Recommendation after ECJ Schrems II (EU-US Privacy Shield)

On 16 July 2020 in its ruling C-311/18[1], the **European Court of Justice declared** the **"EU-US Privacy Shield" to be ineffective**. The ruling does not provide for a grace period and the reasons do not allow any further political delaying tactics (as it was the case in 2015, according to ECJ Schrems I regarding the annulment of the previous agreement "Safe Harbor"). With this ruling, the Court of Justice explicitly interprets at several points **Articles 7 and 8 of the EU Charter of Fundamental Rights**, the fundamental rights to privacy and data protection. These provisions are part of the so-called primary law of the EU, thus the ECJ has also drawn **clear limits for the E U legislator**. What has long been a political tug-of-war has now finally been legally decided by the ECJ. The resulting "digital trade conflict" between the USA and the EU still has a political dimension of course, but **EU companies are now under pressure to act**.

In its ruling, the court also examined the **validity** of the European Commission's Decision 2010/87/EC on **Standard Contractual Clauses** (SCC) and **held it to be valid**. However, the Court pointed out, in particular, that Decision 2010/87/EC imposes an **obligation on** a **data exporter and** the recipient of the data (the **"data importer"**) **to verify**, prior to any transfer, and taking into account the circumstances of the transfer, **whether that level of protection is respected in the third country concerned**. The Decision further **requires the data importer to inform** the data exporter **of any inability to comply with the standard data protection clauses**, and where necessary to fulfil any supplementary measures to those offered by those clauses. The data exporter then, in turn, is obliged to suspend the transfer of data and/or to terminate the contract with the data importer.

The **validity of transferring** personal data to the United States **on the basis of SCC depends on the outcome of the assessment in each individual case**, taking into account the circumstances of the transfer and any additional measures you might take. The **supplementary measures and SCC** would have to ensure, following a case-by-case analysis of the circumstances of the transfer, that U.S. law does not compromise the adequate level of protection that they guarantee. In any event, however, the **judgment establishes** an **obligation of the controller for active examination** with regard to any **transfer of personal data to the United States**.

However, top priority should be given to those data transfers to US companies[2] that are currently based only on the EU-US Privacy Shield. These are now illegal according to the ECJ judgement and should be replaced as soon as possible. This applies in particular to "Google Analytics"[3], also in the "anonymised" variant. For example, Matomo[4] provides for a data protection-friendly alternative.

Data protection officers and coordinators **should urgently forward this letter to their managing bodies**, especially since there is a **risk of personal liability for decision-makers**. At the same time, this **risk can be significantly reduced** or even eliminated with a few relatively simple **steps according to these instructions**. It is important to act actively, and to make use of the existing solutions and possibilities of the technology market.

[1] Decision available at http://curia.europa.eu/juris/liste.jsf?language=de&num=C-311/18 (29.07.2020).

[2] Note that also data transfers from non-US companies to US sub-processors might be based on Privacy Shield.

[3] Currently only the services Google Cloud Platform and G Suite are also based on "EU Model Contract Clauses" and therefore still provide for a legal basis, https://privacy.google.com/businesses/compliance/?hl=en_US (29.07.2020).

[4] https://matomo.org/ (29.07.2020).

In line with the FAQs of the European Data Protection Board (EDPB-FAQ[5]) and in coordination with the recommendations of noyb.eu[6] on the "Schrems II" judgment, Research Institute strongly recommends that any organisation, whether a data controller or a processor, implement the following steps in a timely manner:

1. **Check all external data flows** (including to EU companies, which in turn might transfer data to non-EU companies) **for data transfer to third countries**

2. **Legal basis examination** (two-step check)
   - On what legal basis under Articles 6 to 9 GDPR (consent, performance of contract, legitimate interests) is the processing carried out?
   - How is the adequate level of data protection established? (e.g. adequacy decision, exceptions Art 49 GDPR, Privacy Shield, SCC, etc.)

3. **Examine** "Electronic Communication Service Providers"[7] and "Cloud Providers" in the USA and **any data flow to the USA that is not protected against interception by NSA[8]**

4. **Controller/Processor in the third country rely on SCC:**
   - For non-US companies: examine the relevant facts in the third country – obligation to act if evident (China? Belarus? Other regimes?)
   - For US companies: the ECJ decision "Schrems II" must automatically raise doubts as to whether SCC can be complied with → obligation to act

5. **Positive obligation to act in cases of US services based on SCC:**
   - Many US services are currently still justified by SCC after the annulment of the "privacy shield", e.g. Microsoft or Apple. In our opinion, this justification will be removed by the EU data protection authorities in major cases within 6-12 months.
   - As early as possible, but at the latest in autumn after the holiday period, first steps should therefore be taken to prepare and fulfil the obligations under Art 24 (controller) or Art 28 (processor) GDPR.
   - The first step is the official request to the US companies identified after the internal assessment. For this purpose noyb.eu has developed a guide and sample questions: https://noyb.eu/en/next-steps-eu-companies-faqs
   - Use the editable form[9] and write to the US company concerned. In doing so, you will fulfil an essential part of your duty and gain time by claiming the US partners responsibility. Furthermore, the further course of action will be determined by the answer to your inquiry.

