Handling data transfers in a changing landscape

Although privacy has long been a discussion point within technology, its role in the use of Cloud services has not always demanded close attention. This changed in 2020, when the Schrems II ruling invalidated Privacy Shield. As a result, companies who relied on Privacy Shield for data transfers to the U.S., including the use of Cloud services, are now non-compliant and must take action. In this article, we will take a closer look at the impact of the ruling, and steps that organizations can take to manage the consequences.

Laura Huijts LL.M. CIPP/E CIPM CIPT
is a senior consultant at the Cyber & Data Privacy Department of KPMG Advisory N.V.
huijts.laura@kpmg.nl

Daniela Gonzalez Riedel CIPP/E
is a senior consultant within the Cyber & Data Privacy Department of KPMG Advisory N.V.
gonzalezriedel.daniela@kpmg.nl

In short: Privacy Shield is now invalid

INTRODUCTION

In the Schrems II case of July 2020, the European Court of Justice ruled that the Privacy Shield is no longer a valid means of transferring personal data to the U.S. The important players in the cloud services domain, like Amazon, Microsoft, Google and IBM are, however, based in the U.S. In most cases it is not a realistic option to look for alternative cloud services outside of the U.S. That does not mean it ends there. For example, it is important to consider the level of encryption and the existence of model contracts. In this article we gathered important considerations that every organization should take into account when using a US-based Cloud provider where data is transferred to or accessed from the US.

Organizations that are based in the EU/EEA and that have data exchanges with companies outside of the EU/EEA, have to meet new EU requirements that require the revision of contracts, the performance of additional jurisdiction analysis and the implementation of measures to mitigate the gaps.

What?
Stricter requirements for companies engaging in data exchanges with third parties or recipients outside of the EU/EEA, following from the Schrems II judgement.

Impact
Contract revisions and remediating actions are required.

Timeline
The ruling of the Central European Court of Justice (CJEU) took place on the 16th of July 2020, invalidating Privacy Shield with immediate, and retroactive, effect.

Fines
As non-compliance would result in non-compliance with GDPR, fines of up to 4% of annual revenue, or 20 million euros, are possible.

Scope
EU-US data transfers (including access to data) which were reliant on Privacy Shield as their transfer mechanism.

A BRIEF OVERVIEW OF THE CONTEXT

What was the Privacy Shield?

In some countries outside the European Union (EU) there are no or less stringent privacy laws and regulations in comparison to those of the EU. In order to enable the same level of protection for EU citizens, the General Data Protection Regulation (GDPR) rules that personal data cannot be transferred to persons or organizations outside of the EU, for example the US, unless there are adequate measures in place. In this manner, the GDPR ensures that personal data of EU citizens are also protected outside the EU. Organizations can only transfer personal data outside of the EU to so-called 'third countries' when there is an adequate level of protection, comparable to that of the EU.

The US does not offer a comparable level of protection, because there is no general privacy law. Because organizations in the EU transfer personal data on a large scale and on a daily basis to the US, a new data treaty was adopted in 2016 – the Privacy Shield (successor of Safe Harbour). Under the Privacy Shield, US-based organizations could certify themselves, claiming they complied with all privacy requirements deriving from GDPR.

What happened in the Schrems II case?

The Schrems II case owes its name to Max Schrems, an Austrian lawyer and privacy activist who put the case forward. He was already known from the Schrems I case in 2015, in which the European Court of Justice declared that Safe Harbour (the predecessor of Privacy Shield) was no longer valid. The same fate now hits the Privacy Shield.

In the Schrems II case, Max Schrems filed a complaint against Facebook Ireland (EU), because they transferred his personal data to servers of Facebook Inc., which are located in the US. Facebook transferred this data on the basis of the Privacy Shield. Schrems' complaint was, however, that the Privacy Shield offered insufficient protection. According to American law, Facebook Inc. is obliged to make personal data from the EU available to the American authorities, such as the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI).

