Key Takeaways From the European Commission's Article 28 Standard Contractual Clauses

by David Dumont and Bridget Treacy, Hunton Andrews Kurth LLP, with Practical Law Data Privacy Advisor

Articles | Law stated as of 02-Aug-2021 | European Union, United Kingdom

An Article discussing the background and key takeaways from the European Commission's new standard contractual clauses (SCCs) between EEA-based controllers and processors under GDPR Article 28(7).

On June 4, 2021, the European Commission adopted final versions of two Implementing Decisions on standard contractual clauses (SCCs):

- Implementing Decision and Annex on SCCs for the transfer of personal data from the EEA to third countries (Transfer SCCs); and
- Implementing Decision and Annex on SCCs between controllers and processors under GDPR Article 28(7) (Article 28 SCCs).

(For more, see Legal Update, European Commission adopts final versions of standard contractual clauses under EU GDPR.)

Most attention has focused on the Transfer SCCs applicable to cross-border data transfers. However, the European Commission also issued Article 28 SCCs for data transfers between controllers and processors within the European Economic Area (EEA) enabling organizations to meet their EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) Article 28 obligations using standardized terms.

GDPR Article 28 sets out the minimum requirements that a controller must impose on a processor when outsourcing or subcontracting personal data processing activities, including implementing a contract that defines the scope of the personal data processing activity and imposing certain requirements on the processor (see GDPR Article 28 Contractual Requirements).

The GDPR permits national data protection authorities and the European Commission to adopt standard contractual clauses (SCCs) which controllers and processors may choose to implement to meet their GDPR Article 28 obligations (Articles 28(3), (4), (7), (8) and Recital 81, GDPR). The Danish Data Protection Authority and the Slovenian Data Protection Authority both submitted Article 28 SCCs to the European Data Protection Board (EDPB).

GDPR Article 28 Contractual Requirements

The previous EU Data Protection Directive (Directive 95/46/EC) imposed a general obligation on EEA controllers to implement data processing agreements with processors. However, the specific requirements for these data processing agreements varied significantly at EU member state level, resulting in confusion and uncertainty for multinational organizations.

The GDPR introduced prescriptive requirements for data processing agreements, requiring any agreement to set out:

- The subject-matter and duration of the processing.
- The nature and purpose of the processing.
- The type of personal data and categories of data subjects.
- The controller's obligations and rights.

(Article 28(3), GDPR.)

The data processing agreement must also require the processor to:

- Process personal data only on the controller's documented instructions.
- Impose confidentiality obligations on all personnel authorized to process the personal data.
- Implement appropriate technical and organizational information security measures.
- Only engage sub-processors with general or specific authorization from the controller and implement an agreement to flow down the processor's data protection obligations to the sub-processor.
- Implement measures to assist the controller in responding to data subject rights requests.
- Assist the controller to comply with its obligations concerning information security, data breach notification, data protection impact assessments and prior consultations with supervisory authorities.
- At the controller's election, delete or return the personal data at the end of the relationship, unless EU or national law requires a longer retention period.

In practice, most organizations subject to the GDPR have developed their own template data processing agreements which suit their ways of working and risk appetite. Smaller controllers are often forced to accept the data processing terms of larger vendors which typically seek to limit certain data protection requirements that must be imposed under GDPR Article 28.

For more, see Practice Note, Data Processor Obligations Under the GDPR: Processor Contractual Requirements.

Article 28 SCCs: Key Takeaways

Scope

The Article 28 SCCs can be used when an EEA-based processor processes personal data on behalf of an EEA-based controller. The Transfer SCCS incorporate the Article 28 SCCs and should be used to meet the GDPR Article 28 requirements where the processor is both:

- Located in a non-adequate jurisdiction outside the EEA.
- Falls outside the GDPR's territorial scope of the GDPR.

It remains unclear if the new Article 28 SCCs can be used for transfers to non-EEA processors that are directly subject to the GDPR based on Article 3(2). On a generous reading of the Transfer SCCs this may be possible, but the position is unclear and further guidance from data protection authorities is needed.

No Amendment

The Article 28 SCCs are standard clauses approved by the European Commission. The parties can only amend the clauses where explicitly permitted in the text, for example where specific options are given or where additional information is required, such as to complete the various annexes (Clause 2(a), Article 28 SCCs).

Inclusion in a Wider Contract

The parties can incorporate the Article 28 SCCs into a wider agreement or supplement them with further clauses or additional safeguards, provided that any additions:

- Do not contradict or dilute the Article 28 SCCs.
- Negatively impact data subjects' fundamental rights or freedoms.

(Clause 2(b), Article 28 SCCs.)

