BCLP. Client Intelligent

Insights

THE EDPB RECOMMENDATIONS ARE OUT – WHAT'S NEXT FOR YOUR COMPANY?

Nov 16, 2020

Introduction

In July 2020 the Court of Justice of the European Union ("CJEU") handed down its judgment in the case known as "Schrems II". In its judgment, the court invalidated the EU/US Privacy Shield Framework, thereby closing down one of the legal gateways to transfer personal data outside the European Economic Area ("EEA"). Another popular "mechanism" - the European Commission-approved "model clauses" or Standard Contractual Clauses ("SCCs") - survived the legal challenge; however, the court ruled that use of the SCCs alone did not automatically ensure an adequate level of data protection for GDPR purposes and that (unspecified) "supplementary measures" may be required depending on the circumstances. This was a significant change and one that created confusion and concern for organizations both in and out of the EEA.

On November 10, 2020, the European Data Protection Board ("EDPB") released its recommendations, which are intended to help companies put into practice the requirements established by the CJEU in Schrems II (the "Recommendations"). The Recommendations provide guidance to controllers and processors about the steps that companies must take when considering their international transfers, and in particular on the elusive "supplementary measures" that may need to be implemented for transfers to third countries. The Recommendations are subject to a public consultation until 30 November 2020.

The Recommendations

The Recommendations are broken down into the six steps described below that organizations should work through for all transfers of personal data out of the EEA.

Step 1: Know Your Transfers

Unsurprisingly, the first step is for companies to identify their international transfers, including any onward transfers. Existing records of processing (Article 30 GDPR records) can form a basis for this, but organizations should make sure that they are updating this information on a regular basis.

Step 2: Identify the Transfer Tools you are Relying on

Step 2 involves identifying the transfer mechanism, or "legal gateway", that is to form the basis of the transfer. The Recommendations confirm that transfers may take place without the need for further steps to be taken if the destination country has been recognized as "adequate" by the European Commission, or a derogation set out in Article 49 of the GDPR applies to the transfer. For all transfers except those to countries subject to an "adequacy decision" (e.g., Argentina, Canada), organizations are instructed to move through the remaining steps prior to transferring personal data.

Step 3: Assess whether the Transfer Tool is Effective

Companies must consider whether the relevant transfer tool provides an effective level of protection for personal data in practice, by establishing a level of protection in the third country that is essentially equivalent to that guaranteed in the EEA (see the next section for additional discussion of this step). If the outcome of the assessment is that the transfer tool relied on does not provide an essentially equivalent level of protection, it is the exporter's responsibility to either put in place effective supplementary measures or refrain from transferring personal data.

Step 4: Adopt Supplementary Measures

Having identified that supplementary measures are necessary, companies must determine what steps could be taken to provide an essentially equivalent level of protection for personal data. These measures can be contractual, technical or organizational in nature.

Step 5: Procedural Steps if you have Identified Effective Supplementary Measures

These steps will vary depending on the underlying cross-border transfer mechanism and are detailed more broadly in the Recommendations and/or are still be addressed by the EDPB. For example, the effect of Schrems II on transfers made on the basis of Binding Corporate Rules ("BCR") and Article 49 ad-hoc clauses is still being assessed and will be addressed by additional EDPB guidance.

Step 6: Re-evaluate at Appropriate Intervals

As part of broader accountability efforts, organizations must monitor, on an ongoing basis, developments in the relevant third country and their impact on data transfers.

A Closer Look at Step 3

The structure of the Recommendations suggests upon cursory review that applying the step-by-step approach is relatively straightforward, and some of these steps – such as understanding and cataloging data transfers and/or identifying the relevant cross-border transfer vehicle – will or should be part of a well-developed privacy program. Nevertheless, other steps – particularly Step 3 – will present significant obstacles for companies seeking to work through this process.