[5] https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118.pdf (29.07.2020).
[6] https://noyb.eu/en/next-steps-eu-companies-faqs (29.07.2020); RI Scientific Director C. Tschohl is a board member of noyb.eu along with M. Schrems and P. Leupold, but was not operationally involved in the project.
[7] See the list of the providers definitely affected and the sample requests at https://noyb.eu/en/next-steps-eu-companies-faqs (29.07.2020).
[8] With regard to the US legal basis 50 USC § 1881a (= FISA 702) and EO 12.333.
[9] https://noyb.eu/files/CJEU/EU-EU_form_v3.docx (29.07.2020).

Possibilities to ensure a proper legal basis

1. As far as possible and economically feasible: implement alternatives within the EEA or third countries with an adequate level of data protection[10] or "on-premise" solutions such as Matomo for web traffic analysis. Those who quickly initiate a plan will also be met with understanding if the implementation takes some time.
2. Comprehensible explanation of the US partner, through which technical and organisational measures data are protected against access by "the NSA". Especially for US providers with data centres in the EU (e.g. Microsoft), a complete technical and legal/organisational separation of the spheres between operations in the USA and in the EU/EEA must be ensured. If there is a clean separation, there is no processing in the third country at all.
3. Design measures in your own sphere: Through measures of encryption or innovative approaches to cloud computing in distributed systems, in some cases it can also be achieved that no personal data (in the legal sense) is processed in third countries. Depending on the importance of the existing systems, this might be a promising approach.
4. If nothing else helps: Extend users consent to processing in a third country without adequate protection. This possibility is provided for in Art 49 para 1 lit a GDPR. The data protection declaration (information) must then be explicitly supplemented by the transfer of data to an “unsafe” third country and the exception in Art 49 para 1 lit a GDPR.

Termination of processing in the third country

Data transfers to a third country should be stopped in the following cases:

- your organisation or one of its partners continues to rely solely on Privacy Shield to justify an "adequate level of data protection",
- your organisation transmits data to a US "Electronic Communication Service Provider" and there is no exception under Art 49 DSGVO, or
- the data transmission cannot be protected against interception by NSAs in any other way (in particular by technology design).

If, despite a negative assessment, you still wish to transfer data to the USA on the basis of SCC, Binding Corporate Rules (BCR) or other comparable legal instruments, for instance because there are compelling practical reasons for doing so, you should consider involving the national data protection authority. In the case of large service providers such as Microsoft or Apple, where currently virtually no alternative exits to some extent, the European data protection authorities are on the ball.

[10] See the good overview of the EU Commission on the "adequacy decisions": https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (29.07.2020).

Summary and outlook

No company can or must solve the problems of the world alone, this is not expected. However, it is to be expected that a company – especially in the role of the controller – will actively strive to achieve a lawful state, and thus also activate the responsibility of partners in third countries. Above all, any existing company group should be motivated to a joint approach of group companies in order to give more weight to critical requests.

Within the sphere of influence of Research Institute alone, there are a number of organisations which, with respect to their international group connections, can also exert considerable influence beyond the Republic of Austria. The more these recommendations are followed and thus create pressure on the digital US economy, the more promising this approach will be. However, most importantly, it prevents you from accusations of violating positive acting obligations and thus enormously reduces the risk of your organization and the management.

Please note, that according to the established case law of the European Court of Justice (especially "Fashion-ID" and "Planet49"), there is often a joint controllership (with joint responsibility and liability), especially when integrating "social media plug-ins" into your services. Such processing bears a further risk of illegal data processing, which many controllers are not even aware of. This risk has now increased in connection with the invalidation of Privacy Shield.

The first (internal) steps should therefore be taken as early as possible, especially if the justification was based solely on Privacy Shield. With regard to US partners with Standard Contractual Clauses (SCC) however, it should also be early enough if the first steps are taken in September after the holiday period.

The team of the Research Institute - Smart Rights Consulting and me are happy to assist you with our consulting. Despite all the challenges, we wish you a pleasant summer and all the best.

Yours sincerely

Ing. Mag. Dr.iur. Christof Tschohl

Scientific Director, ppa

Vienna, 29.07.2020

research institute
Arnulfsenstraße 9, 1170 Wien
Tel: +43 (1) 58 040 83 – 0
E-Mail: office@researchinstitute.at
Web: http://www.researchinstitute.at