

757/14/EN
WP 214

Working document 01/2014 on Draft Ad hoc contractual clauses “EU data processor to non-EU sub-processor”

Adopted on 21 March 2014

Decision 2010/87/EU on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council sets out the safeguards and conditions to frame the processing activities of a processor in a third country but also the sub-processing activities. It ensures that the data controller maintains sufficient control over those activities thus ensuring that the personal data being transferred continues to be protected notwithstanding the subsequent transfer to a sub-processor.

This Decision applies to transfers of personal data from data controllers established in the EU to data processors established in third countries. It does not apply to the situation by which a processor established in the EU performs the processing of personal data on behalf of a controller established in the EU and subcontracts his processing operation to a sub-processor established in a third country. Recital 23 of Decision 2010/87/EU provides that “in such situations, Member States are free whether to take account of the fact that the principles and safeguards of the standard contractual clauses set out in this Decision have been used to subcontract to a sub-processor established in a third country with the intention of providing adequate protection for the rights of data subjects whose personal data are being transferred for sub-processing operations”.

The Article 29 Working Party considers it appropriate to work on a new set of contractual clauses dedicated to the international transfers of personal data from an EU data processor to a

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

non-EU data sub-processor. This working document contains a draft of such a set of contractual clauses.

The contractual clauses contained in this working document have not been adopted by the European Commission and therefore do not constitute a new official set of model clauses, nor a finalised set of ad hoc clauses that may be used by companies in order to offer sufficient guarantees in accordance with Article 26.2 of Directive 95/46/EC. This working document captures the state of play of the current reflections of the Article 29 Working Party on this matter. The reflections are still ongoing and may result in further updates to this document in due course.

This aim of this working document is to provide advice to the Commission should the Commission in the future consider the possibility of amendments or supplementations to the existing model clauses adopted by the Commission pursuant to Article 26 of Directive 95/46/EC. It also aims to contribute to the uniform application of national measures authorising transfers of personal data.

Comments: CEDPO welcomes the initiative undertaken by the WP29 and is thankful for the opportunity given to its members to provide comments on this set of clauses. The comments below gather the views of DPOs, professionals in charge of the protection of personal data and law firms working for both data controllers and data processors, considering the experience gathered in the past years with the existing data transfer solutions (Commission's model clauses, BCR, Safe Harbour) from the following member states: Austria, France, Germany, Ireland, The Netherlands, Poland, and Spain. The comments provided below reflect our main suggestions at this stage of the reflexion on a general standpoint and some thoughts on the wording of the main sections of the clauses. Our working groups would need additional time to provide further comments, in particular on wording, as to address our general comments we would revisit the structure of the clauses and we would comment on ancillary clauses as well. Standard Model Clauses have helped many organisations in transferring data to third countries, allowing European organisations access to processing resources world-wide. However, CEDPO believes that a significant amount of work still needs to be put into this document, before it can be put into practice.

- Although draft clauses are called “ad hoc clauses,” we understand that this document may become the basis for future model clauses for data processors. It is therefore essential that these ad hoc clauses be drafted in such a way that they correspond to the reality of data processing operations, and to the working of contractual schemes. The clauses should encourage businesses and organisations to adopt European style effective data protection when data is processed in third countries.

- In Spain where these clauses are being used, it has removed the obligation to obtain the data transfer authorisations from the data controllers in cases where data transfers are actually decided by the data processors. We would welcome a clarification whether the conclusion of these ad hoc data transfer clauses by an EU data processor would also shift the burden of corresponding formalities in other EU countries.

- It is certain that a set of clauses for the transfer of personal data between an EU based processor and a non EU based processor would fill in an gap as in practice an important amount of data transfers outside of the European Union are carried out by service providers in

the framework of services provided for their European customers, while the current data transfer solutions adopted by the EU Commission are not offering a satisfactory answer.

The Commission has indeed considered that the Controller to Processor model clauses of 2010 do not apply to cases where data is transferred to a processor established in the EU who then transfers it to a subprocessor established in a third country¹. Currently in order to ensure the protection of the transferred data in the third country in such a case, most companies implement the structure suggested by the WP29 in FAQ 3.b²; while a Framework Contract is signed between the client-data controller and the EU data processor, the data controller gives the EU processor an authorisation to sign the 2010 clauses on its behalf with the subprocessor established outside of the EU. This scheme entails the granting of a power of attorney and creates an artificial contractual link between the data controller and the subprocessor, link which would otherwise never have occurred. Indeed in most instances in a client-provider relationship, the client prefers to deal with one single contact : his contractual partner, for simplicity reasons but also to deal with one person responsible for the whole delivery of the service. The service provider does not like either to create a direct contractual relationship between the customer and his subprocessors, to avoid confusion in the performance of the agreement, to protect his know-how and commercial offering, to allow flexibility in the relationship with subcontractors (e.g. be able to terminate to adjust technology, or change their scope of services) and for tax reasons. In addition from a contract law point of view, a direct contractual link is not necessary because the service provider is liable towards the client/data controller for any subcontractors' action. Therefore, this artificial link only creates a distortion, in particular, in terms of liability. The focus of the data controller in relation with subcontracting should be to impose conditions upon the performance of the subprocessing rather than willing to have that subprocessors act on his behalf. As with the existing model clauses, the length of the "ad hoc clauses," is problematic. The length of the clauses, often 3 to 4 times longer than the main agreement, and its complexity, will be stumbling blocks during the negotiation process..

