CLIENT ALERT

Data Transfers from the EU: What Does "Good" Look Like?

Nov.17.2020

Last week was another important week for privacy professionals: the European Data Protection Board (EDPB) issued its long-awaited recommendations on the so-called "supplementary measures" together with recommendations on the European Essential Guarantees for surveillance measures. Not to be outdone, the European Commission (EC) issued its even-longer-awaited updated standard contractual clauses. The first and third document are open for feedback until November 30, 2020, and December 10, 2020, respectively.

Why Are These Documents So Important?

One of the cornerstones of the European Union (EU) is the free movement of goods, services, capital, persons, and – quite important in today's digitalized world – personal data. The European General Data Protection Regulation (GDPR) created a harmonized legal framework and, thus, one single territory without regulatory obstacles for the transfer of personal data from one EU Member State to another.

To make this uniform approach possible, the bar was set high: all EU Member States needed to provide a similarly solid level of protection of personal data. As the right to the protection of personal data is enshrined in the EU Charter of Fundamental Rights, the EU legislator wanted to make sure that such protection would not be diminished when data leave the EU's protected environment by imposing such obligation upon the organizations that decide to send data outside the EU. Or, as the EDPB puts it: the protection "must travel with the data wherever it goes."

While there are derogations for specific situations, the options to lawfully transfer personal data are rather limited: whether they are sent to a country that is considered to provide a similar, and thus "adequate", level of protection or, if this is not the case, "appropriate safeguards" should be implemented. In practice, companies massively opted for the most straightforward solution of Standard Contractual Clauses (SCCs), which in essence is a standard language contract in which both the exporting and importing organization commit to set the bar for the protection of personal data outside the EU as high as within the EU.

Unfortunately, this data transfer mechanism is flawed for two main reasons: firstly, it has not been updated and, thus, still refers to the pre-GDPR legal framework, and secondly, since the CJEU's Schrems II judgment, it is no longer sufficient on its own for transfers to countries lacking an "adequacy" decision from the EU Commission, which means that "supplementary measures" must be taken. The documents that have been issued now address both these challenges, which means that their importance cannot be underestimated.

Supplementary Measures

The EDPB was very clear when it issued its FAQ document after the Schrems II judgment: apart from appropriate safeguards such as SSCs and Binding Corporate Rules (not discussed herein), supplementary measures should be put in place when a data

exporter and a data importer conclude that the legal framework of the data importer's country does not provide an adequate level of protection. For several months it was unclear what such measures should look like, until now.

The EDPB's recommendations provide a series of steps to follow, potential sources of information, and some examples of supplementary measures that could be put in place.

The EDPB recommends a structured stepped approach. The first three steps are the ones that we also recommended in our client alert of July 16, *i.e.*, the mapping of the data transfers and corresponding mechanisms and the assessment of the legal framework of the country of destination, while the last three steps relate to the taking and (re-)evaluating of the supplementary measures.

The EDPB clarifies that supplementary measures could be of contractual, technical or organizational nature, which is in line with what we recommended in our recent webinar on international data transfers.

Some examples are provided in Annex 2 of the recommendations:

A non-exhaustive list of technical measures that could potentially be effective in certain scenarios/use-cases to ensure an essentially equivalent level of protection:

Use Case	**Technical Measures**
Data storage for backup and other purposes that do not require access to data in the clear	• Strong encryption before transmission • Algorithm and parameters robust against cryptanalysis • Reliable management of encryption keys • Keys under control of the data exporter
Transfer of pseudonymized data	• Data no longer attributable to an individual without additional information • Additional information held exclusively by data exporter • Disclosure of additional information prevented by appropriate technical and organizational safeguards • Recipient country public authorities cannot use information in their possession to identify the individual
Encrypted data merely transiting third countries	• State-of-the-art encryption

	• Decryption only possible outside the non-adequate third country • Agreement on a trustworthy public-key certification authority or infrastructure • Algorithm and parameters robust against cryptanalysis • No backdoors • Reliable management of keys
Protected recipient	• The law of a third country exempts a resident data importer from potentially infringing access to data held by that recipient for the given purpose, e.g., by virtue of a duty to professional secrecy applying to the data importer • The data importer does not employ the services of a processor in a way that allows the public authorities to access the data while held by the processor, nor does the data importer forward the data to another entity that is not protected, on the basis of Article 46 GDPR transfer tools • The personal data is encrypted before it is transmitted with a method conforming to the state-of-the-art guaranteeing that decryption will not be possible without knowledge of the decryption key (end-to-end encryption) for the whole length of time the data needs to be protected • The decryption key is in the sole custody of the protected data importer, and appropriately secured against unauthorized use or disclosure by technical and organizational measures conforming to the state-of-the-art, and the data exporter has reliably established that the encryption key it intends to use corresponds to the decryption key held by the recipient
Split or multi-party processing	• Data split into two or more parts, each of which

	can no longer be attributed to a specific data subject • Each data element is transferred to a separate processor located in a different jurisdiction • The algorithm used for the shared computation is secure against active adversaries • There is no evidence of collaboration between the public authorities located in the respective jurisdictions where each of the processors are located, which would allow them access to all sets of personal data held by the processors and enable them to reconstitute and exploit the content of the personal data in a clear form in circumstances where such exploitation would not respect the essence of the fundamental rights and freedoms of the data subjects • The controller has established by means of a thorough analysis of the data in question, taking into account any information that the public authorities of the recipient countries may possess, that the pieces of personal data it transmits to the processors cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information

Some scenarios/use cases in which no technical measures could be identified by the EDPB to ensure this level of protection:

- Transfer to cloud services providers or other processors which require access to data in the clear; or
- Remote access to data for business purposes.

