Navigating eDiscovery technology and process challenges without the Privacy Shield

Legal, Compliance and Technology Executive Series

EY
Building a better working world

Background on the EU-U.S. Privacy Shield and *Schrems II*

The U.S. Department of Commerce and the European Commission designed the Privacy Shield to help companies comply with the General Data Protection Regulation (GDPR) when transferring personal data from the EU (European Union) to the US, but as of 16 July 2020, that option is no longer available because the Court of Justice of the European Union (CJEU) in *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems* (often referred to as *Schrems II*) found that the Privacy Shield is inadequate to enable data transfers under EU law.[1] It did, however, hold that standard contractual clauses (SCCs) were valid to transfer EU residents' personal data to the US and third countries.

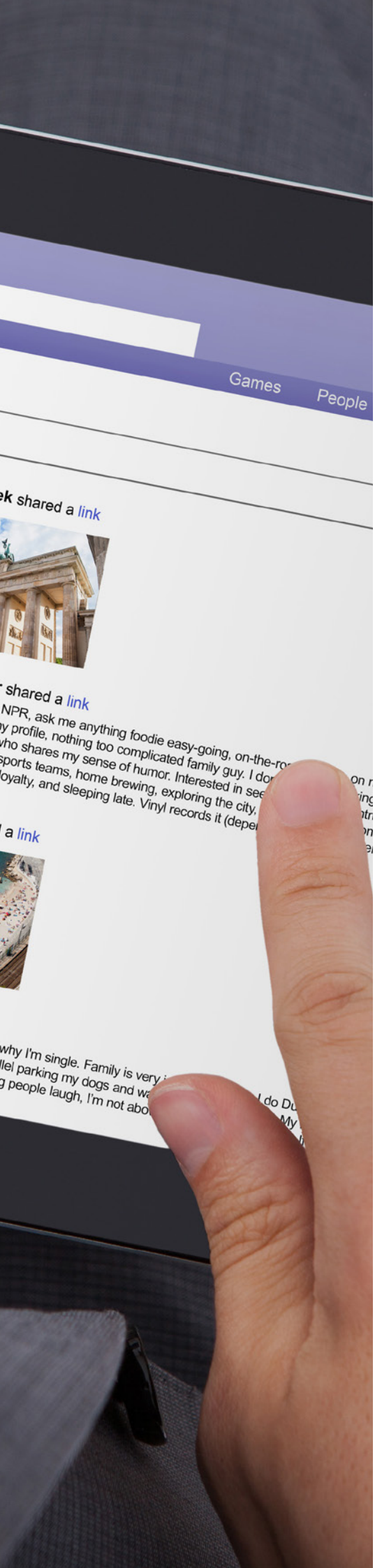
By way of background, Facebook requires users living in the EU to contract with its subsidiary in Ireland because it transfers some of the personal data stored on its servers there to the US for processing. Max Schrems, an Austrian lawyer and Facebook user living in Austria, filed a complaint with the Data Protection Commissioner in Ireland (the DPC) on 25 June 2013.

He asked the DPC to prevent Facebook from transferring his personal data from the EU to the US because he did not think that Facebook ensured sufficient protection of his data from US government surveillance activities and finally in 2015, the CJEU invalidated the Safe Harbor, which was the predecessor to the Privacy Shield. Mr. Schrems then argued and persuaded the CJEU that the Privacy Shield, like the Safe Harbor, failed to provide adequate protections resulting in its invalidation.

[1] InfoCuria Case-Law, 16 July 2020.

Of special interest to:

- Legal counsel
- Corporate security officers
- Information security executives
- Compliance executives
- Risk management executives
- Internal audit



Introduction

In July 2020, the EU's highest court, the CJEU, invalidated the EU-U.S. Privacy Shield — also known as the *Schrems II*[2] decision. As a consequence, organizations can no longer rely on the Privacy Shield for transfers of personal data from the EU to non-EU countries. Organizations that previously relied on the Privacy Shield must immediately institute an alternative approved transfer mechanism or risk running afoul of the GDPR and may incur a fine of up to four percent of their annual revenue or €20 million (about US$23 million), whichever is higher.

