European Data Protection Board issues response to Schrems II decision

EY Global Law Alert

December 2020

Building a better working world

Executive summary

The Court of Justice of the European Union (CJEU) decision in the Schrems II case invalidated the Privacy Shield arrangement relied upon by organizations transferring personal data between the European Union (EU) and the United States (US). The CJEU held on 16 July 2020 that conforming to the Privacy Shield did not provide data subjects with guarantees substantially equivalent to those required by EU law. This article discusses the European Data Protection Board (EPBD) response to the Schrems II decision.

The CJEU also specified that the Commission Decision 2010/87 on Standard Contractual Clauses (SCCs) for the transfer of personal data from the EU to data processors located in third countries was still valid but that data exporters (i.e., controllers or processors) must verify "on a case-by-case basis and, where appropriate, in collaboration with the importer in the third country" whether the recipient country provides adequate protection under EU law for personal data transferred under the SCCs. If this is not the case, data exporters should implement supplementary measures to comply with the level of protection required by EU law.

Following the Schrems II decision, on 10 November 2020, the EDPB issued two recommendations:

- Recommendation 01/2020 on measures that supplement transfer tools to confirm compliance with EU standards for protection of personal data (Supplementary Measures Recommendations). These recommendations specify how data exporters should assess third countries and when it is necessary to implement supplementary measures
- Recommendation 02/2020 on the European Essential Guarantees for surveillance measures

These recommendations introduce a comprehensive regime for data controllers transferring personal data from the EU to a third country for storage, processing or any other purpose. Data controllers must adhere to the 'Accountability principle' set out in the EU's General Data Protection Regulation (GDPR) and follow the six-step methodology that the EDPB set out in order to determine if supplementary measures need to be implemented. The EDPB guidance provides non-exhaustive examples of organizational, technical or contractual measures which need to be implemented to meet appropriate standards for transferring personal data.

Furthermore, the data controller also becomes responsible for determining whether the non-European Economic Area (EEA) countries, where the data importers are located, conform to EU standards. The recommendations set out the steps that data controllers should take to confirm whether or not the third countries meet the European Essential Guarantees for surveillance measures.

The EDPB's recommendations confirm that the Accountability Principle is paramount for data controllers and, should they not be able to establish supplementary measures and meet the European Essential Guarantees, they should consider ceasing all data transfers to those third countries, including where the transfer is to a group company. Failure to do so could result in enforcement action by the relevant EU Member States' Supervisory Authorities (SA), including monetary penalties.

While these recommendations are not binding, they provide organizations with guidance following the Schrems II decision about the expectations of the SAs responsible for enforcement of the GDPR.

The Accountability Principle

The implementation of supplementary measures as part of transferring personal data to a third country is based on the Accountability Principle (see Article 5.2 GDPR and the Schrems II judgment). The principle establishes an active and continuous responsibility of the data controller and data processor to maintain the integrity of all personal data by implementing legal, technical and organizational measures to confirm effectiveness. In addition, the data controller and processor must be able to demonstrate these efforts to data subjects and SAs.

To comply with this principle, data exporters need to document the assessment and supplementary measures and confirm that such documentation is available to the SA. The EDPB's recommendations suggest that, in the future, SAs will expect data controllers responsible for EU citizens' personal data to meet high standards when transferring data to non-EEA countries.

EDPB methodology for determining whether supplementary measures are required

1. Identify any changes outside the EEA

   Since the Schrems II decision, most organizations transferring data from the EU to the US have been re-examining their data estates, the efficacy of their contractual partners responsible for data processing and the transfer mechanisms upon which they rely. It is not surprising for these organizations to see the EDPB's initial steps in its six-step methodology for determining if supplementary measures are required:

   A data exporter must be fully aware of the transfer by recording and mapping all transfers of personal data to third countries. The data exporter must know where the personal data is processed and located, knowing that remote access from a third country or cloud storage outside the EU is also deemed to be a transfer. Further, a re-examination of the third country data importer may also be required, as many processors further outsource activity to sub-contractors.

2. Identify the data transfer mechanism on which the organization relies

   There are a limited number of mechanisms on which the data controller may rely to transfer personal data to non-EEA countries. These include:

   2.1 Adequacy decisions: If the transfer is to a country for which the EU has provided an an adequacy decision, there is no further step to follow (other than continuing to monitor that the adequacy decision is still current).

   2.2 Binding Corporate Rules (BCR): Global organizations may implement an intra-group framework compliant with Article 47 of the GDPR and obtain the necessary approval for an organization-specific BCR. In any case, the recent recommendations appear to suggest that assessing whether a third country meets the Essential Guarantees will still be required even if BCRs, considered to be the 'gold standard' transfer mechanism, are implemented.

