24 July 2020

Navigating the Atlantic with Personal Data

*Guillaume Seligmann; Adeline Raut**

Executive summary

In a repeat move echoing the previous invalidation of the "Safe Harbor", on 16th July 2020 the Court of Justice of the European Union ("CJEU") invalidated the "Privacy Shield", which had allowed the transfer of data between the EU and U.S. by American companies adhering to its data protection principles. This "Privacy Shield" had been approved by the European Commission in 2016 as a replacement of the "Safe Harbor" policy.

Companies must therefore stop transferring personal data to the United States based on the "Privacy Shield" legal framework.

This client alert details the situation and the practical steps that can be taken by companies on both sides of the Atlantic in order to remain in compliance with the General Data Protection Regulation ("GDPR") in force in Europe.

The cancellation of the Privacy Shield

The "Privacy Shield" came into force on 1st August 2016, almost a year after the "Safe Harbor" was invalidated by the CJEU, as a new way to allow U.S. companies to process European personal data through an active self-certification mechanism recognized by the European Commission as offering an adequate level of protection.

Within the framework of a preliminary ruling, a lower court had referred the Privacy Shield question to the CJEU, seeking guidance on (i) the applicability of the GDPR to transfers of personal data based on Standard Contractual Clauses ("SCCs") contained in the Commission's Decision 2010/87 and Decision 2016/1250 regarding the adequacy of protection provided by the Privacy Shield, (ii) the level of protection required by the GDPR in the context of such a transfer, and (iii) the obligations of supervisory authorities in that context.

The CJEU's decision

The CJEU did not fully invalidate Decision 2010/87 on SCC, on the ground that (i) the legal mechanisms provided by that Decision make it possible to ensure compliance with the level of protection required by EU law, and that (ii) transfers of personal data pursuant to such clauses are suspended or prohibited in the event of a breach of such clauses or where it is impossible to proceed with transfers in compliance with them.

However, the Court has invalidated the Commission's Decision 2016/1250 on the adequacy of the protection provided by the "Privacy Shield".

Specifically, the CJEU considered that the limitations on the protection of personal data resulting from U.S. regulations do not meet the requirements of the GDPR, in particular with respect to the protection of personal data and the right to effective judicial protection.

The Court underlined that the internal U.S. rules concerning access to, and use by, U.S. authorities of personal data transferred from the EU to that third country (i) do not impose any limitation on the access to data which the implementation of those programmes entails, and (ii) do not provide any guarantee of protection for the non-U.S. persons who are potentially targeted.

Moreover, the Court considered that, in relation to such monitoring programmes, the U.S. legislation does not offer the persons concerned the required effective and judicially enforceable rights against the U.S. authorities.

Practical steps for the transfer of personal data between the EU and the U.S.

EU data protection laws only allow the transfer of personal data outside the European Union and the European Economic Area if a sufficient level of data protection is ensured. Companies must take into account the consequences of the CJEU ruling by adapting their practices in that respect. Failure to act swiftly will expose EU established companies to the risk of substantial sanctions by the relevant data protection authorities in their countries of operation.

- The first step is for companies (whether acting as data controllers or as data processors) to identify those of their contracts that involve a transfer of personal data to the U.S. on the basis of a "Privacy Shield" certification (as opposed to SCCs or Binding Corporate Rules ("BCRs"), which remain valid).

- The second step is to find the most appropriate transfer conduit to implement their processing activities.

The EU data protection legislation offers various frameworks for the transfer of personal data to third countries.

As data controllers or as processors, companies may:

(i) adopt SCCs as part of their contractual relationships with third parties requiring international personal data transfers (including mere access to data by U.S. persons or entities).

The European Commission has issued two sets of SCCs (for EU data controllers to data controllers established outside the EU, and for EU controllers to processors established outside the EU) in order to ensure that the rights of individuals are guaranteed.

As data controller, companies bear responsibility for ensuring that processing activities are compliant with EU data protection laws and thus need to ensure that relevant SCCs are adopted following the invalidation of the Privacy Shield.