→ In order to be well accepted by businesses and therefore used to protect international data flows, the new set of clauses:

- should not break civil and commercial contractual rules and, therefore, should respect the contractual distance and liability rules between the client – controller and the subcontractors
- should adopt a simple wording and should be limited in length to what is necessary to protect individuals
- should more consistently take into account that the EU service provider will use these clauses in most instances (e.g. cloud computing scenario) not to address a specific data processing project requested by a single customer, but to ensure the compliance of its service offering, which is made to numerous customers/data controllers who are likely to be based in several EU Member States.

- The ad hoc clauses, in their current draft, are very complex to read. This is in particular due to the numerous references made (e.g. to the Framework agreement, to the contract between the Processor and Sub-Processor, to the Data importer and its Sub-Sub-Processor(s) etc.) It does not appear as a step towards a simplification of the contractual

¹ Recital 23 of Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC

² WP 176 - FAQs adopted on 12 July 2010

relationships compared to the existing direct contracts between the EEA-based controller and the non-EEA-based processor (see WP 176 lit. 3). The use of additional definitions to refer to a situation repeated across the clauses, could help simplify the wording for a better rationalization. Also, we think that the structure should be reconsidered in order to ease the reading and understanding of the clauses. Since the purpose of the clauses is to ensure an adequate protection of the personal data once it is outside the EU, the substantial clauses should begin with the obligations of those who will process the data outside of the EU, instead of beginning with the obligations of the data exporter. Most of these obligations actually refer to the obligations of the data importers, leading to repetitions and complex intellectual construction, which are a real deterrent to the reader. Moreover, the same obligations are repeated twice or three times at the level of the data exporter, data importer and then sub-processor. For the sake of clarity, we suggest to state the essential data protection obligations which must be complied with all along the chain of sub processing in one of the first provisions of the clauses and then address in distinct clauses those obligations which are specific to each player. It implies getting away from the usual structure of the Standard contractual clauses.

- It is important to acknowledge that international data transfers take place in the context of very different types of situations.

In the simplest situations the EU subprocessor subcontracts to a third supplier exactly part of the service which was entrusted to him by the client-controller. For example a company engages a supplier in the EU for a direct marketing campaign including phone calls to consumers. The EU supplier will process the customer and prospect database of the controller remotely (the database remains hosted on the client's site) in the EU to segment the targets according to specific profiles and will subcontract the calling campaign to a supplier who runs a call center in Morocco. In this example where the project entrusted by the controller to the processor clearly identifies the call campaigns as a processing activity, it is possible for the EU processor to pass on to the Moroccan processor the relevant instructions of the controller regarding to the processing.

However, this simple scenario corresponds only to few situations. In most instances the reality is more complex. Numerous suppliers could be considered as processing personal data because of the broad definition of a data processing under the Directive 95/46/EC, although part of the service performance *stricto sensu* is not subcontracted to them and they are carrying out ancillary tasks, not even contemplated by the controller. An EU based data controller, EuroCo, requests an EU based supplier, Eurosupply, to handle its travel and living processes. For this purpose, expense receipts are sent to IndianScan, the Indian affiliate of the supplier (subprocessor) who scans them and then has the paper receipts stored by a sub-subprocessor in India. The scanned receipts are sent/made available to a supplier in the US (subprocessor) who works with contractors in Mexico, Morocco, Mauritius and India (all sub-sub processors) to translate them into English. They will then be analysed by another Indian supplier, IndiaReview (subprocessor) to verify whether the expense receipt matches with the travel/expense authorisation request. This subprocessor is requested to make incident reports for each individual case and also monthly reports. Its IT systems on which the personal data is processed are hosted in a data center operated by a third party supplier, as sub-subprocessor ; the remote maintenance of the network is done by another non EU vendor who may access personal data exceptionally and under supervision and strict security clauses, also a sub-sub-processor ; Printed versions of the draft reports made by the staff have to be shred, the emptying of shredders is operated by another vendor, also a sub-sub-processor and defective

PC hard drives are also maintained, destroyed and replaced by another vendor, sub-sub-processor. Needless to say, IndianScan and IndiaReview are providing the same type of services for numerous companies from the EU and from all around the world, it is standardized service and their own suppliers the sub-sub-processors³ (translators, hosting company, maintenance suppliers, shredding company ...) do not apply different working processes depending on the origin of the data (i.e. whether the data comes from a specific data controller or another), as their work methodology is standardized, even if it may involve some data processing activities. Some of the sub-subprocessors are likely to change during the term of the Framework Contract between EuroCo and EuroSupply.

