Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Significant Impact on Personal Data Transfers Due to the New Standard Contractual Clauses and Final Guidance on Supplementary Measures

September 27, 2021

On September 27, 2021, all new contracts that involve cross-border personal data transfers must incorporate the updated standard contractual clauses ("New SCCs") for controllers and processors. On June 4, 2021, the European Commission adopted its highly anticipated decision on the New SCCs. These New SCCs impose more onerous obligations on importers and exporters of personal data from the European Economic Area (EEA) and take account of Schrems II, including a requirement that businesses assess the laws and practices of the destination country to determine if they would prevent them from complying with their obligations under the New SCCs. Businesses with cross-border personal data transfers out of the EEA should begin reviewing their existing contractual arrangements and data processing operations now, because the transition period is short, by **December 27, 2022** all existing contracts need to be updated, and as of **September 27, 2021** for new contracts the New SCCs must be used. Supplementary measures will be an important consideration for any company relying on the New SCCs, binding corporate rules, or any of the other safeguards listed in Article 46(2) of the General Data Protection Regulation (GDPR) for data transfers to countries that do not offer sufficient data protection. We set out below the key features of the New SCCs and the European Data Protection Board's finalized recommendations on the use of supplementary measures.

Key Highlights of the New SCCs

The New SCCs replace the standard contractual clauses implemented under the old Data Protection Directive ("Old SCCs"), which were last updated in 2004 and 2010 for controller-to-controller and controller-to-processor transfers, respectively.

In terms of timing, until **September 27, 2021**, contracts were able to be concluded on the basis of the Old SCCs. As of September 27, 2021, any new contracts relying on standard contractual clauses as the mechanism for transfer of personal data must now implement the New SCCs. Any contracts concluded on the basis of the Old SCCs may only be relied upon until **December 27, 2022**, and businesses will have to have transitioned to the New SCCs by that date.

Contact Information

If you have any questions concerning this alert, please contact:

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505
Abud Dhabi
+971 2.406.8500

Michelle A. Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

Jenny Arlington
Counsel
jarlington@akingump.com
London
+44 20.7012.9631

Rachel Claire Kurzweil
Associate
rkurzweil@akingump.com
Washington, D.C.
+1 202.887.4253

Jay Jamooji
Associate
jay.jamooji@akingump.com
London
+44 20.7012.9845

Sahar Abas
Associate
sahar.abas@akingump.com
Dubai
+971 4.317.3052

The New SCCs span over 25 pages and adopt a layered, modular approach. The key highlights include the following:

1. **GDPR Spirit**. The New SCCs impose obligations on the data exporter and the data importer that are consistent with the GDPR, and the New SCCs should be read and interpreted in light of the GDPR. The New SCCs also address certain inconsistencies with the GDPR that were present in the draft proposal. For example the obligation to notify data subjects and the relevant supervisory authority in case of a personal data breach has been updated to refer to a breach that is likely to result in a risk to the rights and freedoms of individuals, as opposed to resulting in a "significant adverse effect" which was proposed in the November 2020 drafts.

2. **Wider range of parties / relationships allowed under a "modular" approach**. Under the New SCCs it is possible for more than two parties to adhere to the same set of SCCs, and additional controllers and processors (such as in the case of onward transfers of data) are permitted to accede to the SCCs throughout the life cycle of the contact by virtue of a "docking clause". Further, the New SCCs combine certain general clauses with a "modular approach" where parties can tailor the clauses for their specific transfer scenario, reflecting the complexity of modern processing chains.

3. **Obligation on all parties to conduct and record a transfer impact assessment**. The New SCCs address the concerns aired in Schrems II in relation to cross-border transfers to countries where no adequacy decision has been adopted by the European Commission. Specifically, the New SCCs include a declaration by the parties, in all modules, that they warrant that "**they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under [the New SCCs]**". The parties are obliged to take account of certain elements in order to carry out the assessment which underpins that warranty, such as the specific circumstances of data transfers (including the content and duration of the contract, the type of recipient and purpose of processing), the laws and practices of the third country destination that are relevant to the data transfer and any safeguards in place to supplement the measures under the New SCCs. Where the parties need to introduce qualifications to that warranty, they would need to implement so-called "supplementary measures" (see below). The New SCCs also state that the parties have to document the transfer impact assessment, and make it available to the relevant data protection regulator on request.

