the new SCC from the European Commission.
3. **Recognise and recommend other technical measures that should be taken by importing cloud providers**. These measures may strongly reduce the impact of transfers of personal data to countries without an adequate data protection level and thus provide a pragmatic solution to ensure little or no infringement on the fundamental rights of data subjects in the EU. We suggest the following measures:
    - Enable users and admins to minimise the collection of Diagnostic Data and Website/Cookie Data;
    - Allow for the creation of pseudonymous accounts, where the data controller only holds the identifying data through for example Single Sign-On
    - Ensure the data controllers can fulfil data subject access rights by granting full access to all personal data the cloud providers collect in their role as data processor through an Admin Console;
    - Minimise the retention periods of pseudonymised data;
    - Organise independent annual privacy audits on specific compliance with the rules on access to the different categories of personal data within the recipient company and its subprocessors and compliance with the contractually agreed purpose limitation rules
4. **Issue pro-active, dynamic, up to date guidance** to public and private sector organisations in the EU **about the justifiability of transfers of personal data to the top-of most frequently used specific productivity, hosting/VM and communication cloud services offered by US-based companies**. Explain the necessary mitigating measures for each of these particular services: how data controllers should use technical measures to justify ongoing systematic transfers. This could for example, include an analysis of the new encryption tool offered by Microsoft, and potentially, also of encryption tools developed by other cloud providers.
5. **Bundle technical knowledge and enforcement powers in a new European supervisory body**.

It appears that the EDPB currently relies on guidance developed as a result of inspections or responses to complaints from individual National Supervisory Authorities. This implies a relatively passive role for the EDPB, to coordinate potentially conflicting points of view. Such analysis should however, not be left to individual authorities, in our opinion, but should be performed centrally. We think it is inefficient for national NSAs to each spend a considerable amount of their scarce technical capacity on analysing global cloud services. This could be done much more efficiently by asking the European Commission to create a new European supervisory body., based on a new separate Regulation, with its own investigation and supervision powers, dedicated to the supervision of data protection compliance of globally operating cloud service providers. The GDPR harmonisation model with the lead supervisory authority has created an insurmountable burden for the Irish Data Protection Commissioner. In practice, the different NSAs issue their own guidance, without waiting for enforcement by the lead NSA and subsequent coordination by the EDPB. In practice, we already note critical differences in the analysis of the GDPR compliance of cloud video conferencing software by the Dutch and by the Berlin data protection authorities.[15] This puts data controllers in an undesirable position between a rock and a hard place.

6. **Promote long term structural compliance of the US cloud providers with the European data protection standards**. Develop a strategy with the European Commission, the European Parliament, the Council of Ministers, and a representative group of globally operating cloud providers to create secure EU data havens. This could be aligned with initiatives such as GAIA-X.[16]

Kind regards,

Paul van den Berg

[15] Dutch DPA table with guidance about video conferencing software, URL: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/keuzehulp_privacy_videobellen_versie_2.pdf , URL: Berlin DPA analysis video conferencing software, URL: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf

[16] See: https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html