In the cloud industry the reality is even more complex, as the cloud provider generally offers a standard service based on mutualisation of resources. In building its technical and commercial offer, the cloud provider selects the best suited sub-processors based on a number of predefined criteria's. These sub-processors can be located either inside or outside of the EU and will be bound by the contractual terms of the cloud service provider. These sub-processors can have very diverse roles from directly processing data to merely providing maintenance or back-up services. Based on the offer of the cloud provider and its level of transparency, the potential cloud user/client will have the responsibility to evaluate the service offered by the cloud provider in order to determine if it is fit for its purposes and to ultimately choose to use or not to use the cloud service. The client will generally not be able to ask that the service be modified and that some sub-processors be changed or their location modified. The cloud provider – client relationship is in fact based on a “take it or leave it” approach. Additionally, once the client has made its choice, it will not be able to impose any additional constraints or give specific instructions to the cloud service provider. Therefore, in the cloud computing world, the service provider cannot request for approval of the client to change sub-processors or modify the location of data, as such would totally undermine the cloud business model. The absence of control of the client on the execution of the service and the impossibility to give instructions to the cloud provider is inherent to cloud computing services. The new set of clauses should take into account this specific business model and provide for some exceptions where the client is not materially in a position to give any instruction to the cloud provider. That should not necessarily mean that personal data is not protected; In the opposite, using a cloud service provider generally improves security and as such protection of personal data as data is entrusted to a provider whose core business is to provide security services and can work with the most appropriate providers and locations to offer such high security level; the cloud provider can choose to modify the location of data or change the sub-processors especially because it considers that such would enhance the security of data; In doing so, it should not have to require a prior specific authorisation from its clients for each subcontractor as we should expect that a cloud provider is more versed in security solutions than its clients who are generally not IT specialists.

➔ In order to be well accepted by businesses and therefore used to protect international data flows, the new set of clauses:

- should respect the principle of contractual freedom and should not attempt to codify most of the contractual relationship. It should therefore offer in some instances alternative language or options that contracting parties may choose between, depending on the type of data transferred and the type of services rendered and the level of control that the data controller

³ **The US translation service provider also resorts to an external hosting company and to IT maintenance providers and a media disposal provider. So do any of the other translation agencies around the world and IndiaScan.**

elects to exercise

- should take into consideration the fact that a “one size fits all” approach requires to avoid provisions which are possibly well adapted to a fluid chain of subcontracting (e.g. 1st example), but which are inadequate and therefore will not be accepted in other instances, such as where the service rendered by the sub-subprocessor does not vary depending on the identity of the data controller. It is of the essence that, the subprocessors processing personal data, do commit to protect it and secure it as defined in the contractual provisions. However, we have to acknowledge the difficulty faced by data processors who have to comply with the instructions of hundreds of data controllers who are often unknown to them. The instructions of the data controller must be reflected in a document which must be passed from the EU processor to each other relevant processor in contracting documents.

- We believe that it would be very useful to businesses to receive guidance in the preamble of the WP29 decision on the use of this new set of clauses. The guidance could address several issues, such as examples of practical situations where the clauses could be used. For instance a question arises as to whether an EU based commercial entity of a service provider, merely in charge of sales operations, not taking part to any data processing operations entrusted by the data controller should be considered as a data processor who could conclude these ad hoc clauses, although the data processing operations as defined by the Directive⁴ would be carried out by the subprocessors located outside of the EU. A clarification of the notion of data transfer would be useful in this context.

In addition, a clarification of the notion of processor and subprocessor, in order to clearly delimit in which instances of service supply, EU data protection authorities expect the ad hoc clauses to be used, would be of crucial guidance to businesses and DPOs (e.g. under the second example above. Indeed the question arises whether the mere contact with personal data constitutes a subprocessing requiring compliance with the clauses or whether the clauses should be used only when part of the initially entrusted service is subcontracted).

Moreover, the document could clarify whether the clauses can be used in a situation where a data controller is based outside of the EU but resorting to the services of an EU based supplier who in turns exports the data outside the EU.

Guidance could also be provided as to when these ad hoc clauses can be used in light of the Commission’s 2010 Standard Contractual Clauses for the transfer of personal data to processors established in third countries. Although we have indicated above that some businesses find uncomfortable the use of the solution recommended by the WP29 in its FAQs, other businesses have been implementing this solution for the past 4 years and are now familiar with it and would find it difficult to have to modify their contractual processes to adjust to another tool. It is the reason why we think that the two systems should be maintained in parallel and that the choice should be left to data controllers and processors to choose between the use of the 2010 clauses concluded by the data controller, or ad hoc clauses. We recommend that the Working Party clarifies this situation.

⁴ Article 2.b) of Directive 95/46/EC : « *processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;* »

For a better understanding of the economy of the clauses, it would be helpful to add visualisations of the different contractual relationships between Controller, Processor and subsequent Sub-Processors. Furthermore a simple and also explanatory graphical illustration of the different responsibilities and liabilities between Controller, Processor and Sub-Processor etc. and towards the data subjects would also be helpful in order to address the complexity of the contractual scheme.

- We believe that in many instances the approach of an imposed contractual framework misses flexibility and is disconnected from the reality. We believe that alternatives, closer to data processing projects should be considered and we would like to suggest the idea of a “Data Protection Circle” as food for thought. From a Data Subject standpoint. "Model Clauses" sounds very legal language and does not convey a message of protection.

A Data Protection Circle would be created for one application/platform (or a category of applications, any consistent set of applications basically managed by the same stakeholders for the same purposes).

The initiator of a Circle would be the Data Controller. A Data Controller could maintain one or several Circles over time.

Contrary to BCR, the Data Protection Circle would be open in the same way to applications managed internally by companies of the same Group, and to applications involving external processors.

A unique entry point to the Circle would be defined, bringing more clarity and visibility for the data subjects.

