CEDPO

CONFEDERATION OF EUROPEAN
DATA PROTECTION ORGANISATIONS

Bonn, Bucharest, Dublin, Lisbon, Madrid, Milan, Paris, The Hague, Vienna, Warsaw

European Commission
DG Justice and Consumers
Unit JUST C.3 - Data Protection
Unit JUST C.4 - International data flows and protection
1049 Brussels/Belgium

Attn: Raffaella Papes/Alisa Vekeman/Olivier Micol

By email: JUST-C3@ec.europa.eu; JUST-C4@ec.europa.eu

December 14th, 2020

Dear Ms. Papes, Dear Ms. Vekeman, Dear Mr. Micol,

as members of the national professional organisations constituting CEDPO (the Confederation of European Data Protection Organisations), we would like to thank you for giving us the opportunity to comment on the Draft Standard Contractual Clauses for data transfers within the EU and to third countries.

If you have any questions concerning our comments, please do not hesitate to contact us.

Yours Sincerely,

Steffen Weiß

On behalf of the members of the Confederation of Data Protection Organisations

CEDPO

CONFEDERATION OF EUROPEAN
DATA PROTECTION ORGANISATIONS

About CEDPO:

CEDPO was founded in September 2011 by European Data Protection Organisations, namely, AFCDP (Association Française des Correspondants à la Protection des Données à Caractère Personnel) of France, APEP (Asociación Profesional Española de Privacidad) of Spain, GDD (Gesellschaft für Datenschutz und Datensicherheit) of Germany, and NGFG (Nederlands Genootschap van Functionarissen voor de Gegevensbescherming) of the Netherlands. In February 2014, ADPO (The Association of Data Protection Officers) of Ireland, ARGE DATEN of Austria, and SABI (Stowarzyszenie Inspektorów Ochrony Danych) of Poland joined CEDPO. The latest to additions to CEDPO took place between 2018-2020 when ASSO DPO (Associazione Data Protection Officer) of Italy, AEPD (Associação de Encarregados de Proteção de Dados) of Portugal and ASCPD (Asociatia Specialistilor in Confidentialitate si Protectia Datelor) of Romania became member associations.

CEDPO aims to promote the role of the Data Protection Officer, to provide advice on balanced, practicable, and effective data protection and to contribute to a better harmonisation of data protection law and practices in the EU/EEA.

Contact information

Email: info@cedpo.eu / Website: www.cedpo.eu

I. Comments on Standard Contractual Clauses EU (Article 28) for processing personal data within the EU

It is regretted that the public link to these clauses was not easily available because of a malfunction. CEDPO comments made on the art 46 SCC which are identical to these Clauses are valid also for these Clauses and not repeated below.

SECTION II OBLIGATIONS OF THE PARTIES

Clause 7

Obligations of the Parties

- (a) The data processor should inform the data controller of the requirements in Union or Member State law applicable to its organisation obliging the processor to process personal data outside the instructions of the controller unless this is prohibited by Union/Member State law.

7.2. Erasure or return of data

- It should also be acknowledged that personal data may be stored even after the termination of the contract between the parties, for a period of time, such as the time limit set by Union / Member State law or even by the parties themselves (e.g., to keep personal data to evidence proper performance of a contract).

7.3. Security of processing

- (a) The reference made to the "personal data breach" in the first sentence seems unnecessary.

  Instead of requiring the processor to notify the controller of a personal data breach "without undue delay and at the latest within 48h …" in order to take a more realistic approach reflecting experience it could be specified that "the processor shall notify the data controller of a personal data breach without undue delay and where feasible at the latest within 72h after becoming aware of the breach."

  Besides, changes to technical and organisational measures are not reflected in the Clauses. The processor should be allowed to make changes to security measures, but these changes may not undermine the initial assured level of data security. The data processor should be obliged to inform the data controller of significant changes to its technical and organizational measures in order to allow the controller to assess the adequacy of these changes.

7.6. Use of sub-processors

- (a) It could be specified in case of general authorizations that sub-processors would be automatically approved if they meet a list of detailed criteria, pre-approved by the data controller (e.g., member or not of the same corporate group, holder of a specific ISO or service license, adherence to a specific Code of Conduct, presence in a specific region, etc.)