For example, the parties may seek to limit liability as between themselves, usually by making the Article 28 SCCs subject to any limitation of liability contained in the relevant services agreement. Provided the amendment does not limit liability in relation to a data subject, such an amendment is permitted, and is regarded as a commercial issue. There is little substantive guidance concerning what further clauses or additional safeguards can be incorporated, but in practice parties can push the boundaries of what is likely to be permitted. Where there is a conflict between the SCC provisions and the provisions of related agreements between the parties, the SCCs must prevail (Clause 4, Article 28 SCCs).

Complex Data Processing Chains

The Article 28 SCCs accommodate multiparty scenarios by allowing multiple controllers and processors to complete Annex I. There is also an optional accession mechanism or docking clause enabling new controllers or processors to join during the lifetime of the Article 28 SCCs (Clause 5, Article 28 SCCs). This adds flexibility and recognizes the reality of complex and evolving data processing chains. The accession mechanism is straightforward, however parties should consider whether new parties should accede to the Article 28 SCCs only or the whole agreement. Acceding to the whole agreement is likely in an intragroup context, and any accession mechanism should apply to the agreement as a whole rather than the Article 28 SCCs alone. In other cases, there may be commercial reasons why multiple parties will enter into separate agreements addressing the same data processing activities. Where there are separate commercial agreements, separate Article 28 SCCs should also be used.

The Commission Decision appears to anticipate the parties completing a single master signature page. This is unlikely to be workable in practice, and parties are likely to add a provision enabling signatures in counterpart.

New parties are liable once they complete and sign the applicable Annexes (Clause 5(b), Article 28 SCCs). New parties have no rights or obligations before signing the applicable Annexes (Clause 5(c), Article 28 SCCs).

Data Protection Obligations

The Article 28 SCCs are designed to satisfy the requirements of GDPR Article 28 (see GDPR Article 28 Contractual Requirements). The Article 28 obligations are not repeated here, but it is worth noting the following:

- **Instruction rights**. One of the core features of a controller-processor relationship is that the processor must process personal data according to the controller's instructions. The draft version of the Article 28 SCCs released in November 2020 contained a dedicated annex in which parties may document the controller's instructions. This annex was not retained in the final version of the Article 28 SCCs. The European Commission requires the controller to provide a description of the data processing activities in an annex, which is in line with current market practice.
- **Purpose limitation**. Clause 7.2 of the Article 28 SCCs requires processors to process personal data according to the purpose limitation principle, unless it receives further instructions from the controller. Although a key GDPR principle, including an explicit reference to purpose limitation in the Article 28 SCCs is surprising as the GDPR itself does not impose direct obligations on processors in terms of purpose limitation and is not included as a requirement in Article 28. This provision is favorable to controllers, who otherwise must ensure compliance with the purpose limitation principle by restricting the processor's ability to process personal data except according to the controller's instructions. This is as an example of the European Commission "gold-plating" the GDPR. Processors must be aware of this provision and ensure compliance with it before signing the Article 28 SCCs.
- **Technical and organizational measures.** The explanatory notes to Annex III of the Article 28 SCCs clarify that a generic description of the technical and organizational measures implemented to secure data is not sufficient. The measures must be described concretely and in detail. The European Commission set out examples of the types of measures which the parties may consider in Annex III, which includes measures to protect data in transit.
- **Sensitive data**. The Article 28 SCCs require processors to apply specific restrictions and safeguards where its processing activities involve processing personal data revealing:
  - racial or ethnic origin;
  - political opinions;
  - religious or philosophical beliefs;
  - trade union membership;
  - genetic data;
  - biometric data;
  - data concerning health or sex life
  - sexual orientation; or
  - data relating to criminal convictions and offenses.

  (Clause 7.5, Article 28 SCCs.)

  The draft Article 28 SCCs combined this section with a specific annex which listed the additional restrictions and safeguards concerning the processing of sensitive personal data. The final version does not include this annex. The processor must instead identify the additional restrictions and safeguards relating to the sensitive personal data processing in the main description of the processing activities in Annex II. This may be viewed as on onerous addition for the processor, however in practice it is likely to be helpful for the processor to specify these safeguards. The processor will likely have standard procedures that apply across all of its services and will not wish to customize these for individual customers. The European Commission has provided examples of the types of additional restrictions and safeguards that may be implemented considering the nature of the data and the risks involved, including:

- strict purpose limitation;
- access restrictions (including access only for staff that have received specialized training);
- maintaining a record of access to the data;
- onward transfers restrictions; and
- additional security measures.

(Annex II, Article 28 SCCs.)