4. **Obligations on the data importer to notify exporter of public authority access request, and review the legality of such access request**. A data importer who receives a legally binding request from a public authority to disclose personal data transferred pursuant to the New SCCs, or who becomes aware of direct access to such data by the public authorities, is obliged to promptly notify the data exporter and, where possible, affected data subjects. If a data importer is prohibited, under the laws of the destination country, from notifying the data exporter or data subjects, the data importer must use its best efforts to obtain a waiver of the prohibition, with a view to be able to communicate as much information as possible and as soon as possible. The data importer must document its efforts and present that to the data

exporter on request. To the extent permissible, the data importer must regularly provide information about the requests it receives. Further, the data importer must review the legality of the request for disclosure, and challenge it (including on appeal) if there are reasonable grounds to do so under the laws of the destination country or international law. When responding to a request for disclosure, the data importer has to provide the minimum amount of information possible. With yet another obligation to document, the data importer is required to document its assessment and challenge of the access request and make the documentation available to the exporter and the relevant data protection authority on request.

5. **Transparency obligations**. The transparency obligations of a data importer who is a controller are strengthened, with the importer having to inform individuals, either directly or through the data exporter, of various details about the transfer, including "meaningful information" of the recipients in case of onward transfers of the data.

6. **Onward transfers**. The New SCCs elaborate on the restrictions on onward transfers, stating that a data importer cannot disclose the personal data to any third party that is in the country of the data importer or in another country outside the EEA, unless certain limited exemptions apply.

7. **Strengthening the data subjects' rights**. The New SCCs allow data subjects to enforce certain of their rights as third party beneficiaries against either the data importer or the data exporter. This contrasts with the position under the Old SCCs where a data subject was only permitted to proceed directly against a data importer if the data exporter, on the data subject's request, failed to take appropriate action against the data importer itself.

8. **Warranty by the data exporter and obligation to inform of the data importer**. The data importer has a number of obligations under the New SCCs, including those mentioned above. The New SCCs include a warranty by the data exporter that it has used reasonable efforts to determine that the data importer is able to satisfy its obligations under the New SCCs. Conversely, in the event that a data importer has reason to believe it cannot comply with the SCCs, it has to inform the data exporter. The data exporter must subsequently identify measures to address the situation, including in consultation with the relevant data protection authority if necessary and, in the event that no appropriate safeguards can be ensured, or if so instructed by the competent supervisory authority, the data transfer must be suspended.

9. **Submission of the data importer to a regulator in the EU**. The New SCCs state that the data importer agrees to submit itself to the jurisdiction of, and cooperate with, the relevant data protection regulator of an EU member state, including by responding to enquiries, making itself available for audits and complying with any measures adopted by the regulator (such as remedial and compensatory measures).

10. **Technical and organizational measures**. The New SCCs envisage that the parties in all modules agree on technical and organizational measures, including to ensure the security of the data. Annex II to the New SCCs lists 17 examples of such measures which parties could adopt, including pseudonymization and encryption, protection of data during transmission and during storage, ensuring physical security of locations, ability to restore availability and access, events logging, ensuring accountability, data minimization etc. These technical and organizational

measures are envisaged regardless whether parties implement supplementary measures or not; further, enhanced technical, organizational or contractual measures would be necessary if supplementary measures are required.

