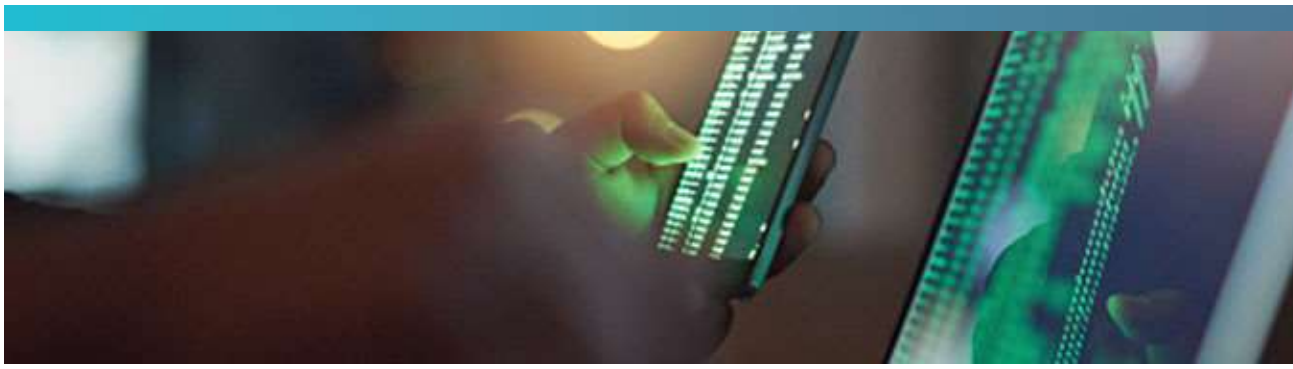
protiviti®
Face the Future with Confidence



EU-US Privacy Shield Invalidation

On the 16th of July 2020, the Court of Justice of the European Union (CJEU) ruled on the Schrems II case, determining that the EU-US Privacy Shield (Privacy Shield) was invalid. So, what does that actually mean?

Privacy Shield — What was it and why was it necessary?

The EU General Data Protection Regulation (GDPR) only permits personal data to be shared outside of the EU when the data recipient will uphold an equal standard of data protection as is afforded under the GDPR. There are a couple of legal mechanisms for ensuring this standard, these include:

- Adequacy Status: where the EU Commission determines that local legislation affords individuals an equivalent level of rights as those which are provided by the GDPR;
- Binding Corporate Rules (BCRs): Entities implement internal policies and standards which enforce an equivalent level of rights as those which are provided by the GDPR; or
- Standard Contractual Clauses (SCCs): Entities enforce a standard set of contractual terms with third parties which enforce an equivalent level of rights as those which are provided by the GDPR.

With this in mind we must look at the US Privacy legislation. The US Privacy Act essentially provides that *'No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains'*. Ostensibly, this looks great, however there are twelve exemptions which require organizations to disclose personal information to the US government for a range of reasons (including for law enforcement purposes, congressional investigations, routine use within a US government agency, etc.). In addition, the US Privacy Act only affords these rights to US Citizens and lawful permanent residents. This meant that European Citizens were explicitly excluded from these provisions and therefore not able to seek redress in the US court system for infringement of their privacy rights.

Consequently, the Privacy Shield was implemented, this relied upon enaction of the US Judicial Redress Act into US law. This act extended the rights afforded under the US Privacy Act to Europeans. This also meant that Europeans could seek redress in the US court system for violations of the Privacy Act. To take advantage of the Privacy Shield Mechanism, US entities would be required to undergo a self-certification process. Privacy Shield certification required commitment to 23 'Privacy Principles' regarding the use and treatment of personal data received from the EU.

Based on implementation of the US Judicial Redress Act & the Privacy Shield Framework, the EU implemented an adequacy decision for the US.

OK, so what went wrong?

Donald Trump's Executive Order

In 2017 Donald Trump signed an executive order entitled 'Enhancing Public Safety in the Interior of the United States' the content of this order included that:

Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information

On the face of it, it would seem that this order would reverse the provisions afforded to Europeans. However, because the US Judicial Redress Act was passed into law, the executive order did not override these rights.

Schrems II Case

The Schrems II case sought to challenge the validity of the SCCs and the Privacy Shield. The case was overseen by the CJEU and the ruling was delivered in July 2020. The consequences of this invalidation are significant as it not only impacts upon the validity of personal data transfers to the US but to data recipients in any other country where local legislation may directly contradict the rights afforded under the SCCs/BCRs. In summary, the court determined the following:

- The Privacy Shield was invalidated and can no longer be used as a legal mechanism for transferring data from the EU to the US. This is because the court determined that it was not possible to uphold an equivalent level of data protection in the US, due to the precedence of national laws.
- The court upheld the validity of the SCCs and the BCRs. However, it states that data transfers to non-adequate countries are prohibited in the instance that it is not possible for the SCCs or BCRs to be enforced. It therefore imposes an obligation on the data exporter and the recipient of the data to verify, prior to any transfer, whether the level of protection described in the SCCs or BCRs will be respected in the third country. It also requires the recipient to inform the data exporter of any inability to comply with the standard data protection clauses.

Please note that this legal analysis is drawn from the EDPB

What Happens Now?

Technically any personal data transfers which are on the basis of the SCCs/BCRs with the US (or the Privacy Shield) or any other country where the local laws contradict the rights afforded by those clauses, are in contravention of the GDPR. This obviously has broad reaching implications. As yet, there is no clear direction from the EU or US as to whether a new agreement will be drafted. In the interim, we recommend that you undertake a systematic risk assessment to determine which contracts may be invalidated by this ruling, you should undertake the following:

1. **Scope.** Identify all data transfers to non-adequate countries operating on the basis of the Privacy Shield, SCCs or BCRs. Consider a) your company locations and b) vendor / third party locations.
2. **Country assessment.** Assess non-adequate countries where you or your business partners operate and make an assessment as to whether local legislation prevents effective implementation of the standards described in the BCRs or SCCs.
3. **Determine whether you can legally still undertake data transfers or not.** The EDPB states that 'it is the responsibility of the data exporter and the data importer to assess whether the level of protection required by EU law is respected in the third country concerned in order to determine if the guarantees provided by the SCCs or the BCRs can be complied with in practice. If this is not the case, you should assess whether you can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EEA, and if the law of the third country will not impinge on these supplementary measures so as to prevent their effectiveness.'
4. **Impact assessment.** Assessment of the risk / impact of the data transfers.
5. **Mitigation plan.** Develop a plan to address non-compliant data transfers. These should be split into two categories:

   - Non-essential data transfers: data transfers that should be terminated.
   - Essential data transfers: data transfers which are essential to your business operations.

   You must develop supplementary measures to address those data transfers which you have deemed are essential. Measures may include obtaining explicit consent from data subjects or re-housing data/processing activities. Note that as yet, the EDPB has not defined a set of appropriate supplementary measures.
6. **Notify your supervisory authority.** If you are unable to enforce compliant processing, you should immediately cease transferring data. If you do not cease transferring data, then this must be reported to your supervisory authority. It should be noted that, because you do not have adequate legal mechanisms for transferring data, this would constitute a data breach and the related procedures should be invoked.

Contacts

Tjakko de Boer
Privacy Lead
+31(0)20-346.0400
Email Tjakko de Boer

Kate Robinson
Risk Management
+31(0)20-346.0400
Email Kate Robinson