GIBSON DUNN

November 24, 2020

EUROPEAN DATA PROTECTION BOARD ISSUES IMPORTANT NEW GUIDANCE ON TRANSFERS OF PERSONAL DATA OUT OF THE EUROPEAN ECONOMIC AREA

To Our Clients and Friends:

On 10 November 2020, the European Data Protection Board (EDPB) issued important new guidance on transferring personal data out of the European Economic Area (EEA). The guidance addresses a key question for many companies: how to transfer personal data out of the EEA to the United States or other countries not recognized by the European Commission as ensuring an adequate level of protection for personal data. The guidance thus begins to lessen some of the uncertainty caused by the Court of Justice of the European Union's July 2020 ruling in the landmark *Schrems II* decision.

The EDPB's guidance have been published for consultation by citizens and stakeholders until 21 December 2020, and may thus be subject to further changes or amendments. Although the guidance take the form of non-binding recommendations, companies that transfer personal data out of the EEA would be well-served to review their approach to such transfers in light of the EDPB guidance.

I. Context

As a reminder, under the EU's omnibus privacy law, the General Data Protection Regulation (GDPR), a transfer of personal data out of the EEA may take place if the receiving country ensures an adequate level of data protection, as determined by a decision of the European Commission. In the absence of such an adequacy decision, the exporter may proceed to such data transfer only if it has put in place appropriate safeguards.

In the *Schrems II* ruling in July 2020, the CJEU invalidated the EU-U.S. Privacy Shield, which had been a framework used by companies transferring personal data from the EEA to the U.S. to provide reassurance that the data would be protected after the transfer. The CJEU's decision allowed the use of the Standard Contractual Clauses, known as the "SCCs," approved by the European Commission, to continue as another framework or method to cover such transfers. However, the CJEU required companies to verify, prior to any transfer of personal data pursuant to the SCCs, whether data subjects would be granted a level of protection in the receiving country essentially equivalent to that guaranteed within the EU, pursuant to the GDPR and the EU Charter of Fundamental Rights.[i]

The Court specified that the assessment of that level of protection must take into consideration both the contractual arrangements between the data exporter and the recipient and, as regards any access by the public authorities of the receiving country, the relevant aspects of the legal system of that third country.

Due to their contractual nature, SCCs cannot bind the public authorities of third countries, since they are not party to the contract. Consequently, under *Schrems II*, data exporters may need to supplement the guarantees contained in the SCCs with supplementary measures to ensure compliance with the level of protection required under EU law in a particular third country.

The EDPB issued on 10 November 2020 two sets of recommendations:

1. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, which are aimed at providing a methodology for data exporters to determine whether and which additional measures would need to be put in place for their transfers; and

2. Recommendations 02/2020 on the European Essential Guarantees (EEG) for surveillance measures, which are aimed at updating the EEG[ii], in order to provide elements to examine whether surveillance measures allowing access to personal data by public authorities in a receiving country, whether national security agencies or law enforcement authorities, can be regarded as a justifiable interference.

II. Recommendations on how to identify and adopt supplementary measures

The EDPB describes a roadmap of the steps to adopt in order to determine if a data exporter needs to put in place supplementary measures to be able to legally transfer data outside the EEA.

Step 1 - Know your transfers. The data exporter should map all transfers of personal data to countries outside the EEA (and verify that the data transferred is adequate, relevant and limited to what is necessary in relation to the purposes for which it is transferred to and processed in the third country).

Step 2 - Verify the transfer tool on which the transfer relies. If the European Commission has already declared the country as ensuring an adequate level of protection for personal data, there is no need to take any further steps, other than monitoring that the adequacy decision remains valid.

In the absence of an adequacy decision, the data exporter and the data importer would need to rely on one of the transfer tools listed under Articles 46 of the GDPR (including the SCCs) for transfers that are regular and repetitive. Derogations provided for in Article 49 of the GDPR[iii] may be relied on only in some cases of occasional and non-repetitive transfers.

Step 3 - 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 transfer tools relied on, in the context of the transfer (see section III below).