Supplementary Measures

Once parties carry out the transfer impact assessment envisaged under the New SCCs, they may decide that supplementary measures are required. Whilst such supplementary measures were referred to by the Court of Justice of the European Union (CJEU) in its Schrems II judgment, on June 18, 2021, the European Data Protection Board (EDPB) adopted Recommendations 01/2020 explaining what these measures might contain (the "Recommendations"). These measures were first published in draft form in November 2020 (see our alert here). The CJEU had acknowledged that data exporters are responsible for verifying on a case-by-case basis if the law or practice of the third country infringes on the effectiveness of the appropriate safeguards set out in the Article 46 GDPR transfer mechanisms, or tools. In these instances, the CJEU left open the possibility of implementing supplementary measures to fill any gaps and enhance the level of protection to the level required under EU law. As the CJEU did not further specify the nature or substance of such measures, the EDPB adopted the Recommendations to provide data exporters with a series of steps to follow, potential sources of information and certain practical examples of supplementary measures that could be adopted. Although the Recommendations are not legally binding, they serve as helpful guidance and an insight into the EDPB's approach to data transfers. The Recommendations should be closely considered by organizations relying on the New SCCs, binding corporate rules or other appropriate safeguards set out in Article 46 of the GDPR to transfer personal data outside the EEA.

Key features of the Recommendations include the following:

1. **A "roadmap" of steps to determine if supplementary measures are required**. The Recommendations contain a "roadmap" of steps to take in order for data exporters to determine if supplementary measures are required to be implemented to legally transfer data outside the EEA. Broadly, the EDPB advises exporters to: (i) understand their data transfers; (ii) verify the transfer tools relied upon; (iii) assess whether the law or practice in the third country impinges on the effectiveness of the relevant transfer tools (including standard contractual clauses, binding corporate rules and certification mechanisms); and (iv) if applicable, identify and adopt supplementary measures (including taking formal procedural steps and re-evaluating the level of protection at regular intervals) necessary to bring the level of protection of the data transferred to the EU standard.
2. **Access to data by public authorities must be considered**. In assessing whether there is anything in the law or practices in force in the third country that may impinge on the effectiveness of the appropriate safeguards relied upon, the Recommendations note that factors concerning access to data by public authorities "must" be considered; this includes whether public authorities may access data without the data importer's knowledge or access data through telecommunication providers.

3. **The practices of third countries must be considered**. Ultimately, the EDPB notes that the characteristics of each transfer must be considered, though the scope of the assessment should be limited to the legislation and practices relevant to the protection of the specific data being transferred. In particular, the Recommendations emphasize the need to consider the **practices** of the third country as well as the relevant legislation. For example, the Recommendations provide that while relevant legislation in the third country may formally meet EU standards on fundamental rights and freedoms, the practices of its public authorities may indicate they do not comply with the legislation governing their activities – in such instances, the practices of the public authorities must be taken into consideration such that the additional supplementary measures may be required. Organizations are further encouraged to take into account both their own experience and the experiences of other actors in the same sector dealing with similar data transfers. Likewise, the Recommendations recognize that in the absence of legislation in a third country (such as legislation on access to personal data held by the private sector) organizations cannot automatically presume the transfer tools can be effectively applied; instead, in such instances, organizations must review the indications of practices in force in the country and thereafter determine if additional supplementary measures are required.
4. **Differences between the Recommendations and the November 2020 draft recommendations**. Although the Recommendations broadly reflect the draft recommendations published in November 2020, there are notable differences. For example, where a transfer impact assessment indicates that the applicable legislation in the third country may be "problematic" (such as legislation not respecting the essence of the fundamental rights and freedoms recognized by the EU Charter of Fundamental Rights), the exporter may proceed with the transfer of data in the absence of additional supplementary measures, provided that the exporter considers that the problematic legislation will not be applied in practice. However, exporters must nevertheless be able to document and demonstrate in a detailed report that the relevant legislation will not be applied in practice. Annex 3 of the Recommendations include a comprehensive list of "possible sources" of information by which to assess a third country, such as case-law of the CJEU and resolutions and reports from inter-governmental organizations. Unlike the draft recommendations, the Recommendations do not limit the use of Article 49 GDPR derogations to "occasional and non-repetitive transfers", but instead emphasize that derogations cannot become "the rule" in practice and must be restricted to specific situations. The Recommendations also state that an essentially equivalent level of protection to that guaranteed within the EU must accompany personal data both "during and after the transfer".
5. **Examples of technical, contractual and organizational measures**. Annex 2 of the Recommendations set out a non-exhaustive list of possible technical, contractual and organizational measures that may be considered effective. The EDPB acknowledges that future technological, legal and organizational developments may result in the emergency of additional supplementary measures for organizations to consider. The adoption of one or more of the measures does not, however, necessarily mean that the transfer of data ensures an essentially equivalent level of protection to that which is required under EU law. Any supplementary measures adopted may only be deemed effective if, and