As noted above, Step 3 (transfer impact assessment) requires organizations (both controllers and processors) to assess whether "there is anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools" relied on, "in the context of [the] specific transfer." The transfer tool (e.g., SCCs) must, according to the Recommendations, ensure that the level of protection guaranteed by the GDPR is not undermined by the transfer itself and that the level of data protection afforded by the recipient country (or supplementary measures) must be essentially equivalent to that provided by the EEA.

According to the EDPB, this assessment should pay particular attention to the legal framework governing access to personal data by public authorities in the third country (e.g., for criminal law enforcement, regulatory supervision, and national security purposes), and whether such access by public authorities is limited to "what is necessary and proportionate in a democratic society." Where a country's laws or practices would prevent the data importer from complying with its obligations under the chosen Article 46 GDPR transfer tool – and absent effective supplementary measures – the transfer tool would be rendered ineffective in practice and, according to the Recommendations, personal data should not be transferred, unless these issues can be addressed via supplementary measures. As with the CJEU itself in the Schrems II decision, the EDPB specifically calls out that data transfers subject to section 702 of the U.S. Foreign Intelligence Surveillance Act ("FISA") must be supplemented by technical measures to make access to the transferred data impossible or ineffective, making clear that transfers of personal data to the United States are of particular concern.

The Recommendations indicate that organizations undertaking this assessment should consider the updated European Essential Guarantees for surveillance measures ("EEG") to provide guidance for assessing a third country's laws and practices when exporting personal data outside of the EEA. The EEG outlines the following four factors for the assessment of the "level of interference with the fundamental rights to privacy and to data protection" presented by public authority surveillance measures in third countries.

1. Processing should be based on clear, precise and accessible rules.

2. Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated.

3. An independent oversight mechanism should exist.

4. Effective remedies need to be available to the individual (i.e., individual redress).

The EDPB recommends starting with examination of the legislation publicly available in the third country, and if such information is not available, assessing other relevant factors such as precedents and academic reports. Significantly, the EDPB states that exporters should not rely on subjective factors, such as the likelihood of public authorities' access to that particular organization's when working through Step 3.

For many organizations – particularly smaller or mid-size organizations with more limited legal departments and/or budgets – this will be a herculean if not impossible task. In order to determine whether data transferred to an entity in a third country will have the benefit of an essentially equivalent level of protection, companies will need to understand how law enforcement and other agencies in that country can access data as part of an investigation, and/or in furtherance of national security objectives, and what guardrails exist, if any. They will also need to understand who will be subject to such laws and under what circumstances. Often – as would be the case for the United States – that analysis will need to include federal laws and regulations across multiple law enforcement agencies, as well as an analysis of state and local laws and regulations. For obvious reasons, this imposes a significant burden on companies that wish to transfer data to a third country, and especially so if they plan to transfer data to multiple third countries.

To illustrate the complexity of such an assessment, consider the challenge of determining under FISA whether a particular organization (or any of its service providers that might store or have access to personal data) qualifies as an "electronic communication service" ("ECS") provider and/or utilizes vendors that may fall into this category. ECS is broadly defined by reference to several other terms that appear in other US laws, such as the Wiretap Act and the Stored Communications Act, 18 U.S.C. § 2510 *et seq*. The US Department of Justice advises that the definition is broad enough to potentially capture any company that provides its employees with corporate email or a similar ability to send and receive electronic communications (e.g., a chat function), regardless of the company's primary business or function.[1]

The reality is that most countries around the world (including some in the EEA) have implemented surveillance and national security laws that would appear not to meet the rigorous standards established in Schrems II and the EEG and/or that could not be circumvented by the types of supplementary measures discussed as Step 4 in the Recommendations. Moreover, businesses will not necessarily know whether or not their analysis is correct until there is a legal challenge. This means that even if a business conducts its due diligence in good faith and makes significant effort to adapt supplementary measures, it could still be found to operate in violation of the GDPR, and ultimately be

subject to significant penalties.

Where Do Organizations Go From Here?