The recommendations specify that: (i) the data importer should be in a position to provide the relevant sources and information relating to the third country in which it is established and the laws applicable to it; and (ii) the data exporter may also refer to several sources of information (e.g., case law of the CJEU and of the European Court of Human Rights; adequacy decisions in the country of destination if the

transfer relies on a different legal basis; national caselaw or decisions taken by independent judicial or administrative authorities competent on data privacy and data protection of third countries).

If the assessment reveals that the receiving country's legislation impinges on the effectiveness of the transfer tool contained in Article 46 of the GDPR, Step 4 should be implemented[iv].

Step 4 - Identify and adopt supplementary measures to bring the level of protection of the data transferred up to the EU standard of "essential equivalence".

Supplementary measures may have a contractual[v], technical[vi], or organizational[vii] nature—and combining diverse measures may enhance the level of protection and contribute to reaching EU standards.

The EDPB provides for:

1. Various examples of measures that are dependent upon several conditions being met in order to be considered effective (e.g., technical measures such as encryption or pseudonymization; contractual measures such as obligation to use specific technical measures, transparency obligations, obligations to take specific actions, empowering data subjects to exercise their rights; organizational measures such as internal policies for governance of transfers especially with groups of enterprises, transparency and accountability measures, organization methods and data minimization measures, adoption of standards and best practices); and

2. A non-exhaustive list of factors to identify which supplementary measures would be most effective: (a) format of the data to be transferred (i.e. in plain text, pseudonymized or encrypted); (b) nature of the data; (c) length and complexity of the data processing workflow, number of actors involved in the processing, and the relationship between them; (d) possibility that the data may be subject to onward transfers, within the same receiving country or even to other third countries.

The EDPB clarifies that certain data transfer scenarios may not lead to the identification of an effective solution to ensure an essentially equivalent level of protection for the data transferred to the third country. Therefore, in these circumstances, supplementary measures may not qualify to lawfully cover data transfers (e.g., where transfer to processors requires access to data in clear text or remote access to data for business purposes).

In addition, the EDPB specifies that contractual and organizational measures alone will generally not overcome access to personal data by public authorities of the third country. Thus, there will be situations where only technical measures might impede or render ineffective such access.

If no supplementary measure can ensure an essentially equivalent level of protection for a specific transfer, in particular if the law of the receiving country prohibits the application of the possible supplementary measures envisaged (e.g., prohibits the use of encryption) or otherwise prevents their effectiveness, the transfer should be avoided, suspended or terminated.

Step 5 – Implement procedural steps if effective supplementary measures have been identified[viii].

For example, this could consist of entering into an amendment to complete the SCCs to provide for the supplementary measures. When the SCCs themselves are modified or where the supplementary measures added "contradict" directly or indirectly the SCCs, the procedural step should consist in requesting the authorization from the competent supervisory authority.

Step 6 - Re-evaluate at appropriate intervals, i.e., monitor developments in the third country that could affect the initial assessment.

III. Recommendations on how to assess the level of protection of a third country (Step 3)

The "Recommendations 02/2020 on the European Essential Guarantees for surveillance measures" specify the four EEGs to be taken into consideration in assessing whether surveillance measures allowing access to personal data by public authorities in a receiving country (whether national security agencies or law enforcement authorities), can be regarded as a justifiable interference. Such EEGs should be seen as the essential guarantees to be found in the receiving country when assessing the interference (rather than a list of elements to demonstrate that the legal regime of a third country as a whole is providing an essentially equivalent level of protection):

- Processing should be based on clear, precise and accessible rules;
- Necessity and proportionality with regard to the legitimate objectives pursued must be demonstrated;
- An independent oversight mechanism should exist; and
- Effective remedies need to be available to the individual.

IV. Consequences

Many companies will likely continue to transfer personal data outside of the EEA on the basis of the transfer tools listed under Articles 46 of the GDPR (including the SCCs and binding corporate rules). Companies, in particular data exporters, must therefore **document** the efforts implemented in order to ensure that the level of protection required by EU law will be complied within the third countries to which personal data are transferred.