   2.3 Standard Corporate Clauses or ad hoc contractual clauses: Contractual provisions governing the transfer of personal data should incorporate the wording set out in the SCCs, as amended from time to time. These are further discussed below. Moreover, the recent recommendations appear to suggest that assessing whether a third country meets the Essential Guarantees will still be required even if SCCs or ad hoc contractual clauses are implemented. Further, organizations should note that the European Commission released draft updated SCCs on 12 November 2020, circulated for public comment until 10 December 2020.

   In each of the above examples of transfer mechanisms contemplated under Article 46 of the GDPR, the Accountability Principle makes it incumbent on the transferring organization to confirm that the transfer of personal data has an essentially equivalent level of protection to the one provided by GDPR.

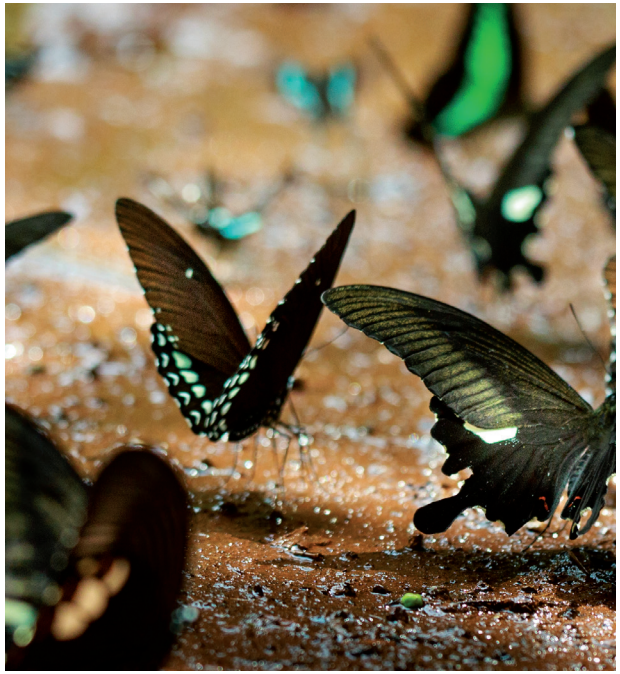
   2.4 Article 49 transfers: Organizations may also transfer personal data based on the exceptions listed in Article 49, which include:

   - 2.4.1 Explicit consent
   - 2.4.2 Transfer is in the public interest
   - 2.4.3 Required for contractual performance
   - 2.4.4 Necessary to protect the vital interests of a data subject

   The GDPR makes it clear that the exceptions listed in Article 49 should not be relied upon for business as usual by data controllers. Derogations under Article 49 do not provide adequate protection or appropriate safeguards for the personal data transferred, and data subjects do not have enforceable and effective rights.

3. Consider all circumstances of the transfer to evaluate effective safeguards

   After considering the matters set out in paragraphs 1 and 2 above, organizations must be able to assess whether their transfer mechanism is effective in practice. For this purpose, the data exporter needs to assess "if there is anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards of the Article 46 GDPR." The assessment should deal with all the parties involved in the data transfer (e.g., controllers, processors, sub-processors) and the characteristics of each transfer. Following the EDPB's recommendations, the data exporter must now also determine how the domestic legal order of the third country applies to the personal data transfer. The EDPB European Essential Guarantees recommendations provide elements to be assessed to determine if the legal framework governing access to personal data by public authorities can be regarded as a 'justifiable interference'.



4. If the third country is deemed to be an inadequate data importer, adopt supplementary measures

   The only circumstances after which SAs will accept from data controllers, based on the EDPB's recommendations, the transfer of data to a non-EEA country which does not meet adequacy standards, is where the data controller can demonstrate it has completed steps 1 and 2 and has also incorporated supplementary measures.

   The EDPB goes into detail about suggested recommendations, which include:

   4.1 Technical measures: Encryption, anonymization, split processing or where there is a 'protected recipient' which is exempt from allowing public authorities access to the data

   4.2 Additional contractual measures: These include requiring transparency on any request from public authorities to access the data, requiring the controller's prior consent before conforming with any such request or obliging the data importer to implement specific technical measures when processing the data.

   4.3 Organizational measures: Internal policies and culture of compliance with data privacy laws and regulations, data minimization measures within the organization to reduce the data estate and utilizing internal agreed frameworks which conform to EU law.

   A combination of diverse measures enhances the data protection. In most situations, only technical measures prevent access to personal data by public authorities in third countries, but organizational and contractual measures may complement and strengthen the protection.