All stakeholders involved in the processing of personal data will become members of the Data Protection Circle which will define its scope (processed data, data processing purposes and restrictions) and the relevant obligations binding all members (more in Annex).

DRAFT AD HOC CONTRACTUAL CLAUSES

“EU DATA PROCESSOR TO SUB-PROCESSOR(S) IN THIRD COUNTRY ~~NON-EU~~”

On ~~data~~ transfer **of personal data** from processors to sub-processors established in third countries according to article 26(2) of Directive 95/46/EC of the European Parliament and of the Council.

Name of the data exporting organisation (Processor):

.....

Address:

.....

Tel.:; fax:; e-mail:

Other information needed to identify the organisation:

.....

(Hereinafter, the **data exporter**)

And

Name of the data importing organisation (Sub-processor):

.....

Address:

.....

Tel.:; fax:; e-mail:

Other information needed to identify the organisation:

.....

(Hereinafter, the **data importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following ad hoc contractual clauses (hereinafter “the Ad hoc clauses”), in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer of personal data by the data exporter to the data importer of the personal data specified in Appendix 1. Provided that the data controller and the data exporter have agreed in a contract, as provided for in article 17 of Directive 95/46/EC and in accordance with the provisions of the applicable data protection law (hereinafter the “Framework Contract”), that data processing, as specified in this Framework Contract and in Appendix 1 of these Ad hoc clauses, may be provided by the data importer.

Clause 1

Definitions

Comment: For clarity purposes, we suggest to use capitalised words for all defined terms (e.g. used for Framework Contract, for Ad hoc Clauses) in order to distinguish them from others in the Clauses. It would avoid risks of misinterpretation (e.g. “applicable law”). A definition of “third country” could also be included to refer to non EEA countries which did not receive an adequacy finding. The term “Framework contract” may be seen as misleading as it is often used in contractual relationship to refer to an umbrella agreement defining the key terms applicable to possible future contracts. Also, the text would need before finalisation to be reviewed to ensure that defined words are used consistently.

For the purposes of the Ad hoc clauses:

- a) “personal data”, “special categories of data”, “process/processing”, “controller”, “processor” and “data subject” shall have the same meaning as in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. **“controller” under these Ad hoc clauses encompasses both singular and plural forms, in the event the data exporter transfers data provided by multiple data controllers under these Ad hoc clauses;**
- b) “data exporter” means the processor ~~that~~ **who** processes personal data on behalf of and under the instruction of the controller and **who** transfers personal data to a third country outside the European Economic Area;
- c) “data importer” means the sub-processor engaged by the data exporter who agrees to ~~receive personal data intended for processing on behalf of the controller and in accordance with its instructions, the provisions of the Framework Contract and the terms of the Ad hoc clauses~~ **process all or part of personal data** and who is not subject to a third country’s system ensuring an adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

Comment: it is preferable that definitions do not include obligations, otherwise there is a risk of misinterpretation in case of wording differences with the main clauses which set the contractual obligations.

- d) “subsequent sub-processor” means any ~~subsequent~~ **subsequent to the data importer**, engaged by the data importer or by any other subsequent sub-processor ~~who agrees to process, personal data on behalf of the controller in accordance with its instructions, with the provisions of the Framework Contract, the terms of the Ad hoc clauses and the terms of the written sub-processing agreement in accordance with the Ad hoc clauses~~ **processes all or part of personal data and who is not subject to a third country’s system ensuring an adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;**
- e) “Framework Contract” means the agreement concluded between the controller and the data exporter in accordance with applicable national data protection law transposing Article 17 of Directive 95/46/EC;
- f) “applicable data protection law” means the legislation protecting the fundamental rights and freedoms of individuals and in particular, their right to privacy with respect to the processing of personal data, applicable to the controller. However, as regards to the **data protection** security measures, the law where the data exporter is established will also be applicable. If detailed rules ~~regarding~~ relating to security measures in the law applicable to the controller and the law applicable to the data exporter as provided by Article 17(3) of Directive 95/46/EC are in conflict, the law of the data **exporter** prevails;

Comment: Data exporters operating in several EU countries today have to operate under different standards which is not practical and which is putting them under a competitive disadvantage.

g) “technical and organisational security measures” or “security measures” means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data ~~by over a~~ networks, **and against all other unlawful or any other illicit** forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

Comment: the text has been aligned with the official translation of the 95/46/EC Directive.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data, where applicable, are specified in Appendix 1 which forms an integral part of the Ad hoc clauses.

Clause 3

Third-party beneficiary clause

Comment: We believe that this Clause and Clause 6 should be simplified. It could be done by restating at first the following principle : each party/processor can be held liable to the data subjects for the damages suffered as a result of a breach of the Ad hoc Clauses which are caused by said party/processor or any subprocessor it has engaged. The Clause should also take into consideration the commercial link between the parties : it is only in case of inaction or inability to act of the direct contracting party of a processor, that the controller should be entitled to enforce the Clauses against such processor. Besides, consistency with clause 4b) (15) must be ensured.