Examples of contractual measures may relate to:

- Providing for the contractual obligation to use specific technical measures;
- Transparency obligations;
- Obligations to take specific actions; or
- Empowering data subjects to exercise their rights.

Examples of organizational measures may consist of:

- Internal policies for governance of transfers, especially with groups of enterprises;
- Transparency and accountability measures;
- Organization methods and data minimisation measures; or
- Adoption of standards and best practices.

In Annex 3, the EDPB provides a quite limited list of possible sources of information to assess a third country.

Standard Contractual Clauses

As mentioned above, updating the outdated SCCs was long overdue. EU commissioner Reynders referred to "modernized" SCCs in several occasions, and while the draft document is not the final version yet, we can certainly assess whether we can indeed talk about a "modernization."

Privacy professionals who have been working – and struggling – with the current versions for many years, certainly welcome the following changes:

- one single document: may be used by controllers or processors for transfers to controllers or processors;
- entire data processing chain covered: may also be used for onward transfers and for transfers from processors to subprocessors;
- extraterritoriality: may also be used by non-EU-based controllers or processors;
- modular approach: general clauses combined with clauses for specific scenarios, which allows organizations to tailor the document to the specific situation and each party's roles and responsibilities; and
- multi-party approach: may now be used by several controllers or processors and new parties can opt-in by adhering to the existing document.

While these changes may feel like a breath of fresh air when compared to the current version, and while they should certainly be considered as an important improvement, these are arguably not really innovative changes from a European contract law point of view.

Furthermore, some additional obligations will certainly be challenging from an operational point of view. For example, individuals (so-called "data subjects") should always be informed about the identity of the data importer, which goes a step further than the current transparency obligations stemming from the GDPR, which impose to inform about the "categories" of recipients and "the fact" of an (intended) international data transfer.

Additionally, onward transfers are more strictly regulated. Barring a limited number of exceptions such as the consent of the data subject, onward transfers are only allowed to a party that is or agrees to be bound by the SCCs.

The shadow of the Schrems II judgment can clearly be seen when reading the clauses referring to the local laws affecting compliance with the SCCs and the obligations of the data importer in case of government access requests. The draft Commission decision authorizing the new SCCs explicitly includes a placeholder for the EDPB guidance on required "supplementary

measures" that are discussed above, and reiterates the requirement that the parties to any transfer must "take into account the specific circumstances of the transfer" when determining whether the appropriate level of protection is provided. Clause 2(b)(ii) of the new SCCs requires importers and exporters to consider "relevant practical experiences with prior instances" of requests or "the absence of requests for disclosure" as part of this analysis – a more explicit requirement than that parties consider the factual question of whether transferred data is likely to be actually subject to a request, rather than solely considering what national law may apply to an importer.

Additionally, the draft decision emphasizes that data importers must notify both data subjects and data exporters, should an importer receive a legally binding request from a public authority, or otherwise become aware of any direct access by public authorities to personal data transferred.

And lastly, it is not surprising that GDPR principles such as accuracy, data minimization and storage limitation are called out specifically, and the focus on third-party beneficiary rights for data subjects is also in line with the expectations, as well as the fact that SCCs should provide for rules on liability between the parties and with respect to data subjects, as well as rules on indemnification between the parties.

So now that we have this new kid on the block, what about the old SCCs? There will be a transitional period of one year during which organizations can still rely on existing SCCs, unless there are changing circumstances. Note, however, that the need for supplementary measures imposed by Schrems II is required for both the old and the new SCCs.

In summary, the new SCCs provide a more workable instrument for international data transfers and, if approved, organizations will be able to start using them in the beginning of 2021. It is, however, more than ever clear that compliance with international data transfer obligations and restrictions is not a box that can be checked just by entering into an agreement. There is homework to be done, both before and after the transfer, and with both regulators and privacy activists looking over their shoulders, organizations certainly know where to focus their data protection compliance efforts.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Maarten Stassen
Partner – Brussels
Phone: +32.2.214.2837
Email: mstassen@crowell.com

Jeffrey L. Poston
Partner – Washington, D.C.
Phone: +1 202.624.2775
Email: jposton@crowell.com

Robert Holleyman
Partner and C&M International President & CEO – Washington, D.C.
Phone: +1 202.624.2505
Email: rholleyman@crowell.com

Jeane A. Thomas, CIPP/E
Partner – Washington, D.C., Brussels

Phone: +1 202.624.2877, +32.2.282.4082
Email: jthomas@crowell.com

Frederik Van Remoortel
Partner – Brussels
Phone: +32.2.282.1844
Email: fvanremoortel@crowell.com

Jarno Vanto, CIPP/E, CIPP/US
Partner – New York
Phone: +1 212.803.4025
Email: jvanto@crowell.com

Laurence Winston
Partner – London
Phone: +44.20.7413.1333
Email: lwinston@crowell.com

Lee Matheson, CIPP/US/E/A, CIPM, PCIP
Associate – Washington, D.C.
Phone: +1 202.654.6728
Email: lmatheson@crowell.com