Although the *Schrems II* decision invalidated the Privacy Shield Framework and participants can no longer rely on it as an approved data transfer mechanism, the Federal Trade Commission will continue to hold companies accountable for the data protection commitments made under the Privacy Shield. The U.S. Department of Commerce will also continue to administer the Privacy Shield program while an alternative solution is developed. This decision by US regulators aligns with the Privacy Shield's requirement that organizations "continue to apply the Principles to such data for as long as the organization stores, uses or discloses them, even if it subsequently leaves the Privacy Shield for any reason."[3] This effectively means that participant organizations are still obligated to apply the Privacy Shield Principles to any data that was transferred to the US prior to the *Schrems II* decision.

While the CJEU upheld the validity of SCCs as an approved transfer mechanism, they will require prior to any transfer stricter scrutiny and a case-by-case assessment by the exporting and importing parties as to whether the laws of the importing country provide an adequate level of protection essentially equivalent to that guaranteed within the EU by the GDPR. If the parties determine that the SCC cannot be complied with due to the local laws, the CJEU instructs the data exporters to immediately cease all data transfers and/or to terminate the SCC. In addition, the Court holds that supervisory authorities, e.g., Data Protection Authorities (DPAs) in EU, are required to suspend or prohibit a transfer of personal data to a third country if either of the following two situations apply:

1. The SCCs are not or cannot be compiled with inside that country.
2. The protection of the data transferred that is required by EU law cannot be ensured by other means where the data exporter established in the EU has not itself suspended or put an end to such transfer.

It is also worth mentioning that the European Data Protection Board (EDPB) considers *Schrems II* as applicable in the context of binding corporate rules (BCRs)[3] as well, since in the case of the US, domestic law will also have primacy over this tool. Similar to SCCs, the parties cannot rely on BCRs as a transfer mechanism without first completing a case-by-case assessment. The parties must determine if the importing country provides an adequate level of protection or if additional supplementary measures are required in addition to the BCRs, to "ensure that US law does not impinge on the adequate level of protection they guarantee."[4]

[2] Judgement of the Court (Grand Chamber) of 16 July 2020 in case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems.

[3] EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce. See supplemental principle 'Self-Certification' (sec.6.f), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg

[4] "Frequently Asked Questions on the judgement of the Court of Justice of the European Union in Case C-311/18 – *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*," European Data Protection Board (EDPB), 23 July 2020.

What *Schrems II* means for SCCs?

Without the Privacy Shield, companies may still transfer personal data from the EU to the US with appropriate safeguards, which may consist of making use of SCCs or BCRs, only if they include mechanisms that make it possible in practice to ensure compliance with the level of protection guaranteed by the GDPR. The European Commission and the DPAs issue SCCs for data controllers and processors who must have proper technical and organizational measures in place to protect personal data. Those safeguards should ensure compliance with data protection requirements, including the availability of enforceable data subject rights and of effective legal remedies.

The CJEU highlights that the primary responsibility of the data exporter and data importer is to make a case-by-case assessment and to provide necessary supplementary measures. Whether or not you can transfer personal data on the basis of SCCs will depend on the result of that assessment, taking into account the circumstances of the transfers and the supplementary measures you could put in place, which would have to ensure that in practice US law does not impinge on the adequate level of protection they guarantee.

While the CJEU validated the use of SCCs as a method to transfer that personal data from EU to non-EU countries, eDiscovery practitioners could cautiously use SCCs but might have to implement other supplementary measures to ensure compliance with the GDPR and other strategies. That may include using the derogations under the GDPR Article 49 based, for example, on consent of the data subject or on the performance of a contract to transfer personal data out of the EU to the US but there are a number of steps and requirements that need to be taken into account before using those derogations as a lawful basis for data transfer.