1. The data subject can enforce against the data exporter this Clause, Clause 4(a) to (e), and (g) to (q), Clause 5 (a) to (c), and (e) to (k), Clauses 6 and 7, Clause 8(2), and Clauses 9 to 13 as third-party beneficiary, where the controller has factually disappeared or has ceased to exist in law, unless any successor entity has assumed the entire legal obligations of the controller by contract or by operation of law, as a result of which it takes on the rights and obligations of the controller, in which case the data subject can enforce them against such entity.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (c), and (e) to (k), Clauses 6 and 7, Clause 8(2), and Clauses 9 to 13 as third-party beneficiary, in cases where both the controller and the data exporter have factually disappeared or have

ceased to exist in law unless any successor entity has assumed the entire legal obligations of the controller and the exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the controller and the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subsequent sub-processor this Clause, Clause 5(a) to (c) and (e) to (k), Clauses 6 and 7, Clause 8(2) and Clauses 9 to 13 as third-party beneficiary, in cases where both the controller, the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data importer by contract or by operation of law as a result of which it takes on the rights and obligations of the data importer, in which case the data subject can enforce them against such entity. Such third-party liability of the subsequent sub-processor shall be limited to its own processing operations under the Ad hoc clauses.

~~4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by applicable law.~~

Comment: This wording will give rise to interpretation. The clauses cannot give a right by contract to collective redress; this is the role of national laws. Also, the wording implies that the parties may have a right to object to such proceedings if they exist under law. If national law has stated the possibility for an association to act on behalf of data subjects in a collective manner for data protection purposes (rather than consumer purposes), no objection may alter or impair such an action. The clause appears as redundant to recourses provided under applicable law.

5. The controller can enforce against the data exporter ~~or the entity at the origin of the breach (i.e. the data importer or any subsequent sub-processor)~~ this Clause, Clauses 4 ~~and 5~~, Clause 6(4), and Clauses 7 to 13 as third-party beneficiary. **The controller can enforce against the entity at the origin of the breach (i.e. the data importer or any subsequent sub-processor) this Clause, Clause 5, and Clauses 7 to 13 as third-party beneficiary when required by applicable law, in case of inaction of the data exporter or concerned sub-processor or if the latter has factually disappeared or ceased to exist in law.**

Comment: This clause must reflect the economic reality of contractual schemes where the data controller is rarely in contact with subprocessors and does not want such a contact. In day to day activities it will be the direct contracting party of the processor who will take action. The clause should acknowledge this and should take into consideration the efforts taken by the direct contracting party of the processor who is at breach to get the breach cured.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) That it has signed a ~~contract~~ (“Framework Contract²²) with the controller in accordance with the applicable data protection law;

(b) That the Framework Contract provides ~~for~~ **that**:

(1) The controller has processed and will continue to process the personal data in accordance with the relevant provisions of the applicable data protection law and that the processing does not violate this law;

(2) The controller instructs⁵ the data exporter and that it will instruct it throughout the duration of the personal data processing services to process the personal data exclusively on the controller’s behalf and in accordance with the applicable data protection law and the Framework Contract;

Comment: We do not understand the justification for the constraint bearing upon the EU supplier –data exporter to make contractual commitments towards its sub contractors on these matters. In the relation between data importer and data exporter, what matters is that the data exporter be made aware that (i) the data controller has to comply with data protection laws and that (ii) the data exporter can only act upon instructions of the data controller.

The clauses shall not replace national data protection laws. These laws provide for obligations bearing upon data controllers and determine what is the required content of the contract between the controller and the EU processor.

Most of the obligations provided under this section 4 are already stated under national data protection laws. It makes the clauses unnecessarily lengthy to repeat such obligations. Moreover, we believe that the content of the Framework Contract should be left to the negotiation between the data controller and the data processor, acknowledging that they are bound to comply with data protection rules and that the contract must meet the requirements set up by applicable data protection law. The data sensitivity and the type of processing carried out will drive the level of precision of the data protection contractual clauses which will be included in the Framework Contract. It should not be determined in advance. The variety of contracts which we see in our practices show the need for various scales in the data protection provisions.

~~(3) The controller ensures that the Framework Contract including the technical and organisational security measures described in it are in accordance with the applicable data protection law and that the data exporter and any importer or subsequent sub processors~~

⁵ The instructions of the data controller under these ad hoc Clauses must be understood as follows: any instructions provided to the data importer/sub-processor about the processing of personal data, which

- (i) must be only issued if necessary to comply with data protection legal requirements;
- (ii) cannot alter the scope of the services agreed between the data controller and data exporter in the Framework Contract (as reflected in the description of the processing operations in the Annex); and
- (iii) must be provided to the data importer/sub-processor (a) through the data exporter/the data processor; or (b) if the Framework Contract so allows, directly by the data controller ; then the data controller must keep the data exporter informed thereof in all cases.