7.7 International data transfers

- (a) Under this section, the parties agree in advance, that in case of data transfers, SCCs may be used as safeguards. They could also agree to data transfers to adequate countries or if safeguards are approved BCRs.

Clause 8

Data subject rights

- (b) The obligation of the data processor to assist the data controller is reasonable but should be subject to the nature of the processing and the information available to the data processor. Especially in cases of some SaaS services the processor may be unaware of the scope of the data processing by the data controller.

- (c) This paragraph deserves a specific Clause called "Other obligations" as they are not related to data subject rights.

- (d) This section should be either in the Clause "other obligations" or added to Clause 7.3.d.

Clause 9

Notification of personal data breach

- General remark: The data processor obligations with regard to a personal data breach are not just mentioned in Clause 9 but also in other Clauses (7.3., 8 (c)). It would make sense to stipulate the processor's obligations in one single Clause 9.

- (a) The name of the SA is not relevant information for the data processor. What is required from the processor is to provide the data controller with the information needed by the data controller, whatever the SA may be. In addition, the name of the SA may not be known at the time of signature of the agreement if the processing activity relates to the data of individuals located in several Member States but only some of them are impacted by the breach

- (b) It cannot be anticipated in advance, what elements the data processor will have to provide to assist the data controller, as it is contextual, it will depend on the breach and on the form and requests of the SA.

Annex III Technical and organizational measures

- In practice, technical and organizational measures are predefined by data processors subject to a certain assured level of data security; the standard contractual clauses should enable the parties to make reference to data security reports, audit reports or security certifications.

Annex V: Specific restrictions and/or additional safeguards concerning data of special category

- Extended guidance would be helpful concerning additional technical and organizational measures in cases of a processing of special categories of data. Sect. 22(2) of Germany's Federal Data Protection Act makes reference to further measures, such as:
  - measures to ensure that it is subsequently possible to verify and establish whether and by whom personal data were input, altered or removed;
  - measures to increase awareness of staff involved in processing operations;
  - designation of a data protection officer;
  - restrictions on access to personal data within the controller and by processors;
  - the pseudonymization of personal data;
  - the encryption of personal data;
  - measures to ensure the ability, confidentiality, integrity, availability and resilience of processing systems and services related to the processing of personal data, including the ability to rapidly restore availability and access in the event of a physical or technical incident;
  - a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Annex VI: List of sub-processors

- The list of sub-processors should indicate a certain level of information, such as,
  - Name of the entity/person
  - Processing tasks
  - Location of processing establishment(s)

II. Comments on Standard Contractual Clauses (Art. 46) for data transfers outside the EU

- **Sunset period.** We welcome the one year sunset period, that will probably be insufficient for organisations that have implemented a great number of SCCs. Indeed, the experience of the execution of SCCs after the Safe Harbor invalidation proved to be a burdensome exercise, that took more than 2 or 3 years to complete, in many circumstances because numerous organisations took the opportunity to re-open commercial aspects of the main agreements to which the Clauses use to be incorporated by way of annexes or otherwise. Reference should be made also to include Clauses under Decision 2004/915/EC under this sunset period.

Clarification in the Decision would be welcome by a clear indication that after the sunset period all previously concluded Standard Contractual Clauses are no longer valid and cannot constitute appropriate safeguards to the data transfers.

- **Appropriate interplay with Art. 3(2) GDPR.** We also welcome the fact that these Clauses can be used by exporters which are not established in the EU but subject to GDPR (Art. 3(2)) with data importers that are not subject to GDPR. There is a need to clarify in FAQs or in the Decision whether two parties located outside of the EU and not subject to GDPR could use these Clauses (e.g. in the framework of an onward transfer). Since these Clauses would not apply to data transfers between parties which are both subject to GDPR, it would be helpful to provide clear guidance on the interplay between the rules on international data transfers and the territorial scope of the GDPR. In particular, it would be important to expressly confirm (in the Clauses, the Decision and/or the FAQs) that Clauses are not necessary as long as GDPR is directly applicable to the parties involved in the transfer.

