THOMPSON HINE

Privacy & Cybersecurity Update

June 2021

EU Approves New Standard Contractual Clauses for Cross-Border Data Transfers

On June 4, the European Commission adopted new Standard Contractual Clauses (SCCs) to enable organizations to transfer personal data outside the European Union (EU) in accordance with the General Data Protection Regulation (GDPR). The new SCCs are intended to address the complex data processing issues that impact modern businesses, and they impose several novel obligations on organizations. Importantly, the new SCCs address situations where the U.S. government (and other non-EU authorities) request access to personal data, which was the core issue presented in the recent *Schrems II* decision. In order to comply with the GDPR and SCCs, organizations should consider undertaking the following:

- identify the circumstances in which they export or import personal data from the EU,
- determine whether the SCCs are an appropriate data transfer mechanism, and whether they can comply with the onerous requirements set forth in the new SCCs,
- amend existing third-party contracts and intra-group agreements to account for the new SCCs,
- incorporate the new SCCs into contracting process flows for new programs and operations, and
- implement new procedures, where appropriate, and document all policies and assessments for data transfers.

The existing SCCs will be repealed in three months, and, at that juncture, organizations cannot rely on them for new personal data transfers. In the event organizations have executed agreements that incorporate the existing SCCs, those agreements will remain valid for 18 months.

Background and UK Transfers

The existing SCCs address two data transfer frameworks (i) controller-to-controller (C2C) and (ii) controller-to-processor (C2P). The new SCCs continue to address both the C2C and C2P transfers and add two new frameworks (iii) processor-to-processor (P2P) and (iv) processor-to-controller (P2C) transfers. In turn, organizations subject to the GDPR are required to select the data transfer "Module" most applicable to their business model. Although many of the provisions within the new SCCs mirror the requirements set forth in Article 28 of the GDPR (e.g., the parties must define the nature and scope of data processing, provide certain types of assistance to better ensure data protection compliance), they also create new data processing obligations that parties may find burdensome. Organizations are permitted to incorporate additional contractual provisions into the SCCs, provided, however, they do not contradict the terms, conditions and rights set forth in the new SCCs.

Although the SCCs will not automatically be applicable with respect to data transfers from the UK, the Information Commissioner's Office indicated that it will adopt a similar set of data transfer clauses for UK transfers.

Third-Party Rights, Dispute Resolution and Liability

The SCCs furnish data subjects the right, with some exceptions, to invoke and enforce the SCCs as third-party beneficiaries against the data exporter and/or data importer. In addition, data importers are specifically required to inform data subjects in a transparent and easily accessible format (e.g., individual notice, website postings) of a point-of-contact responsible for addressing data subject complaints. The SCCs provide an optional provision wherein the data importer would agree to allowing data subjects to lodge complaints with an independent dispute resolution body, provide the

body is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

A party that breaches its obligations under the new SCCs is liable to the non-breaching party for damages the latter incurs. The different Modules (i.e., C2C, C2P, P2P and P2C) set forth requirements regarding (i) the scope of damages a party may recover in the event of a breach, (ii) joint and severable liability, and (iii) when a party can "claim back" compensation corresponding to its damages proffered in response to a claim.

Government Access Requests

The new SCCs address the *Schrems II* decision with respect to government access requests and therefore will help organizations to more uniformly comply in this area. In fact, Section III of the new SCCs (Local Laws and Obligations in Case of Access by Public Authorities) applies to the C2C, C2P and P2P Modules, and the P2C Module where the EU processor combines personal data received from the third country-controller with personal data collected by the processor in the EU. The new SCCs require each party to warrant that they "have no reason to believe" that the laws of the importing country, including any legal requirements furnishing public authorities with the right to access personal data, would "prevent the data importer from fulfilling its obligations" under the new SCCs. In order to make this warranty, the SCCs indicate that the parties should assess the specific circumstances of the transfer, including:

- the length of the processing chain,
- the number of actors involved and the transmission channels used,
- intended onward transfers,
- the type of recipient and the purpose of processing,
- the categories and format of the data transferred,
- the applicable economic sector, and
- the storage location of the data transferred.

In addition to the foregoing, the SCCs provide that the parties should assess (i) the importing country's laws, including the context in which they furnish public authorities rights to access personal data, and (ii) any supplemental contractual, technical or organizational safeguards relevant to the transfer (e.g., measures applied during transmission and to the processing of the personal data in the country of destination). The parties must document and retain these assessments and provide them to supervisory authorities upon request. The SCCs create additional obligations and processes (i) in the event a party can no longer comply with its warranty, (ii) if a party receives a government access request, and (iii) for issuing transparency reports.

Data Security

Given the substantial number of ransomware attacks and data breaches impacting the business community, it is not surprising that the SCCs focus on information security practices. Like its C2P predecessor, the new SCCs delineate the circumstances in which the parties need to document their technical and organizational security in Annex II. However, the new SCCs emphasize that these measures must be described with specificity and not in "generic" terms. In addition to listing the security controls already found in Article 32 of the GDPR, the new SCCs provide the following examples of potentially applicable technical and organizational security measures the parties must implement and maintain:

- user identification and authorization,
- measures to protect data during transmission and at-rest,
- ensuring physical security of data processing facilities,
- ensuring events logging and system configuration,
- measures for internal IT and IT security governance and management, and accountability,
- measures for ensuring data minimization, data quality, and limited data retention, and
- measures for allowing data portability and ensuring erasure of personal data.

Although the SCCs emphasize the potential for including any relevant third-party certifications as part of the SCCs, such security certifications and assurances are only one part of the security process and is not a substitute for a party's broader diligence obligations.

Sub-processors

Clause 9 of the SCCs (Use of Sub-processors) sets forth a framework for employing sub-processors that is similar to Article 28 of the GDPR. For instance, when a data importer engages a sub-processor pursuant to either the C2P or P2P

Modules, the (i) parties may agree to the use of specific, prior authorization of each sub-processors or a general written authorization, and (ii) the data importer must remain fully responsible to the data exporter for the sub-processor's acts or omissions. For the C2P and P2P Modules, the parties must complete Annex III of the SCCs, which delineates the list of approved sub-processors.

Conclusion

Organizations may have to adopt new policies and procedures to comply with the SCCs. For instance, organizations should consider implementing and maintaining a formal government access request policy so they can both efficiently and effectively respond to such requests and comply with the provisions within the SCCs regulating the same. Similarly, they should consider publishing, quarterly, bi-annually, or annually, a transparency report describing how many (if any) government access requests they receive during the applicable time period. However, organizations should not only be prepared to draft and adopt new policies and procedures to comply with the new SCCs, but also ensure they are continuously monitored and evaluated to demonstrate on-going compliance.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G), Certified Information Privacy Professional/United States (CIPP/US)

Elizabeth H. Blattner
937.443.6826
Elizabeth.Blattner@ThompsonHine.com

Jennifer N. Elleman
937.443.6927
Jennifer.Elleman@ThompsonHine.com

Thomas F. Zych
216.566.5605
Tom.Zych@ThompsonHine.com

or any member of our Privacy & Cybersecurity group.