~~provides sufficient guarantees in respect of the technical and organisational security measures described in the Framework Contract;~~

~~(4) The controller will ensure compliance with the security measures;~~

(5) The controller has given its ~~prior written~~ authorisation to the data exporter to allow that data processing services (specified in Appendix 1) entrusted to the data exporter could be subcontracted to the data importer in conformity with the **Ad hoc clauses Framework Contract** and the applicable data protection law;

~~(6) The controller remains free to agree if the data importer may engage subsequent sub-processors and if these latter may subsequently engage other subsequent sub-processors. Any sub-processing could be allowed only with the prior information to the controller and its prior written authorisation;~~

~~(7) Any sub-processing by the data exporter, the data importer or any subsequent sub-processor shall be subject to a sub-processing agreement binding upon them which imposes the same obligations including the technical and organisational security measures (specified in the Framework Contract) as imposed on the data exporter under the Framework Contract. Where the data exporter, data importer or any subsequent sub-processor fail to fulfil their obligations, the data exporter shall promptly inform the controller of such fact, as soon as it is aware about it; in which case the controller is entitled to suspend the transfer of data and/or terminate the Framework Contract which automatically will have the same consequence on the ad hoc clause and any sub-processing contract. Where the data importer or any subsequent sub-processor fails to fulfil its data protection obligations under the Ad hoc clauses or any sub-processing agreement, the data exporter shall remain fully liable to the controller for the performance of the data importer's and subsequent sub-processor's obligations under this Ad hoc clauses and such agreement;~~

~~(8) If the transfer by the data exporter to the data importer includes special categories of data, the controller will inform the data subjects that their data could be transferred to a third country which does not provide an adequate level of protection according to Directive 95/46/EC;~~

Comments : The obligation provided in this section (8) cannot be implemented as it would impose a duty to inform of the lack of adequacy of a contemplated transfer in spite of all the measures implemented by the parties in compliance with data protection law and the authorities's guidance.

~~(9) The controller agrees to deposit a copy of any contractual solution provided to offer sufficient safeguards in respect of the protection of privacy within the meaning of Article 26(2) of Directive 95/46/EC, such as these Ad hoc clauses, with the data protection supervisory authority competent according to the applicable data protection law if it is so required under the applicable data protection law;~~

~~(10) The controller completes the necessary formalities with the Data protection~~

~~supervisory authority competent according to the applicable data protection law in order to obtain the authorisation to carry out international data transfers if it is so required under the applicable data protection law; or the controller authorises the data exporter, when permitted according to the applicable data protection law, to complete the necessary formalities for it and on its behalf before the data protection supervisory authority competent according to the applicable data protection law;~~

~~(11) The controller will forward any notification received from the data exporter according to Clause 4(l) and 4(m) first bullet point, or similar notification from the data importer or any subsequent sub-processor to the data protection supervisory authority where the controller is established if the controller decides to continue the transfer or to lift the suspension;~~

~~(12) The controller will make available to the data subjects and the Data protection supervisory authority competent according to the applicable data protection law upon request a copy of the Framework Contract as well as a copy of any contract for sub-processing services, such as these Ad hoc clauses, with the exception of Appendix 2, and a summary description of the security measures, unless the Framework Contract, the Ad hoc clauses or the contract for sub-processing services contain commercial secret information, in which case it may remove such commercial secret information;~~

~~(13) The controller shall keep an updated list of any sub-processing agreements concluded, and notified by the data exporter pursuant to Clause 4(o) of the Ad hoc clauses, which shall be updated at least once a year. This list shall be available to the data protection supervisory authority competent according to the applicable data protection law;~~

Comment: Updating a list of any sub-processing agreements concluded once a year would constitute an administrative burden with no added value on the privacy of the data subject. Also, this should not be an obligation bearing upon the data controller who does not have direct contractual link with the subprocessors. Additionally this can be seen as a disadvantage compared to non-EU-processors which are not facing this kind of burden in the Standard Contractual Clauses.

~~(14) The controller shall decide if on the termination of the provision of data-processing services, the data exporter, data importer and any subsequent sub-processor shall return or destroy all the personal data transferred and the copies thereof directly to the controller. The data exporter shall certify to the controller the respect of clause 13;~~

Comment: This decision is relevant for the subprocessors' obligations but would be contemplated in the Annex to the ad hoc Clauses.

~~(15) The data subject, who has suffered damage as a result of any breach, by the controller, of its obligations pursuant to the Framework Contract, the applicable data protection law and according to Clauses 4 (b) (1) to (16), or any breach by the data exporter, the data importer and/or the subsequent sub-processors of their obligations according to the~~

~~Ad hoc clauses, and any further sub-processing agreements, is entitled to receive compensation from the controller for the damage suffered;~~

~~(16) The controller shall ensure compliance with Clauses 4(b) (1) to 4 (b) (16);~~ (c) That it processes the data only on behalf of the controller's instructions laid down in the Framework Contract to carry out the service, in accordance with the applicable data protection law and these Ad hoc clauses;

(d) That it has implemented and complies with the technical and organizational security measures specified in the Framework Contract and in accordance with the applicable data protection law;

(e) That it will deal promptly with all inquiries from the controller relating to the processing of the personal data and to abide by the **final decision⁶ advice** of the competent data protection supervisory authority~~ies~~ according to the applicable data protection law;

Comment: the wording has been aligned on the wording of Clause V c) of the Standard Contractual Clauses of 27 December 2004⁷.

(f) That it will agree, at the **reasonable written** request of the controller, to submit its data-processing facilities for audit of the processing activities covered by the Framework Contract which shall be carried out by the controller or an inspection body composed of independent **and impartial** members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the controller, where applicable, in agreement with the competent data protection supervisory authorities according to the applicable data protection law;

Comments :

- The request of an audit by the data controller should be "reasonable", i.e. justified. Indeed, an audit creates disruption in the organization of the data processor. The controller should not abuse of the right to request an audit and should therefore justify his request, for instance because he is conducting an audit himself of his own data processing operations or because he has a legitimate suspicion of a breach.