- **Consistency with the GDPR and ECJ risk-based approach.** We also welcome the risk-based approach of the Clauses which is aligned both with the GDPR and the ECJ decision. Indeed, the safeguards shall take into account all the circumstances of the transfer and therefore rely on the assessment of the likelihood and severity of harm to individuals as well as the benefits. The Commission should work together with the EDPB so that this approach is also reflected in the EDPB final recommendations that are expected to operate consistently with the Clauses.

- **Standard Data Protection Clauses.** Should the clauses be entitled Standard Data Protection Clauses (SDPC) and not Standard Contractual Clauses (SCC) as indicated in Art. 46(2) D GDPR (even though the rest of the Regulation retains the SCC terminology)? The same is true in the French version of the GDPR.

- **Interplay with commercial arrangements.** Since the Clauses are to be incorporated in wider contracts, attention shall be paid to clauses that are commercial by nature in order to avoid conflicts and leave the parties the freedom to regulate them as appropriate. This includes, in particular, indemnity, liability or the mechanics and costs addressed in audit clauses.

- **Flexibility regarding Art. 28 GDPR implementation.** Art. 28 provisions as drafted in the Clauses shall be understood as one possible manner to implement Art. 28 in practice. Organisations may have already invested substantial time and resources (and negotiation efforts) for compliance with Art. 28 GDPR in a different (and sometimes more sophisticated). Adding a mandatory wording that cannot be varied may not fit to all C2P/P2P situations.

- **Methodology to provide comments.** Comments are stated only once. They are not repeated when the clauses are the same for each model.

- **Defined terms.** Neither the terms ‘data exporter’ and ‘data importer’ are defined within the Clauses. Since all parties have to agree on their role within the contractual framework, a definition of these terms is considered beneficial.

Clause 6 Optional

Docking Clause

(a) Entity should be replaced by a person or an organization and then the term should be defined as the data may be transferred by or received by a solo practitioner or by a body which is not an “entity”.

(b) The accession may occur as described in Clause (b) or by any other binding mechanism in accordance with applicable law.

(c) The Clause shall foresee that the date of the entry into force of the rights and obligations for and with respect to the acceding Parties under the Clauses might not coincide with the signing date (e.g., agreed retroactive effects or future effects because the completion of the relevant main agreement to which these Clauses are appended is subject to condition precedents).

SECTION II OBLIGATIONS OF THE PARTIES

Clause 1

Data protection safeguards

MODULE ONE: Transfer controller to controller

- 1.1 If the intended processing is not compatible with the options laid out in the SCCs (Annex I.B.), the Clauses should allow the data importer to use the appropriate GDPR legal basis (Art. 6 or Art. 9 GDPR, as applicable), which are not limited to consent.

- 1.2 (a) (iii) This article requires to inform of the identity of the third party to whom data is disclosed. This goes further than Articles 14 and 13, which only require an information on “categories of recipients”.

- 1.3 (b) It should be specified that this article applies only if one of the Parties becomes aware of an inaccuracy during the performance of the agreement, if there is an ongoing relationship between the two controllers and if both controllers pursue the same processing purposes. Indeed, in practice after the performance of the agreement, several months or years after, the data importer will no longer inform the data exporter of an inaccuracy. Further, the obligation of the parties to keep the others updated of the accuracy of the data does not make sense in all instances where the data importer and the data exporter do not continue to process the same data for the same purposes. In addition, this obligation cannot be indefinite. The data subject will have an independent relationship with each controller and shall be able to determine which data it continues sharing with each of them (example: it may have different shipping addresses for each of them).

- 1.3 (c) Both controllers (and not only the data importer) shall ensure that the data are proportionate to the purpose of the data transfer described in Annex 1.B.

- 1.5 (d) In particular, data breaches have to be notified by the data importer to the data exporter, the authority and the data subjects if they are likely to result in "significant adverse effects". As this introduces a new notion, it would be useful to clarify in FAQs or in the Decision that this a test, equivalent to the high risk of harm test under Art. 34 GDPR. It should be specified, whether the significant adverse effects impact the data subjects, the data exporter or both. What is the justification for requiring a notification to the authority by the data importer (and the authority of which country?) instead of applying the GDPR territorial scope?