As data processor, companies must provide sufficient and adapted guarantees and implement appropriate technical and organisational measures to meet the requirements of the GDPR and ensure the protection of data subjects.

(ii) conclude ad-hoc contractual clauses offering adequate and sufficient personal data protection measures and mechanisms. When the adoption of SCCs is not a workable alternative (because of the specificities of the business relationship), companies can conclude ad hoc contracts, provided they offer strong guarantees and a framework for the transfer of personal data compliant the EU legislation. Such ad-hoc contractual clauses must however first give rise to a review by European Data Protection Board and to be authorized by the relevant data protection authority, in order to ensure that the level of protection of the personal data transferred is sufficient.

(iii) relocate the personal data processing in question in a country of the European Union. Companies may in certain cases require that all processing of their personal data takes place within the EU (or of another country offering sufficient protection).

(iv) anonymize the personal data in a secure and non-reversible way. In cases where the processing carried out outside the EU does not require the provision of data allowing the actual identification of individuals, companies may set up with their provider/partner anonymization (or, in certain cases, pseudonymization) processes, provided that they fulfil the strict conditions imposed by data protection authorities.

(v) adopt BCRs for intra-group cross-border personal data transfers. BCRs are a set of internal rules implemented by multinational companies (with entities outside the EU) carrying out international data transfers within the group, and which are both internally binding and enforceable by data subjects.

BCRs must include all general data protection principles and rights enforceable by data subjects in order to ensure appropriate safeguards for international data transfers.

(vi) terminate existing agreements and manage the repatriation of data to an EU compliant, secure location. However, the ways to manage the situation (in business terms) and the consequences of such a termination (if no other choice is available) will depend upon the provisions of the agreement in question and the principles and rules stemming from the governing law of the agreement as well as those of the party itself.

Finally, it is naturally possible for companies to adopt a multi-channels approach, depending on the needs and specifics of each company and the purposes of the processing in the U.S.

Our experienced team of privacy and data protection attorneys in the EU, the UK, and the U.S. are available to assist and advise you in navigating these complex and changing transatlantic routes and in avoiding legislation and compliance icebergs.

About C&G's Privacy & Data Security Group:

Attorneys in C&G's privacy & data security group advise clients on a broad range of privacy and data protection matters, including developing and implementing privacy policies and procedures, privacy-related litigation, regulatory investigations, global compliance, cross-border data transfers, website terms and conditions, social media and other new information technologies, cybersecurity and network intrusion issues, and contractual matters involving privacy and security.

The Authors:

Guillaume Seligmann
Partner

+33 1 53 53 45 04
gseligmann@cohengresser.com

Guillaume Seligmann is a partner in the firm's Paris office and leads its French technology, privacy, and data protection practice. His practice focuses on all aspects of technology, advising clients on a broad range of technology transactions, disputes, and regulatory matters, both within France and internationally. Guillaume's practice has been recognized by *Chambers Europe* in the Information Technology category, by *The Legal 500 France* in the IT, Telecoms, and Internet category, and by *The Best Lawyers in France* in the Information Technology Law and Privacy and Data Security Law categories. He received his Master's Degree in Business Law from the University of Paris I – Panthéon Sorbonne and his LL.B. with honors from King's College London at the University of London.

*Adeline Rout is an Élève-avocate in C&G's Paris office. She can be reached at arout@cohengresser.com.

About Cohen & Gresser:

Cohen & Gresser is an international law firm with offices in New York, Seoul, Paris, Washington, DC, and London. We have an outstanding record of success in high-stakes and high-profile litigation, investigations, and transactional work for our clients, including major financial institutions and companies across the world. Our attorneys have superb credentials, and are committed to providing the efficiency and personal service of a boutique law firm along with the quality and attention to detail that are the hallmarks of the best firms in the world. The firm has been recognized in a wide range of publications, including *Chambers* and *The Legal 500*.

New York | Seoul | Paris | Washington DC | London

www.cohengresser.com
info@cohengresser.com
+1 212 957 7600

View C&G's Profile