Such efforts should include, **first,** to **assess** whether the level of protection required by EU law is respected in the relevant third country **and, if this is not the case**, to identify and adopt **supplementary measures** (technical, contractual and/or organizational) to bring the level of protection of the data transferred up to the EU standard of "essential equivalence". If no supplementary measure can ensure an essentially equivalent level of protection for a specific transfer, the transfer should be avoided, suspended or terminated.

It is difficult to predict how local supervisory authorities will assess compliance efforts or sanction non-compliant transfers. While the EDPB's recommendations are to be implemented on a case-by-case basis based on the specifics of the concerned transfer, we may not exclude supervisory authorities to assess

independently the level of protection of certain receiving countries and identifying relevant supplemental measures.

In addition, these recommendations raise sensitive issues with respect to **Brexit**, and come at a critical moment in the Brexit negotiations. The U.K. will, in the event of a "No-Deal" Brexit, become a third state from the end of the transition period on 31 December 2020, and there is unlikely to be, at least immediately, an adequacy decision in place in respect of the U.K. One might reasonably expect that, given its membership throughout the currency of the GDPR and the forerunner directive, an adequacy decision in favor of the U.K. would be rapidly forthcoming. While that would be a determination for the European Commission, the EDPB has expressed reservations, making specific reference to the October 2019 agreement between the U.K. and the U.S. on Access to Electronic Data for the Purpose of Countering Serious Crime, which, it says, "*will have to be taken into account by the European Commission in its overall assessment of the level of protection of personal data in the UK, in particular as regards the requirement to ensure continuity of protection in case of "onward transfers" from the UK to another third country*." The EDPB has indicated that if the Commission presents an adequacy decision in favor of the U.K., it will express its own view in a separate opinion. Absent an adequacy decision, transfers from the EEA to the U.K. would fall to be treated in the same way as transfers to other third countries, requiring consideration of Articles 46 and 49, SCCs, supplementary measures, etc.

A separate question is how the U.K. will, post-Brexit transition, treat these recommendations from the EDPB, and the question of transfers to third countries generally (and to the U.S. specifically). It cannot be excluded that this may be among the first area in which we begin to see a limited divergence between EU and U.K. data privacy laws.

It is also worth noting that on 12 November 2020, the European Commission published a draft implementing decision on SCCs for the transfer of personal data to third countries along with a draft set of **new SCCs**[ix]. The new SCCs include several modules to be used by companies, depending on the transfer scenario and designation of the parties under the GDPR, namely: (i) controller-to-controller transfers, (ii) controller-to-processor transfers, (iii) processor-to-processor transfers and (iv) processor-to-controller transfers. These new SCCs also incorporate some of the contractual supplementary measures recommended by the EDPB as described above. They are open for public consultation until 10 December 2020 and the final new set of SCCs are expected to be adopted in early 2021. At this stage, the draft provides for a grace period of one year during which it will be possible to continue to use the old SCCs for the execution of contracts concluded before the entry into force of the new SCCs[x].

In light of the above, we recommend that companies currently relying on SCCs to consult with their data protection officer or counsel to evaluate tailored ways to document and implement the steps to be taken in order to minimize the risks associated with continued data transfers to non-EEA countries — particularly to the U.S.

---

[i] The Charter of Fundamental Rights brings together all the personal, civic, political, economic and social rights enjoyed by people within the EU in a single text.

[ii] The European Essential Guarantees were originally drafted in response to the Schrems I judgment (CJEU judgment of 6 October 2015, Maximillian Schrems v Data Protection Commissioner, Case C-362/14, EU:C:2015:650).

[iii] Under article 49.2 of the GDPR, a transfer to a third country or an international organization may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.

[iv] The CJEU held, for example, that Section 702 of the U.S. FISA does not respect the minimum safeguards resulting from the principle of proportionality under EU law and cannot be regarded as limited to what is strictly necessary. This means that the level of protection of the programs authorized by 702 FISA is not essentially equivalent to the safeguards required under EU law. As a consequence, if the data importer or any further recipient to which the data importer may disclose the data is subject to 702 FISA, SCCs or other Article 46 of the GDPR transfer tools may only be relied upon for such transfer if additional supplementary technical measures make access to the data transferred impossible or ineffective.