only to the extent that, the measures adopted specifically address the deficiencies identified in the assessment of the third country. In the event that an essentially equivalent level of protection cannot be afforded, even with the adoption of certain supplementary measure, exporters must not transfer the personal data, unless one of the limited derogations in the GDPR can be relied upon.

6. "**Use case" examples**. Annex 2 contains seven "use cases", comprising practical situations in which effective measures are and are not identified. One such use case concerns a situation in which a data exporter pseudonymizes data it holds and transfer this data to a third country for analysis (e.g., for research). According to the EDPB, the pseudonymization may be deemed an effective supplementary measure if certain features are present, including: the data no longer being attributable to a specific data subject, the additional information being held exclusively by the data exporter and kept separately in a member state or third country, disclosure or unauthorized use of the additional information being prevented by technical and organizational safeguards, and the controller establishing that the pseudonymized data cannot be attributed to an identified or identifiable natural person (even if cross-referenced with such additional information) following a "thorough analysis of the data in question". The internal policies and procedures of an organization can be an effective supplementary measure, particularly when complimenting technical and contractual measures. One example from the Recommendations is the commitment to transparency by thorough documentation of all requests for access from public authorities.
7. **Practical steps** – mapping international data transfers. Organizations should immediately begin mapping their international data transfers, with each transfer tied to an appropriate transfer tool. A thorough analysis will be required to identify the right supplementary measure for the specific circumstances.

Article 28 Clauses where there is no transfer outside the EEA

Where the processing involves a cross-border element outside the EEA, entering into the New SCCs will also satisfy the requirements of Article 28 of the GDPR, which requires that a data processing agreement, covering specific topics, is in place between a controller and a processor.

Where the processing of personal data does not involve a transfer out of the EEA, there still needs to be an Article 28 compliant agreement between a controller and a processor. On June 4, 2021, the European Commission adopted its decision on Article 28 standard contractual clauses between controllers and processors ("Article 28 Clauses"). The Article 28 Clauses include provisions that a data controller can impose upon a data processor to satisfy the requirements set out under Article 28 of the GDPR.

Next Steps

The New SCCs significantly increase the level of diligence required both by the data importer and the data exporter before a personal data transfer can be carried out in reliance on the SCCs. Specifically, business will have to assess the impact of local laws and practices on data transfers and on the business' ability to comply with the

mandatory obligations under the New SCCs. Similar to the Old SCCs, the provisions of the New SCCs are non-negotiable and non-amendable.

Businesses should begin to identify any contractual arrangements with third parties that rely on the Old SCCs for the transfer of personal data, as it will only be possible to do so until December 27, 2022. It is important to start this process in a timely manner, given that the parties will be required (among other things) to carry out local laws and practices assessments and include detailed security measures when transitioning to the New SCCs. Businesses may wish to consider whether they are best placed to make such assessments or whether obtaining local law advice would be advisable. Practices and procedures would have to be put in place in order to allow compliance with the obligations set out in the New SCCs. Changes to operations may also be required, if the transfer cannot be executed in reliance on the New SCCs.

Businesses that are entering into new contracts with third parties must now adopt the New SCCs at the outset, as it is no longer permitted to enter into new contracts using the Old SCCs.

akingump.com