Considering the complications that stem from Schrems II and the Recommendations, the critical next question for organizations is to consider how they might develop a reasonable risk-based approach forward, particularly in the short-term before additional guidance and industry standards become available. Set out below are some practical steps that organizations could consider to help mitigate risk while not shutting down the flow of personal data.

- **Supplementary Measures.** Step 4 of the Recommendations indicates that where an organization determines that the local laws of the recipient country do not offer an equivalent level of protection to that of the EEA, the organization must, as part of the broader assessment process, work to implement supplementary contractual and other measures to fill the gap. Although organizations will find it hard in practice to address all relevant concerns raised by the CJEU and the EDPB (e.g., providing a right for individual redress), organizations should work to identify supplemental measures that establish a good faith effort to meet these requirements and protect personal data as much as possible. Such steps may include:
  - Implementation of a Government Demands Policy that establishes an organization-wide policy of responding only to formal demands and/or limiting responses where possible.
  - Augmenting service provider terms to include notice and consent obligations associated with the disclosure of personal data.
  - Where feasible, deploying technical solutions such as transport encryption and data-at-rest encryption, or pseudonymization of data before transfer.

- **Understand the Potential Application of Laws to Your Organization and Service Providers.** Notwithstanding the EDPR guidance against reliance on subjective factors, organizations should still evaluate where they sit in terms of the actual versus theoretical possibility that a U.S. intelligence agency – or other government body - could access its data. Organizations will also need to keep in mind whether their service providers (e.g., cloud providers of email or similar services) would also be subject to such laws in their own right. In addition, there is also discussion in the Recommendations themselves (as well as in the Draft Decision on SCCs released after the Recommendations) that suggests that companies should consider the subjective factors such as underlying circumstances and potential risks associated with the actual transfers as part of the overall assessment of the data transfer and related protections provided by the recipient country and/or supplemental measures. Therefore, it will be important for companies to continue to understand the circumstances surrounding their particular transfers.
- **Evaluate the Risk of the Transfer Itself.** Although the GDPR as well as Schrems II apply to all EU personal data, the practical risk associated with transfers of personal data will be different for different types of personal data and the circumstances surrounding the transfer. For example, the transfer of EU clinical trial data will be more tightly controlled and also present a higher risk with regard to data breach and potential interest of data subjects and authorities than the transfer of limited B2B data in the context of a business transaction. Consequently, organizations should consider such underlying risks when trying to address the requirements of the Recommendations and when considering what additional supplementary measures might be appropriate.

- **Consider how to Minimize Data Transfers.** Organizations should continue to focus on understanding what international transfers of personal data are truly necessary, and whether any of the transfers can be avoided or can be conducted with anonymized or pseudonymized data. In addition, cloud providers and other service providers are increasingly providing local instances of solutions to address increasing privacy and security regulation – an option that organizations can consider as part of their broader strategy. These considerations will need to be balanced with business needs, such as cost and commercial benefits associated with transfers, but this evaluation will inevitably need to be part of the overall privacy strategy going forward.

Conclusion

There likely will be no perfect way forward for global organizations that need and want to balance the obligations established by Schrems II and the Recommendations with the practical need to move personal data across borders in order to continue to conduct business and likely meet other regulatory obligations. Therefore, it will be critical for organizations to monitor the developments over the next few months and to understand the other pieces that must be considered, including the update of the SCCs,[2] the potential for an updated Privacy Shield and ongoing privacy developments around the globe, and to be prepared to adapt steps adopted now to address this ever-changing privacy landscape.

1. See Office of Legal Educ., Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Crim. Div., Dep't of Justice 117-18 (2015).

2. On November 12, 2020, the European Commission released its Draft Implementing Decision on standard contractual clauses for the transfer of data to third countries.

RELATED PRACTICE AREAS

- Data Privacy & Security

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be "Attorney Advertising" under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP's principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.

© 2024 Bryan Cave Leighton Paisner LLP.