

# ~~Privacy Shield~~ is History

## 7 QUESTIONS YOU SHOULD ASK NOW

**On July 16, 2020, the European Court revoked the EU US Privacy Shield. Why? EU citizens and companies are not sufficiently protected from American authorities accessing data.**

### High penalties

in case of violations

There are also risks posed by the CLOUD Act (*Clarifying Lawful Overseas Use of Data*), which allows US authorities to access data from US companies and their subsidiaries, even if it is saved or processed outside the US.

As an IT manager, you are directly responsible for your customers', employees', and business partners' data, even if you outsource data processing. Penalties for violations equal up to 20 million euros or 4% of your global revenue – an entirely new magnitude. The authorities can also stop unlawful data transfer. Managers can be held personally liable and D&O insurances have their limits.

What measures do you need to take? No final recommendations from the EDPB (*European Data Protection Board*) or the EU Commission have been made so far. We'd therefore like to provide you with this guide which includes the most important information. Here are the 7 questions you should ask:

## Fax numbers & email addresses

are personal data

## Caution in regards to email security & archiving!

There is **no** grace period

**No equivalent protection** with respect to SCCs and BCRs

### 1) How do I currently transfer personal data?

Personal data is any information relating to natural persons identified or identifiable: name, location, online identifiers (e.g. IP addresses), and facts relating to the physical, mental, economic, or social identity of natural persons, including fax numbers and email addresses. Personal data is transferred, for example, in correspondence via email, fax, or text messages.

This means you must clarify the following: What data do you own or are you collecting? Where is it saved? Who processes it and to where is it transferred? And do you have the legal basis for all of this?

### 2) Do I use IT services provided by US-American companies?

Possible candidates are Google, Facebook, Twilio, Zoom, Slack, Proofpoint, Dropbox, Microsoft, and LinkedIn. If you use these, you should carefully examine whether your data export complies with GDPR regulations, for example in regards to email security and archiving.

### 3) Do I work with companies previously covered by the Privacy Shield?

On the [Privacy Shield Framework website](#) you will find a list of all these companies.

The EU-US Privacy Shield is no longer valid and there is no grace period. If you are currently working with one of these companies, you should immediately verify if these companies comply with GDPR regulations. When in doubt, you should ask for a statement confirming that at no time during data processing will data be transferred to the USA or service providers in the USA.

### 4) Can I replace Privacy Shield with SCCs or BCRs?

According to the EDPB declaration of July 24, 2020, US legislation does not guarantee equivalent protection with respect to SCCs (standard contractual clauses) and BCRs (binding corporate rules). This assessment also applies to corresponding agreements with countries such as China or Russia.

Individual SCC and BCR agreements with each US provider require a high degree of administrative and legal involvement. Furthermore, additional measures are required. However, as of November 2020, there are only [preliminary implementation recommendations from the EDPB](#). Risks posed by the CLOUD Act still remain even if SCCs and BCRs are used.

## Major obstacles

in case of individual consents

## Review of the level of data protection

Retarus guarantees

## intra-European

data processing

## 5) Am I allowed to continue transferring data to the USA according to the special provisions in Article 49 of the GDPR?

Generally speaking, yes, if the requirements are fulfilled. However, the hurdles are high. Individuals must give informed, specific, and explicit consent.

### Wording of Art. 49 GDPR

## 6) Where can I find more information?

- Frequently asked questions about the ECJ (European Court of Justice) ruling (also about SCCs/BCRs and Art. 49 GDPR) answered by the EDPB
- Use this questionnaire to clarify with your service providers if a sufficient level of data protection is ensured.

## 7) What should I do if I am searching for a GDPR-compliant solution for my corporate communication?

Make the switch to Retarus' innovative platform services now and bring your risk factor for data protection to zero. We process all European customer data exclusively in our European data centers – in Frankfurt, Munich, and Zurich. We ensure inner-European processing even during failover or maintenance. Retarus does not use US hyperscalers like Google, AWS, or Azure. Retarus is headquartered in Germany and has been family-owned since its founding, with no foreign companies as stakeholders.

If needed, you can migrate your email, SMS, and fax traffic to Retarus' Enterprise Cloud within as little as 24 hours. Get a quick overview of our services and learn how we support you in implementing compliance requirements.

## Summary

The current data protection situation appears to be unclear and complicated. However, we should not forget that all of this change brings many positives: your sensitive business data will be better protected because GDPR is a top priority of Retarus.

## Links used in this document

List of companies previously covered by the Privacy Shield

<https://www.privacyshield.gov/list>

Preliminary implementation recommendations from the EDPB

[https://edpb.europa.eu/sites/edpb/files/consultation/edpb\\_recommendations\\_202001\\_supplementarymeasurestransferstools\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf)

Wording of Art. 49 GDPR

<https://gdprinfo.eu/en-article-49>

Frequently asked questions about the ECJ ruling answered by the EDPB

[https://edpb.europa.eu/sites/edpb/files/files/file1/20200724\\_edpb\\_faqoncjeuc31118\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf)

Questionnaire to clarify with your service providers if a sufficient level of data protection is ensured

[https://www.retarus.com/wp-content/uploads/2021/01/retarus\\_gdpr-questionnaire\\_en.pdf](https://www.retarus.com/wp-content/uploads/2021/01/retarus_gdpr-questionnaire_en.pdf)

Retarus' GDPR-compliant solutions

<https://www.retarus.com>

Retarus' compliance and certifications

<https://www.retarus.com/why-retarus/compliance-certifications>

---

Please note that this document is only for non-binding informational purposes and does not provide legal advice in the actual sense of the word. The content of this document cannot and should not replace individual, binding legal advice that takes your specific situation into consideration. In this respect, no liability can be assumed for the correctness, completeness, and accuracy of the statements.

---