5. Take procedural steps for organizations which have identified effective supplementary measures

   This step may mean organizations which are not confident of the effectiveness of the contemplated supplementary measures to mitigate their risks need to obtain endorsements from SAs regarding their supplementary measures, or submit their proposed measures for review. In the meantime, they must suspend all data transfers to non-EEA countries.

Note:

Organizations must re-evaluate the effectiveness of these mechanisms at appropriate intervals

Whatever the mechanism an organization relies upon to transfer data to non-EEA countries, the EDPB has indicated that these mechanisms must be monitored for effectiveness. Where supplementary measures are in place, SAs may request information from time-to-time from organizations regarding the number of transfers, measures enacted or public authorities' access to such data. Organizations must build into their updated data protection plans the need to regularly review and amend their data transfer regimes.

Assessing third countries' adherence to European Law regarding data privacy

Of all of the recommendations from the EPBD, the discussion of the obligations now imposed on data controllers regarding carrying out assessments of the local laws and practices in non-EEA countries appears to place the highest burden. While previously data controllers may have utilized SCCs or contractual clauses, the EPBD reminds these organizations that, following the CJEU decision in Schrems II, it is their responsibility to evaluate whether the third country is able to provide adequate data protection and freedom from interference by public authorities.

Many organizations will find this to be an onerous burden and one disproportionate to the business opportunity presented by third country data processors. We may therefore see, in light of the EDPB's recommendations, the rise of in-country data processing within the EU. For countries that wish to carry out the assessment themselves, the EDPB suggests they turn to:

- Case law of the CJEU and of the European Court of Human Rights (ECHR)
- Adequacy decisions in the destination country (if the transfer relies on a different legal basis)
- Resolutions and reports of multi-lateral organizations (e.g., Council of Europe, other regional bodies, United Nations departments and agencies)

- Local case law or decisions taken by independent judicial or administrative authorities (competent on data privacy and data protection of third countries)
- Reports from academic institutions and civil society organizations (e.g., non-governmental organizations and trade associations).

The EPBD also notes in its second recommendation that the four European Essential Guarantees must be adhered to in the third countries when it comes to surveillance measures. These guarantees are:

- Guarantee A — Processing should be based on clear, precise and accessible rules
- Guarantee B — Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated
- Guarantee C — Independent oversight mechanism
- Guarantee D — Effective remedies need to be available to the individual

The Schrems II judgment discussed Guarantee D in some detail, with the CJEU finding that an extremely low likelihood that any data subject whose personal data was seized by US law enforcement authorities would have effective remedies against such authorities. Organizations attempting to carry out third-country assessments should not, therefore, fail to obtain local advice regarding the practical consequences of the local data protection regime (if any).

Failure to meet the new standards for data controllers

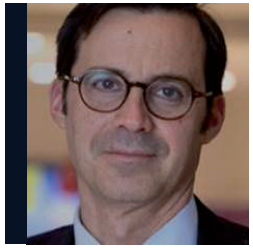
If, after the assessment of the third country's data protection law and guarantees, the country does not offer an adequate level of protection and no supplementary measures are implemented, the data exporter must suspend or end the transfer of personal data. The personal data already transferred should be returned or destroyed by the data importer.

If the data exporter decides to continue the transfer while the data importer is unable to comply with the Article 46 mechanisms, the organization should notify the competent SA, which can suspend or prohibit the transfer.

The SA can also impose corrective measures such as a fine, especially if the organization commences or continues data transfers to a third country despite the fact that the organization cannot demonstrate an essentially equivalent level of protection in that country.

Organizations should note the reputational risk potential from data subjects' complaints. The EDPB makes it clear that data subjects may complain to an SA if they consider that their personal data has not been appropriately processed or transferred.

To discuss any of the issues raised in this alert, please contact:



Fabrice Naftalski

Attorney-at-Law
Partner, EY Société d'Avocats
EY Global Head of Data Privacy
CIPPE/CIPM/Europrivacy

Phone +33 1 55 61 10 05
Mobile +33 6 07 70 87 58
fabrice.naftalski@ey-avocats.com

Peter Katko

Partner, Ernst & Young Law GmbH
EY Global Digital Law Leader

Phone +49 89 14331 25951
Mobile +49 160 939 25951
peter.katko@de.ey.com

Sophie Revol

Attorney-at-law
Associate Partner, EY Société d'Avocats
CIPPE/Europrivacy

Phone +33 1 55 61 10 37
Mobile +33 6 82 59 32 05
sophie.revol@ey-avocats.com

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.

EYG no. 000277-21Gbl

BMC Agency
GA 1017778

ED None

ey.com