- **Documentation and compliance.** In line with the GDPR's accountability principle, the Article 28 SCCs require the parties to be able to demonstrate compliance with the clauses. From the processor's perspective, this accountability obligation requires the processor to:

  - promptly respond to the controller's inquiries;
  - make information available to the controller to demonstrate compliance with the Article 28 SCCs and the processor's direct obligations under the GDPR; and
  - allow and contribute to audits carried out by the controller or an independent auditor mandated by the controller. The Article 28 SCCs limit the controller's audit rights to reasonable intervals with reasonable notice, while allowing additional audits if non-compliance is indicated.

  (Clause 7.6, Article 28 SCCs.)

  Interestingly, the final text did not retain the possibility of the controller relying on an independent auditor mandated by the processor. The controller may instead, but is not required, to consider the processor's certifications when exercising its oversight. (Clause 7.6, Article 28 SCCs.)

- **Sub-processors**. The Article 28 SCCs incorporate the two options provided under the GDPR concerning the engagement of sub-processors. The controller can provide the processor with either:

  - general authorization to engage sub-processors combined with a duty to inform the controller and allow a reasonable time for objection to new sub-processors; or
  - specific authorization each time the processor wishes to engage a new sub-processor.

  (Clause 7.7(a), Article 28 SCCs.)

  Annex IV of the Article 28 SCCs lists the approved sub-processors and must be kept updated during the contract lifecycle. This largely mirrors the GDPR Article 28(2) requirements for the engagement for sub-processors. However, the Article 28 SCCs impose an additional obligation on the processor to provide the controller with information necessary to make its decision to accept or object to the engagement of a new sub-processor (Article 7.7(a), Article 28 SCCs).

Similarly to Article 28(4) of the GDPR, the Article 28 SCCs require the processor to put in place a contract with its sub-processors but appear to slightly lower the standard for the sub-processing agreement. Whereas the GDPR requires that the sub-processing agreement imposes the same data protection obligations, the Article 28 SCCs provide that the obligations should be the same "in substance" which better reflects the business reality that the parties involved in a data processing chain are not necessarily bound by identical data protection provisions (Clause 7.7(b), Article 28 SCCs). However, the Article 28 SCCs require the processor to include a third-party beneficiary clause in its sub-processor agreement, enabling the controller to terminate the sub-processing agreement and to instruct the sub-processor to erase or return the personal data where the processor disappears, ceases to exist in law or becomes insolvent (Clause 7.7(e), Article 28 SCCs). Processors should ensure that they are aware of any additional obligations imposed in the Article 28 SCCs and that those obligations are flowed down as appropriate to any sub-processing agreements prior to signing the Article 28 SCCs.

- **Termination.** The final version of the Article 28 SCCs grant processors an additional termination right where a processor informs a controller that its instructions infringe applicable legal requirements, and the controller insists on compliance with its instructions (Clause 10(c), Article 28 SCCs). Consistent with GDPR Article 28, the Article 28 SCCs permit the controller to decide whether the processor must delete or return the personal data at the end of the relationship, unless EEA or national law requires a longer retention period. The Article 28 SCCs also impose an obligation on the processor to certify to the controller that it has deleted the personal data and if applicable law requires a longer retention period, the processor must continue to ensure compliance with the Article 28 SCCs (Clause 10(d), Article 28 SCCs).

Brexit

As the European Commission adopted the new Article 28 SCCs after the UK left the EU, they do not form part of retained EU law and cannot be used in the UK. It is unclear whether the UK Information Commissioner's Office intends to publish equivalent clauses or whether UK organizations intend to use the Article 28 SCCs as a non-binding starting point when drafting UK Article 28 agreements.

Practical Implications

The Article 28 SCCs are not mandatory, but organizations may wish to review their existing Article 28 provisions and consider updating them in line with the Article 28 SCCs. Many organizations are likely to conclude that their existing approach to GDPR Article 28, combined with additional processor clauses that have been honed overtime, offers sufficient protection without the need to adopt the new Article 28 SCCs. However, there may be some features of the SCCs that are adopted in new contracts, such as the addition of a straightforward docking clause.

More generally, the new Article 28 SCCs are likely to be of interest to smaller businesses, offering a welcome template that can easily be adapted. However, organizations should review and familiarize themselves with the new Article 28 SCCs as there are some provisions which are more favorable to one party than the other and some provisions which go beyond what the GDPR strictly requires.

Organizations ultimately must make a strategic decision on whether they implement some or all of the clauses in their processing agreements as some provisions may be attractive or unattractive depending on the organizations' role in the processing activity and position in the supply chain. The fact that the European Commission has adopted the Article 28 SCCs is likely to be welcomed and may discourage individual EEA countries from seeking to promote their own versions of these clauses. Only time will tell how businesses use the Article 28 SCCs, but overall, these clauses are a positive step.

END OF DOCUMENT