-The clause has been also aligned on the wording of the Clause II g) of the Standard Contractual Clauses of 27 December 2004.

(g) That it **is authorised to** ~~has obtained the prior written authorisation⁸ from the controller according to the Framework Contract for sub-processing sub-process~~ its activities to the data

⁶ final decision against which no further appeal is possible

⁷ Clause V.c) "Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible. »

⁸ See ~~note 1 above~~ footnote under Clause 5 d) on the notion of "reasonable request".

importer **under the Framework Contract, which provides :**

- for a specific authorisation by the data controller in favour of the data importer and each subprocessor,
- for an obligation to inform the data controller prior to the appointment of any subprocessor ; failure by the data controller to object to the appointment in a timely fashion allows to proceed with the appointment of the subprocessor,
- for a general authorisation to subcontract to entities which belong to the same group as the data exporter within a pre-determined geographical scope, provided that their list is made available to the data controller upon grounded request,
- for a general authorisation to subcontract within a pre-determined geographical scope, provided that the list of subprocessors is made available to the data controller upon grounded request,
- for a general authorisation to subcontract to the subprocessors identified on a list, such list to be provided to the data controller at the time of execution of the Framework Contract and thereafter maintained up to date by the data exporter, who shall provide it to the data controller upon request.

Comment: The wording of footnote 1 included in WP 214 is unclear⁹. As we deleted the corresponding provision in article 4, we restated the footnote below. What can be derived from it is that the controller can¹⁰ :

- give a general authorisation to subcontract. A general authorisation corresponds for instance to : “You, data suprocessor may subcontract to reliable companies who undertake to protect the data the same way” . As we understand the footnote, the data controller is not informed of who the initial subprocessors are (otherwise it is not a general authorisation, it is a specific authorisation given for several subcontractors). However, the footnote provides that the data controller must be informed of intended changes in subprocessors. The mechnism does not seem logical to us. A data controller who doesn’t know and who is not interested in knowing who the subprocessors are in the first place is unlikely to want to exercise control over new subprocessors.

- give a specific authorisation for each subprocessor.

We recommend to introduce flexibility in each of the Clauses referring to the selection mechanism of subprocessors in order to reflect the various business realities as expressed

⁹ “Depending on the provisions of the Framework Contract, the controller may have decided that its general prior written authorisation is sufficient, or that its specific authorisation will be required for each new sub-processing. If a general authorisation is given, the controller should be informed on any intended changes concerning the addition or replacement of importers/sub-processors in such a timely fashion that the controller has the possibility to object to the change or to terminate the contract before the data are communicated to the data importer/sub-processors.”

¹⁰ One of the option must be ticked by the data exporter to reflect the Framework Contract.

previously, otherwise we fear that this is likely to have an impact upon the use by companies of these Ad hoc clauses. We suggest instead to provide the parties with options (boxes to tick).

Besides, CEDPO members make good use of the WP29 comparative documents of national legislations. They would welcome guidance **on the extent to which**, in each European Member State, it is required to notify/get prior authorisation by national data protection authorities of data transfers to subprocessors and subsequent subprocessors. In other words, should the data controller perform the formalities only with respect to the first data transfer outside of the EU, or also with respect to subsequent data transfers, in which case setting up a definition of data transfer would be critical. In the example provided above of transfers to subprocessors of IndiaReview and IndiaScan, the formalities would have to be accomplished with respect to numerous data transfers.

(h) That, in the event of sub - processing by the data importer or by a subsequent sub - processor, the processing activity is carried out in accordance with Clause 11 by a subsequent sub - processor providing at least **an equivalent** ~~the same~~ level of protection for the personal data and the rights of data subjects as the data importer under the ad hoc Clauses. The data exporter will inform the data importer on the decision taken by the controller according to the Framework Contract and will transfer any necessary information to the data importer ;

Comment: Same level of protection as the minimum requirement is difficult to impose. For instance, the subsequent sub-processor might not have the necessary license to use the same encryption technology as the importer. He can however use a different encryption technology which is similar to protect the data. The wording creates uncertainty whether the sub-processor is compliant with the ad hoc clauses.

~~(i) That the data importer and any subsequent sub-processor of the importer provide sufficient guarantees in respect of the technical and organizational security measures and that a sub-processing agreement binding upon the data importer and any subsequent sub-processor will impose the same obligations including the technical and organisational security measures (specified in Appendix 2 to the Ad hoc clauses) and the duty to process data in accordance with the controller's instructions as are imposed on the data exporter under the Framework Contract and will guarantee the respect of those duties;~~

Comment: This paragraph is deleted because that instruction will be complied with as a result of section h.

(j) That it will promptly **respond to reasonable written requests made by** ~~inform~~ the controller ~~upon request~~ about the effective implementation of the security measures by the data importer and by any subsequent sub-processor¹¹; ~~in accordance with the instructions of~~

¹¹ **A request by the data controller or data exporter would be deemed reasonable if it is done in good faith in the course of performance of the agreement and for reasonable justification. Examples of good faith requests are for instance without being exclusive in case of reasonable suspicion of a breach of its security obligations, in case of a request by a competent data protection supervisory authority, if the data**

~~the controller;~~

Comment: Safeguards must be put in place to ensure this obligation is not used as a tool by the data controller to terminate the Framework Contract. Showing “effective implementation” all along the subprocessing chain upon any request of the data controller for any type of security measure can provide to be very difficult, burdensome, time consuming and costly.