- 1.7 Onward transfers shall be permitted according to the applicable provision of Chapter V GDPR, which is not limited to the appropriate safeguards and the adequacy decisions or consent. Indeed, the recipient of the onward transfer may claim other data transfer safeguards such as BCR, Code of Conduct or certification.
- 1.9 The content of Annexes 1, 2 and 3 can be the reference base for this documentation to avoid any difficulty in interpretation on the expected content of the "documentation".

- 1.9 (a) It should be specified that the expected documentation relates to the processing activities "operated under the transfer".

MODULE TWO: Transfer controller to processor

- 1.1 "…within the framework of the contract agreed …"

- 1.1 (a) In some situations there may be multiple data controllers/data exporters, it would be useful to create an optional mechanism, whereby the processor interacts only with one controller/data exporter who represents all other data exporters in order to make the Clauses implementation more manageable.

- 1.2 It should be added that if the data importer engages in data processing activities outside of these purposes or of the documented instructions of the data exporter, the data importer shall be deemed as acting data controller and in breach of its contractual obligations.

- 1.3 The information on the Clauses shall not be provided by the "Parties" but by the data controller. For this purpose, if the request is received by the data processor, it shall notify this immediately to the data controller for it to answer.

- 1.5 In the last sentence "to the extent possible" creates uncertainties; the level of protection should be maintained to the extent legally required and permissible. The wording is too prescriptive regarding the timing and the available options. For instance, it should also be admitted that personal data can be kept also to evidence proper performance of a contract. Furthermore, the controller shall be able to determine the destination of the data before the termination of the agreement (according to a prior notice previously agreed), that may include the deletion and/or the return to the data controller, directly or to another processor appointed by the data controller. The parties may also agree to a regime by default if the controller fails to communicate its decision to the data processor in the agreed term.

- 1.6 (a) The provisions relating to pseudonymization could be inserted in the security section of Module One. They could be useful for instance when two parties are involved in research activities. However, the wording "exclusive control" assumes that pseudonymisation will always be performed by the exporter and therefore excludes the data importer to offer the pseudonymisation service as an enhanced privacy security measure to data exporters.

- 1.8 The data importer shall only disclose personal data to a third party on the basis of documented instructions from the data exporter. If the data exporter has agreed that the data importer can use sub-processors, it must be understood that these are written instructions. In any event, if the processor's disclosure is an onward transfer, it shall be subject to Chapter V, which is not limited to appropriate safeguards and adequacy decisions.

- 1.9. (d) This article should not address the issue of costs of the audit. This is a commercial issue to be addressed by the parties. Or if it does, it should do it in a more balanced way as there are situations, where an audit may be requested by a data exporter as a result of a claim or a concern and if the audit results confirm the issue, then costs should be borne by the data importer. In any event, to avoid conflicts with the services agreements to which these Clauses will be appended that use to regulate audit rights, it would be recommended to identify in the Clauses the aspects that an audit clause should address (e.g., when, prior notice, subject-matter of the audit and costs) and propose an audit wording as a possible example of how to implement an audit right, to be tailored to the actual circumstances of the services.

MODULE THREE: Transfer processor to processor

- General remark: Clarification is welcome that this processor to processor scenario applies to both scenarios (i) EU processor to third country processor data transfers, (ii) third country processor to another third country processor.
- 1.1 (a) and following which refer to the controller(s). When a group of companies contracts with a supplier, several controllers are involved. Maintaining the full list of affiliates is difficult to attain.

It should be provided upon request only. When there are multiple data controllers, it is useful to create an optional mechanism whereby the processor interacts only with one controller who represents all other data controllers in order to make the Clauses implementation more manageable.

- 1.1(b) It is not realistic to require that the documentation held by the data importer be so under the responsibility of the data controller which whom it has no contractual nor commercial relationship. Under GDPR, and also when GDPR applies as a result of Art. 3.2 (territorial scope), the processor must maintain its own documentation under its own responsibility.