In the Schrems II case, the Court investigated the level of protection in the US. Important criteria are the existence of 'adequate safeguards' and if privacy laws of EU citizens are 'effective and enforceable'. The Court concluded that under American law, it cannot be prevented that intelligence agencies use personal data of EU citizens, even when this is not strictly necessary. The only legal safeguard that the US offers, is that the intelligence activities need to be 'as tailored as feasible'. The Court ruled that the US is processing personal data of EU citizens on a large-scale, without offering an adequate level of protection. The Court also ruled that European citizens do not have the same legal access as American citizens. The activities of the NSA are not subject to judicial supervision, and there is no means to appeal it. The Privacy shield ombudsman for EU citizens is not a court and does not offer adequate enforceable protection. In short: Privacy Shield is now invalid.

This ruling has far-reaching consequences, given that a large number of EU based companies using cloud providers use a US-based provider. It is important to note that the liability rests on the organization who "owns" the data and exports it, not on the Cloud Provider. Therefore, it is critical that measures are taken so that running business as usual is not jeopardized. There are a number of steps which organizations can take to minimize the impact of this ruling and ensure continued compliance with GDPR. We have outlined these for you, to help you on your Cloud compliance journey.

WORKING TOWARDS PRIVACY CONSCIOUS CLOUD COMPLIANCE

Changing US -based Cloud providers, for EU-based ones will in many cases not be desirable or feasible, regardless of being the most compliant approach for handling EU data in the cloud post-Schrems II. Thankfully there are alternatives. There are three key elements to consider when beginning the journey towards compliance:

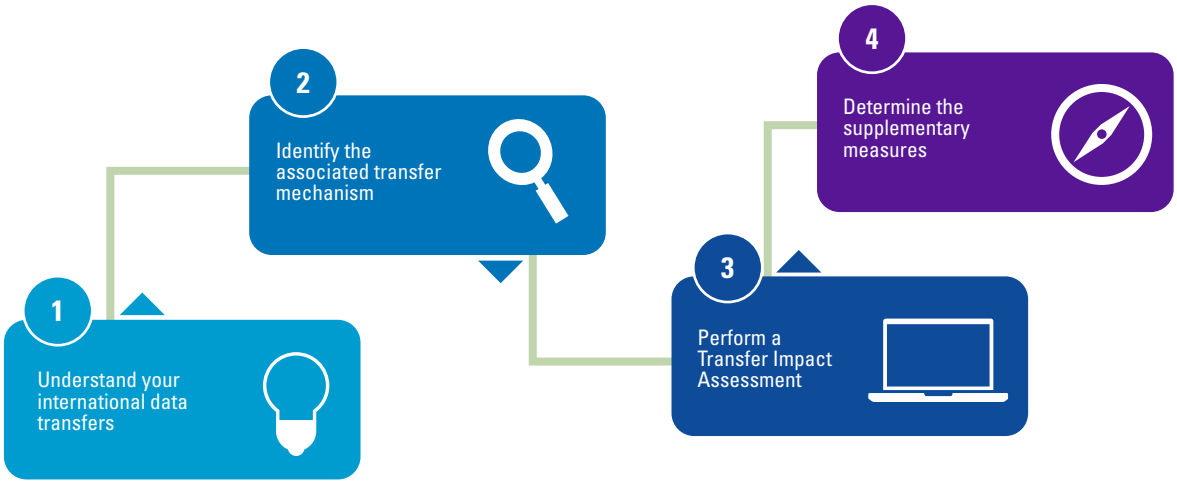
- Data mapping – understanding where data transfers exist within the organizations
- Contractual measures – using legal instruments in managing transfers with third parties
- Supplementary measures – reducing risks through enhanced protection

Each of these items is explored in greater depth in the following sections, bringing together recommendations from the European Data Protection Board, and best practices.