Schrems II emphasizes that the SCCs must also address guarantees that prevent access to the data by public authorities or surveillance services. It is particularly important for companies relying on SCCs for eDiscovery to revisit them following the CJEU's decision and ensure GDPR compliance because the EDPB, for example, may scrutinize them for transfers to and from the EU as well as to other jurisdictions.

Besides, on 5 October 2020, the European Data Protection Supervisor (EDPS) has issued an order[5] to European Union institutions, bodies, offices and agencies (EUIs) to carry out an inventory of all ongoing processing operations and contracts involving transfers to third countries, particularly toward the US institutions are requested to complete a mapping exercise and report it to the EDPS by 15 November 2020 at the latest, with special focus on "high-risk transfers" to the US to entities clearly subject to Section 702 FISA or E.O. 123333, among other categories of transfers.

Furthermore, EUIs will be asked to carry out case-by-case transfer impact assessments (TIAs) to identify whether an essentially equivalent level of protection as provided in the EU/European Economic Area (EEA) is afforded in the third country of destination.

Also, in spring 2021, the EDPS will ask EUIs to submit reports on certain transfers, including:

1. Transfers based on the use of derogations.
2. Transfers that are continued toward a third country that does not have an essential equivalent of protection.
3. Transfers that are suspended or terminated due to the absence of essential equivalent protection in the country that is importing the data.

Consequently, in its order the EDPS has strongly encouraged EUIs to avoid processing activities that involve transfers of personal data to the US.

[5] "Strategy for Union institutions, offices, bodies and agencies to comply with the "*Schrems II*" Ruling," European Data Protection Supervisory (EDPS), 29 October 2020.

Key considerations for moving EY eDiscovery forward

Start with a risk-oriented level of protection assessment

Companies relying on SCCs to collect and process EU personal data should conduct an assessment of the level of protection offered by the non-EU country and identify additional safeguards that may be necessary to transfer the information safely to the US. This review should take into consideration both the contractual clauses, the possibility of any access by the public authorities of the importer country to the data transferred and the relevant aspects of its legal system.

If the data includes personal data, you can remove it or identify additional procedural and technical safeguards. One option might be to anonymize the personal data, which would remove it from the scope of the GDPR or the use of proper pseudonymization.

Remove data cautiously

When redacting personal information from documents, it is important to recognize that this alters its form, raises authentication issues and threatens its admissibility in court. It may be more productive to segregate documents with personal information from the data set, process them in the EU member state and transfer the remaining data to the US.

Avoid removal by safeguarding details

In lieu of removing personal data, you can anonymize or deidentify the data in EU to hide the EU data subjects' individual details. Alternatively, use pseudonymization techniques to mask this information. Although it does not completely sanitize the material, it remains an appropriate method to safeguard it from unauthorized access.

Policies must reflect proportionality

The CJEU reasoned in *Schrems II* that any interference with fundamental freedoms and rights protecting data privacy must satisfy the proportionality principle, i.e., that interference should be limited to what is strictly necessary. Companies should, therefore, update their compliance policies and procedures governing discovery requests and data processing to reflect the proportionality principle.

In the view of the Court, the limitations on the protection of personal data arising from the domestic law of the United States, as well as on the access and use by US public authorities of such data transferred from EU to a third country, are not circumscribed in a way that satisfies essential equivalent requirements under EU law by the principle of proportionality, insofar as the surveillance programs based on those provisions are not limited to what is strictly necessary.

Avoid eDiscovery overstretch

In fact, they must outline clear and precise rules addressing the scope and application of eDiscovery and impose safeguards to protect personal data against the risk of abuse. To that end, companies should:

- Oppose overly broad eDiscovery requests for data in the EU
- Re-evaluate the need for cross-border discovery and determine whether the records at issue are accessible from US sources
- Determine whether an EU service provider can process the data instead of one based in the US

Minimize eDiscovery data collection and processing

It is essential for company policies and procedures to comply with the letter and principles of the GDPR, which means that eDiscovery data collection and processing must use data minimization as a pillar. Parties must limit data processing and storage to what is strictly necessary when collected, then promptly erase unnecessary material without preserving or retaining it for possible future litigation.