Clause 2

Local law affecting compliance with the Clauses

- (b) The Clauses should make clear that under the Clauses, organisations should assess the risk of a specific transfer by itself taking into consideration all the specific circumstances of the transfer which may include consideration of applicable local laws. Among the criteria to be taken into account to conduct this risk-based approach exercise, in Clause 2(b), the Clauses must also refer to (i) the categories of data that are or not, in practice, subject to requests from public authorities of the recipient country and for which purposes and (ii) the rule of law and human rights approach of the third country of destination.

- (c) Clause 2(c) should be based on “reasonable” efforts (aligned with Clause 1) only and not on “best” efforts, which is an impossible standard to achieve. Similarly, the obligations of the parties would be more accurately reflected if they “enabled” or “permitted” compliance with the Clauses, rather than if they ensured compliance with the Clauses, which is by definition unachievable.

- (f) The GDPR does not provide for obligations of notification of data transfers to supervisory authorities. The paragraph which provides that the data exporter must notify the authority if it decides to continue the transfer after having put in place technical and organizational measures, recreates this notification obligation contrary to the spirit and the letter of GDPR. Instead, the Clause could provide that the data exporter or the data importer can consult the supervisory authority on the efficiency of the measures.

  Furthermore, Clause 2(f) only enables the exporter to terminate the contract in case of a problematic transfer. This requires further nuance as total termination of the contract may be disproportionate if it only affects a limited part of the intended processing activities. If the importer is unable to comply with the Clauses only in regard of a limited number of data subjects, or a specific processing activity, then the suspension of those specific transfers should suffice where that is practicable.

Clause 3

Obligations of the data importer in case of government access requests

- 3.1(a) Guidance on when it is deemed possible or not to inform data subjects ("where possible") of a public authority access request, would be useful. For this purpose, the following should be taken into account:
  - Only the controller shall provide this information to the data subjects. Regarding processors, to notify the controller (rather than the data subject) would be the appropriate action.
  - The duty to inform shall not refer to all the requests but only to those requests which are problematic vis-à-vis compliance with the Clauses.
  - A delayed notification should be considered acceptable where justified, due to exceptional circumstances that impose a non-disclosure period linked to public security or safety reasons arising, for example, from counterterrorism and child safety. A delayed notification still enables data subjects to exercise their rights.

- 3.1(b) and (c) As it happens with Clause 2(c), the "best effort obligation" or the obligation to communicate "the greatest possible amount of information" are impossible standards to reach for the importer. On the one hand, the "best efforts" obligations shall be replaced by a "reasonable efforts" obligation since with a less adverse legal effect, they are leading to the same results in practice. Indeed, in some circumstances involving imminent harm or endanger a child or public safety, it will be impractical or counter-productive to notify data subjects of requests for their information or obtain a waiver to do the same prior to disclosure of the information sought. On the other hand, the obligation should be to make relevant information available, not the greatest amount of information possible.

- 3.1(d) The obligation for the importer should be to keep the information pursuant to a government access request as long as reasonably necessary to protect the legal claims of the parties and the interests of the affected data subjects (rather than the duration of the contract, which may be short or long). This information should be made available to the data exporter upon request as well. The data exporter must receive a copy of related communications between the data importer and the supervisory authorities.

- 3.2 In accordance with the GDPR risk-based approach, the data importer cannot be expected to systematically exhaust (and invest each time huge amount of resources) all possible avenues to challenge any and all requests but only if the request does not appear to be legitimate and proportionate and there is a conflict with EU law. This also requires an assessment of likelihood and severity of harm on the concerned individuals' fundamental rights and freedoms.

Clause 4

Use of sub-processors

MODULE ONE: Transfer controller to controller

A Clause should be added whereby where the data importer engages a sub-processors for carrying out data processing activities, it shall do so by way of a written contract ensuring the same level of protection to the data as the level of protection required from the data importer.

MODULE TWO: Transfer controller to processor

- (a) It could be specified in case of general authorizations that sub-processors would be automatically approved if they meet a list of detailed criteria pre-approved by the data controller. (e.g., member or not of the same corporate group, holder of a specific ISO or service license, adherence to a specific Code of Conduct, presence in a specific region, etc.)