1. Know thy transfers – data mapping is key

It is a bit of a no-brainer, although no less crucial: the first step is knowing to which locations your data is transferred. It is essential to be aware of where the personal data goes, in order to ensure that an equivalent level of protection is afforded wherever is it processed. However, mapping all transfers of personal data to third countries can be a difficult exercise. A good starting point would be to use the record of processing activities, which organizations are already obliged to maintain under the GDPR. There are also dedicated software vendors, such as OneTrust, RSA Archer and MetricStream, in the market that are proven to be very helpful in gathering all this (decentralized) information. Keep in mind that next to storage in a cloud situated outside the EEA, remote access from a third country (for example in support situations) is also considered to be a transfer. More specifically, if you are using an international cloud infrastructure, you must assess if your data will be transferred to third countries and where, unless the cloud provider clearly states in its contract that the

Figure 1. Do not wait to take action; start taking steps towards remediation.



data will not be processed at all in third countries. The following step is verifying that the data you transfer is adequate, relevant and limited to what is necessary in relationship to the purposes for which it is transferred.

2. What about standard contractual clauses?

Once you have a list of all transfers to a third country, the next step is to verify the transfer tool, as listed in chapter V of the GDPR, which your transfers rely on. In this article, we will not elaborate on all the transfer tools. We will instead focus on what is relevant for the use of cloud services in the US. That means that we assume that the transfers fall under 'regular and repetitive', occurring at frequent and reoccurring intervals, e.g. having direct access to a database. Therefore, no use can be made of the exception for 'occasional and non-repetitive transfers', which would only cover transfers taking place outside of regular course of business and under unknown circumstances, such as an emergency.

An option that exists for internal transfers within your organization, is to incorporate Binding Corporate Rules. However, most organizations have their cloud services outsourced, and therefore the most logical transfer tool to address in this article is that of standard contractual clauses (SCCs), also sometimes referred to as model contracts. SCCs however, do not operate in a vacuum. In its Schrems II ruling, the Court reiterates that organizations are responsible for verifying on a case-by-case basis if the law or practice of the third country impinges on the effectiveness of the appropriate safeguards.

Relevant factors to consider in this regard are:

- the purposes for which the data are transferred;
- the type of entities involved (public/private; controller/processor);
- the sector (e.g. telecommunication, financial);
- the categories of personal data transferred;
- whether the data will be stored in the third country or only remotely accessed; and
- the format (plain text, pseudonymized and/or encrypted).

Lastly, you will need to assess if the applicable laws impinge on the commitments contained in the SCC. Because of Schrems II, it is likely that the U.S. impinges on the effectiveness of the appropriate safeguards in the SCC. Does that mean it ends there, and we cannot make use of US-based cloud services anymore? It does not. In those cases, the Court leaves the possibility to implement supplementary measures in addition to the SCCs that fill these gaps in the protection and bring it up to the level required by EU law. In the next paragraph we uncover what this entails in practice.

3. Supplementary measures

In its recommendations 01/2020, the European Data Protection Board (EDPB) included a non-exhaustive list of examples of supplementary measures, including the conditions they would require to be effective. The measures are aimed at reducing the risk that public authorities in third countries endeavor to access transferred data, either in transit by accessing the lines of communication used to convey the data to the recipient country, or while in custody by an intended recipient of the data. These supplementary measures can have a contractual, technical or organizational nature. Combining diverse measures in a way that they support and build on each other can enhance the level of protection. However, combining contractual and organizational measures alone will generally not overcome access to personal data by public authorities of the third country. Therefore, it can happen that only technical measures are effective in preventing such access. In these instances, the contractual and/or organizational measures are complementary, for example by creating obstacles for attempts from public authorities to access data in a manner not compliant with EU standards. We will highlight two technical supplementary measures you may want to consider.

Technical measure: using strong encryption
If your organization uses a hosting service provider in a third country like the US to store personal data, this should be done using strong encryption before transmission. This means that 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. Next, the strength of the encryption should take into account the specific time period during which the confidentiality of the encrypted personal data must be preserved. It is advised to have the algorithm verified, for example by certification. Also, the keys should be reliably managed (generated, administered, stored, if relevant, linked to the identity). Lastly, it is advised that the keys are retained solely under the control of an entity within the EEA. The main US-based cloud providers like Amazon Web Services, IBM Cloud Services, Google Cloud Platform and Microsoft Cloud Services will most likely comply with the strong encryption rules.