[v] Example of contractual measures: The exporter could add annexes to the contract with information that the importer would provide, based on its best efforts, on the access to data by public authorities, including in the field of intelligence provided the legislation complies with the EDPB European Essential Guarantees, in the destination country. This might help the data exporter to meet its obligation to document its assessment of the level of protection in the third country. Such measure would be effective if (i) the importer is able to provide the exporter with these types of information to the best of its knowledge and after having used its best efforts to obtain it, (ii) this obligation imposed on the importer is a mean to ensure that the exporter becomes and remains aware of the risks attached to the transfer of data to a third country.

[vi] Example of technical measures: A data exporter uses a hosting service provider in a third country to store personal data, e.g., for backup purposes. The EDPB considers that encryption measure provides an effective supplementary measure if (i) the personal data is processed using strong encryption before transmission, (ii) the encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis performed by the public authorities in the recipient country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them, (iii) the strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved, (iv) the encryption algorithm is flawlessly implemented by properly maintained software the conformity of which to the specification of the algorithm chosen has been verified, e.g., by certification, (v) the keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of an intended recipient, and revoked), and (vi) the keys are retained solely under the control of the data exporter, or other entities entrusted with this task which reside in the EEA or a third country, territory or one or more specified sectors within a third country, or at an international

organization for which the Commission has established in accordance with Article 45 of the GDPR that an adequate level of protection is ensured.

[vii] Example of organizational measures: Regular publication of transparency reports or summaries regarding governmental requests for access to data and the kind of reply provided, insofar publication is allowed by local law. The information provided should be relevant, clear and as detailed as possible. National legislation in the third country may prevent disclosure of detailed information. In those cases, the data importer should employ its best efforts to publish statistical information or similar type of aggregated information.

[viii] It is worth noting that the EDPB indicates that it will provide more details "as soon as possible" on the impact of the Schrems II judgement on other transfer tools (in particular binding corporate rules and as hoc contractual clauses).

[ix] This set of new SCCs should be distinguished from the new draft of clauses published by the Commission on the same day which relates to Article 28.3 of the GDPR (also called SCCs by the Commission). This new draft of clauses will only be optional (the parties may choose to continue using their own data processing agreements) and is also subject to public consultation until 10 December 2020.

[x] Provided the contract remains unchanged, with the exception of necessary supplementary measures; on the contrary, in case of relevant changes to the contract or new sub-contracting, the old SCCs must be replaced by the new ones.

*The following Gibson Dunn lawyers prepared this client alert: Ahmed Baladi, Ryan T. Bergsieker, Patrick Doris, Kai Gesing, Alejandro Guerrero, Vera Lukic, Adelaide Cassanet, and Clemence Pugnet. Please also feel free to contact the Gibson Dunn lawyer with whom you usually work, the authors, or any member of the **Privacy, Cybersecurity and Consumer Protection Group**:*

Europe

Ahmed Baladi – Co-Chair, PCCP Practice, Paris (+33 (0)1 56 43 13 00, abaladi@gibsondunn.com)
James A. Cox – London (+44 (0)20 7071 4250, jacox@gibsondunn.com)
Patrick Doris – London (+44 (0)20 7071 4276, pdoris@gibsondunn.com)
Penny Madden – London (+44 (0)20 7071 4226, pmadden@gibsondunn.com)
Michael Walther – Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Alejandro Guerrero – Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)
Vera Lukic – Paris (+33 (0)1 56 43 13 00, vlukic@gibsondunn.com)
Sarah Wazen – London (+44 (0)20 7071 4203, swazen@gibsondunn.com)

Asia

Kelly Austin – Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Connell O'Neill – Hong Kong (+852 2214 3812, co'neill@gibsondunn.com)
Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com)

United States

Alexander H. Southwell – Co-Chair, PCCP Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Debra Wong Yang – Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Matthew Benjamin – New York (+1 212-351-4079, mbenjamin@gibsondunn.com)
Ryan T. Bergsieker – Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Howard S. Hogan – Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Joshua A. Jessen – Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)
Kristin A. Linsley – San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
H. Mark Lyon – Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Karl G. Nelson – Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Deborah L. Stein – Los Angeles (+1 213-229-7164, dstein@gibsondunn.com)
Eric D. Vandevelde – Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner – Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong – San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)