- (b) It could be indicated in a footnote that the model SCC processor to processor SCC can be used.

MODULE THREE: Transfer processor to processor

- (a) A mechanism should be in place to enable centralization of the requests to the first level processor who will then operate as the main contact for the data controller.

- (e) The data controllers also shall be third party beneficiaries.

Clause 5

Data subject rights

MODULE FOUR: Transfer processor to controller

It should be added “and promptly inform and assist the initial data controller if the request is related to its data processing activities”.

Clause 6

Redress

MODULES ONE, TWO; THREE

- (a) The dispute may relate to the Compliance with the Clauses but more generally “to the data transfer operated under these Clauses”.

- (c) Clause 6(c) should require the existence of tangible, real and evidenced damages ((and not theoretical, merely claimed or unevidenced claims).) to accept that the individuals be represented by an NGO or consumer association.

- (d) Clause 6(d) requires data importers to accept to abide by decisions applicable under EU or Member State law but it should also specify that this should apply notwithstanding any available legal remedy for the data importer in EU courts.

Clause 7

Liability

ALL MODULES

- **Conflict with the main agreement to which the Clauses will be incorporated**. The Clauses are not executed in isolation but incorporated into wider contracts (e.g., services agreements, sale and purchase agreements etc.) through annexes or otherwise. These other contracts always contain indemnity and liability clauses, which are commercial aspects that must be addressed under the applicable contractual law, without prejudice to the GDPR liability of the relevant party. Clauses relating to liability between the parties should be optional or left to the negotiation between the parties.

- If any reference to the liability of the parties is to be kept in the Clauses, the following should be considered:
  - **Real damages.** When damages are mentioned, only tangible, real and evidenced damages for an individual should be enforced and compensated in a court (and not theoretical, merely claimed or unevidenced claims). This will ensure that damages are proportionate and related to the real damage caused.
  - **Interaction between fines and Compensation for damages (Clauses 7 (c) and (d), in each set of Modules respectively).** The compensation amount for damages determined by the court, if any, shall be taken into account in any sanction imposed according to art. 83 GDPR.

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

- (c) This is without prejudice to the liability of the ~~data exporter~~ parties under the GDPR." The other parties may be subject to GDPR because of its territorial scope of application.

- (d) It is suggested to remove "bring an action in court" and replace by "claim third-party beneficiary rights" as other alternatives than courts may be available.

- (e) It should be added: "The data importer may see compensation and indemnification from said sub-processor if the latter has been responsible for the breach."

Clause 9

Supervision

- (a) The clause is difficult to implement when there are multiple data exporters (e.g., a contract concluded on behalf of a group of companies).

  An option is to have as supervisory authority the authority of the Member State where the data importer has appointed a representative, where the DPO is located or where the majority of the data subjects are located.

- (b) The Clauses shall be clear that sole competency about the Clauses does not rest with the DPAs, as courts are those competent to deal with contractual issues (e.g., the validity and enforcement of a third-party beneficiary right).

  If a DPA is involved in a dispute under its competence, the Clauses shall ensure that Commission is timely informed to ensure that a balanced and harmonized interpretation is adopted.

SECTION III FINAL PROVISIONS

Clause 1

Non-compliance with the Clauses and termination

- (e) Parties may be given the possibility to revoke the Clauses by mutual agreement not only in case of an adequacy decision but also if alternative safeguards are available to them such as BCR Codes of Conduct and certification.

Clause 2

Governing law

- It would be useful to have a list of countries which do not recognize third party beneficiary rights. In any event, when the data exporter's law does not recognize third party beneficiary rights, it is unclear which governing law should apply for and, in any event, the solution proposed will create a conflict of law. Even if the law at hand does not recognize this figure, could the parties contractually agree to be bound by a contractual commitment having a similar effect?

  Further, there is a lack of clarity of the choice of governing law when the data exporter is not eligible for the one-stop-shop: Which governing law and jurisdiction applies? Or is a choice possible as long as referred to an EU Member State law and jurisdiction?