Technical measure: transferring pseudonymized data
Another measure is pseudonymizing data before transfer to the US. This measure is effective under the following circumstances: firstly, the personal data must be processed in such a manner that the personal data can no

longer be attributed to a specific data subject, nor be used to single out the data subject in a larger group, without the use of additional information. Secondly, that additional information is held exclusively by the data exporter and kept separately in the EEA. Thirdly, disclosure or unauthorized use of that additional information is prevented by appropriate technical and organizational safeguards, and it is ensured that the data exporter retains sole control of the algorithm or repository that enables re-identification using the additional information. Lastly, by means of a thorough analysis of the data in question – taking into account any information that the public authorities of the recipient country may possess – the controller established that the pseudonymized personal data cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information.

CONCLUSION

In summary, it is important to begin remediation action in light of Schrems II. Good hygiene is important, so start with data mapping, and knowing in which processing activities the transfers to third countries happen. Next, make an assessment on which transfer tool (e.g Privacy Shield) these international transfers are based. For now, SCCs appear to be the way forward when transferring to the US, supported by technical and organizational supplementary measures. To determine which supplementary measures to apply, you should assess the risk of each transfer through a Transfer Impact Assessment, based on at least the following criteria:

- Format of the data to be transferred (plain text/pseudonymized or encrypted);
- Nature of the data;
- Length and complexity of data processing workflow, number of actors involved in the processing, and the relationship between them;
- Possibility that the data may be subject to onward transfers, within the same third country or outside.

Based on this risk, decide which supplementary technical, contractual and organizational measures are appropriate. Make sure you work together with your legal and privacy department throughout the process. Do not wait to take action. Schrems II took immediate effect, and incompliance as a data exporter (i.e. the party contracting the Cloud provider) has the potential for high financial and reputation damage.

References

[AWP17] Article 29 Data Protection Working Party (2017). Adequacy Referential. Retrieved from: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108

[ECJ20] European Court of Justice (2020). Data Protection Commissioner v Facebook Ireland and Maximillian Schrems. Case C-311/18. Retrieved from: http://curia.europa.eu/juris/document/document.jsf;jsessionid=6CD30D2590A68BE18984F3C86A55271E?text=&docid=228677&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=11656651

[EDPB20a] European Data Protection Board (2020). Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Retrieved from: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

[EDPB20b] European Data Protection Board (2020). Recommendations 02/2020 on the European Essential Guarantees for surveillance measures. Retrieved from: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf

[EuPa16] European Parliament and Council of European Union (2016). Regulation (EU) 2016/679. Retrieved from: https://eur-lex.europa.eu/eli/reg/2016/679/oj

About the authors

Laura Huijts LL.M. CIPP/E CIPM CIPT is a senior consultant within the Cyber and Privacy Department of KPMG Advisory N.V. As a member of the Data Privacy Team within KPMG, her work involves conducting audits or maturity assessments, and performing privacy implementations. She has an academic background in law, where her affinity with privacy started. She wrote a bachelor thesis on data retention in criminal law, and a master thesis on medical privacy in employment law. Prior to joining KPMG she worked for a privacy compliance software company, which introduced her to the GDPR and its implementations at organizations.

Daniela Gonzalez Riedel CIPP/E is a senior consultant within the Cyber and Privacy Department of KPMG Advisory N.V. She is a senior consultant within KPMG NL's Cyber team, focused on data privacy. During her experience at KPMG, across the UK and NL practices, she has primarily focused on implementations of privacy programs in large multinationals. Her experience also includes Schrems II remediation support, data breach benchmarking and privacy audits. With over four years of industry experience prior to joining KPMG, predominantly in digital marketing and campaign management, she applies this experience to providing a practical approach to privacy.