New Guidelines for EU-US Data Transfers

Written by Christopher Escobedo Hart

November 19, 2020

Last week saw major innovations in the law of data transfer from the European Economic Area (EEA) to other countries, including the United States. This alert covers one of them: new guidelines from the European Data Protection Board (EDPB) on international data transfers. These guidelines will have significant implications for EEA-US data transfers, requiring organizations that must manage such transfers to adjust their practices in this evolving environment.

The Background

In July 2020, the Court of Justice of the European Union (CJEU) issued a decision, referred to as *Schrems II*. This decision has significant implications for EEA-to-US data transfers which the EDPB's guidelines now address.

Under the General Data Protection Regulation (GDPR), international data transfers may only occur in certain specified cases. Apart from those that are available only occasionally and non-repetitively, each case ensures that European data subjects' data is protected to a level essentially equivalent to the level it would receive in Europe. One such case is when the data exporter (generally a European company) and data importer (generally a foreign company) form a contract that incorporates certain provisions, authored by the European Commission, under which the data importer agrees to treat the data in a GDPR-compliant way. These provisions, known as the Standard Contractual Clauses (SCCs), predate the GDPR and were general upheld as valid in *Schrems II*. (Last week the European Commission updated the SCCs, which are likely to become final in 2021.)

But another holding of *Schrems II* called the SCCs' vitality into question. The CJEU struck down the Privacy Shield – a mechanism by which American companies could self-certify their provision of GDPR-level protection to Europeans' data – because it found that US law both allowed government surveillance beyond what the GDPR would permit, and provided inadequate remedies against the government in the event of a perceived privacy violation. The CJEU reasoned that a company's promise to treat data securely was unavailing, since companies could not prevent the government from surveilling personal data; nor could companies create, through contract, adequate remedies against governmental privacy violations. Promises made under the Privacy Shield thus could not guarantee an adequate level of protection over personal data.

The same logic applies to the SCCs: private parties cannot contract around federal surveillance law. This led some data protection authorities in the wake of *Schrems II* to initially forbid data transfers to the US on the basis of the SCCs, or even entirely. The EDPB took a more moderate path in initial guidance it promulgated immediately in the wake of the CJEU decision: it recognized that the SCCs may not suffice to ensure an adequate level of protection, but noted that they might suffice if combined with certain "supplementary measures." Various data protection authorities followed this guidance. Yet the EDPB did not then say what those "supplementary measures" might be, and the law has since been in limbo.

Last week's new guidance provides clarity as to what supplementary measures the EDPB considers appropriate. Data importers and exporters need not use any particular measure or specific set of them, and the EDPB's list is non-exhaustive; the key issue is whether the particular combination of measures provides an essentially equivalent level of protection.

The Measures

The guidelines describe three categories of supplementary measures: contractual, organizational, and technical. The technical measures are the most important for EEA-US data transfers: according to the EDPB, contractual and organizational measures alone cannot remedy transfers that is inadequately safeguarded because of too much government surveillance in the destination country. This is because contracts among data importers and exporters, and their organizational structures, cannot prevent the government surveillance that

precludes the US from providing essentially equivalent levels of protections.

But technical measures can be sufficient (as can a combination of technical, contractual, and organizational measures). The technical measures all rely on the principle that protection against government surveillance is adequate only if the government *could not* obtain data lawfully – how likely the government would do so is irrelevant. Thus, companies can provide an adequate level of protection in the US by (a) prior to export, encrypting the data so powerfully that the government cannot break the code, even by brute force, and (b) not sending the encryption key to the US. (The key cannot enter the US, even if sent separately, because then the government would be able to lawfully use it to crack the code.) Assuming such a degree of encryption is possible, this solution could be effective for companies who want to host Europeans' personal data in the US, or to route data through the US to a third country. But it would not work for many routine business purposes. For example, it would not allow a European arm of a US company to send European employees' data to the United States for human resources (HR) purposes, since the American company's HR personnel would generally need to access that data in unencrypted form.

Companies can likewise provide an adequate level of protection by sending pseudynomized (*i.e.*, de-identified, but not anonymized) data to the US without transmitting the re-identification key. This could partly solve the HR problem, as it would allow the European arm to send some employee data to the US headquarters. It also enables what the EDPB calls "split processing," where some subset of data is sent to the US and another to a third country, and where neither subset can identify a person. But it would not work for types of data that cannot be pseudynomized, such as certain biometric data. And the EDPB stresses that data is adequately pseudynomized only if the government cannot re-identify the data subject using the information that it already has.

A final technical measure is to send sufficiently encrypted data to a "protected recipient," defined as a person who is immune from the surveillance laws that otherwise render the level of protection inadequate. The data can be decrypted in the US (but must be encrypted in transit) as long as the decryption key is possessed solely by the protected recipient, and is sufficiently secure itself. This measure should be combined with contractual and/or organizational measures that prevent the protected recipient from rendering the data unprotected, such as by forwarding it to an unprotected person. In the US, this type of measure could be useful when feasible to transfer and store data in hard copy – FISA section 702, which the *Schrems II* decision cited when invalidating the Privacy Shield, only allows the government to collect data from electronic communications service providers.

The Path Forward

The EDPB's supplementary measures may be sufficient for some contemplated data transfers. In these cases, companies should implement them. But in many situations they will not be adequate. Yet these cases do not necessarily require EEA data localization. There is still the option to effect some international data transfers using consent, although the GDPR prohibits more than occasional or repetitive consent-based transfers to countries that do not provide an adequate level of protection. Further, Member State data protection authorities, not the EDPB, enforce the GDPR, and may well find less cumbersome methods to be adequate. They will also have their own enforcement priorities. We are on the lookout for both.

RELATED PRACTICES

- Privacy & Data Security