Inform data subjects

Companies must also inform data subjects of how and why their data is processed, justify doing so and update the information provided to them when personal information is collected and transferred. GDPR Article 13 lists the information that the controller shall provide to the data subject at the time when their personal data is obtained. In addition, companies must have an up-to-date record of their processing activities to ensure they are able to demonstrate compliance with the GDPR.

Security scrutiny may increase

The GDPR also requires companies to notify individuals of a data breach resulting in a high risk to their rights and freedoms. If they use technology such as encryption to render personal data unintelligible to anyone who is not authorized to access it, there is no need to provide any direct alert of that breach to the data subjects since the high risk has been negated by the measures taken.

Following *Schrems II*, companies should have a defined process in place and develop notification systems for data exporters, data protection authorities in EU member states and the EDPB when changes occur in data processing. This is also necessary when data becomes subject to civil processes, government authorities or surveillance measures.

Upgrade your eDiscovery IT

Companies should use technology to ensure the availability, confidentiality, integrity and resilience of processing systems and services. Controllers and processors must restore personal data after a physical or technical event so there should be a process to test and assess the systems regularly as well as to evaluate the effectiveness of measures that ensure processing security.

Conclusion

In the aftermath of *Schrems II*, companies seeking eDiscovery in Europe should keep in mind that the validity of the SCCs for transferring data from EU to the US depends on whether these SCCs include effective mechanisms that ensure compliance with the level of protection essentially equivalent to that guaranteed by the GDPR. Therefore, they should also conduct a risk assessment, recognize that removing data has consequences, avoid overbroad collections, minimize eDiscovery, ensure proper notification and deploy strong security measures.

In addition, it is also necessary to keep in mind that the EDPB has been analyzing the Court's judgment to determine the kind of supplementary measures that could be provided in addition to SCCs or BCRs, whether legal, technical or organizational measures, to transfer data to non-EU countries where SCCs or BCRs will not provide the sufficient level of guarantees on their own and adopted on November 10, 2020 the so-called "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data," which have been open for public consultation until 21 December 2020. The final version is yet to come, however they are applicable immediately.[6]

And since the threshold set by the Court for transfers to the US applies for any third country, it is also critical to recognize that with the UK's departure from the EU, effective since 1 January 2021, the *Schrems II* decision could fuel additional confusion about transferring data and require eDiscovery practitioners to navigate a newly created set of guidelines with different obligations. The potential difficulties associated with collecting European data could result in further disputes over proportionality so proactively drafting strong policies now can help organizations address any issues in the near future.

[6] "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data," European Data Protection Board (EDPB), November 10, 2020.6 See, on July 12, 2016, the Commission determined the Privacy Shield adequate to transfer personal data in Decision 2016/1250, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG.

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

About EY Forensic & Integrity Services

Embedding integrity into an organization's strategic vision and day-to-day operations is critical when managing complex issues of fraud, regulatory compliance, investigations and business disputes. Our international team of more than 4,000 forensic and technology professionals helps leaders balance business objectives and risks, build data-centric ethics and compliance programs, and ultimately develop a culture of integrity. We consider your distinct circumstances and needs to assemble the right multidisciplinary and culturally aligned team for you and your legal advisors. We strive to bring you the benefits of our leading technology, deep subject-matter knowledge and broad global sector experience.

EYG no. 008763-20Gbl
WR #2010-3617083
ED None

ey.com

Authors:

Meribeth Banaschik
Partner, Forensic & Integrity Services
Ernst & Young GmbH
Wirtschaftsprüfungsgesellschaft Germany
meribeth.banaschik@de.ey.com

Scott Clary
Principal, Forensic & Integrity Services
Ernst & Young LLP
scott.clary@ey.com

Michelle Kilbane
Manager, Forensic & Integrity Services
Ernst & Young LLP
michelle.kilbane@ey.com

Sergi Arino Mayans
Senior, Forensic & Integrity Services
Ernst & Young GmbH
Wirtschaftsprüfungsgesellschaft Germany
sergi.arino.mayans@de.ey.com