~~(k) That it has communicated the instructions and throughout the duration of the personal data processing services subject to the Ad hoc clauses, will communicate the instructions of the controller to the data importer to process the personal data transferred exclusively on controller's behalf and in accordance with its instruction and with the terms of the Framework Contract, the applicable data protection law and the Ad hoc clauses;~~

Comment : This paragraph is deleted because that instruction will be complied with as a result of section h.

(l) **Option 1** That it has no reason to believe that the legislation applicable to the data importer and any subsequent sub-processor prevents the latter(s) from fulfilling the controller’s instructions and their respective obligations under the Ad hoc clauses and their sub-processing agreements, and if the data exporter becomes aware of such facts, for instance from a notification received from the importer according to Clause 5(h) or in the event of a change of legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Ad hoc clauses, the Framework Contract and the applicable data protection law, the data exporter will promptly inform the controller of such fact, as soon as it is aware about it; in which case the controller is entitled to suspend the transfer of data and/or terminate the Framework Contract;

Option 2¹² That the Framework Contract provides that the data exporter has no reason to believe that the legislation applicable to the data importer and any subsequent sub-processor prevents the latter(s) from fulfilling their respective obligations under the Ad hoc clauses and their sub-processing agreements, and if the data controller becomes aware of such facts, for instance from a notification received from the data importer according to Clause 5(h) or in the event of a change of legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Ad hoc clauses, the Framework Contract and the applicable data protection law, the data controller (i) will promptly inform the data exporter of such fact, as soon as it is aware about it, and (ii) is entitled afterwards to suspend the transfer of data ;

Comment : We understand the rationale for this clause. We suggest to introduce an option because in practice, it happens that it is the data controller who requires the service provider to outsource part of the performance to a specific country either because the data controller has operations there or for cost reasons. In such a case, the data exporter is not in a position to

~~controller is under a legal requirement to demonstrate a certain level of compliance with security measures.~~

¹² ~~The data controller has influenced the country of export~~

negotiate and to assess the applicable local legislation, it must find a supplier in the concerned region. It would be unfair to leave the liability upon the data exporter in such a case. It is the reason why we suggest to introduce an option.

We deleted the reference to the “controller’s instructions” following the reasoning developed previously. Besides, this reference is not necessary, as the “controller’s instructions” are already included in “*their respective obligations under the Ad hoc clauses and their sub-processing agreements*”.

(m) That ~~the data exporter~~ **it** will promptly notify the controller about:

- Any legally binding request for disclosure of the personal data by a law enforcement authority made to the data importer or any subsequent sub-processor, unless the data importer or any subsequent sub-processor are otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
- Any accidental or unauthorised access;
- Any request received directly by the data exporter, the data importer or any subsequent sub-processor from the data subjects without responding to that request, unless it has been otherwise authorised to do so; and
- Any notification of the data importer in accordance with Clause 5 or ~~13~~**1**(1);

~~(n) That the Ad hoc clauses are made binding towards the controller through a specific reference to it in the Framework Contract, for instance as an appendix;~~

(o) That it shall give to the controller an updated list of any sub-processing agreements and notified by the data importer pursuant to Clause 5(f) of the Ad hoc clauses, which shall be updated at least once a year. Such updates shall be promptly communicated to the controller. The data exporter shall send promptly to the controller upon request a copy of these Ad hoc clauses and any sub-processing agreement and in particular Clause 11;

(p) To make available to the data subjects upon request a copy of the Ad hoc clauses, or any **clauses relating to the processing of personal data included in** sub-processing agreements in those cases where the data subject is unable to obtain a copy from the controller with the exception of Appendix 2 which shall be replaced by a summary description of the security measures, unless the Ad hoc clauses or the **relevant clauses of the** sub-processing agreements contains commercial secret information, in which case it may remove such commercial secret information;

Comment: The parties should not be bound to provide the suprocessing agreement in their entirety, in particular commercial clauses such as price, indemnities,...

(q) That it will ensure compliance with Clauses 4(a) to (q). Where the data exporter cannot

provide compliance to its duties according to the Framework contract or the Ad hoc clauses or where the data importer or any subsequent sub-processor fail to fulfil their duties, the data exporter agrees to inform promptly the controller of such inability to comply, in which case the data exporter shall remain fully liable to the controller and this latter is entitled to suspend the transfer of data and/or terminate the Framework Contract **as appropriate having regard to the nature and consequences of the breach and the ability of the defaulting party or the data exporter to cure it**. If it does so, the data exporter shall suspend the transfer of data and/or terminate the Ad hoc clauses in accordance with the controller's instructions.

Comment: we would like to find way to avoid this clause to be instrumented by data controllers for any type of breach, as minor breaches can be fixed and have no consequences for the data subject and should not be claimed as an argument to terminate the Framework Contract thanks to this contractual clause. In commercial service agreements based on common law, contract termination clauses usually include an element of materiality of the breach and give the possibility to cure the breach before terminating the agreement. We have attempted to avoid inconsistencies with commercial service agreements and to make sure that a proper proportionality assessment is made by the data controller before using this termination clause.

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

- (a) To process the personal data ~~only on behalf of the controller and in compliance with its instructions, either given directly by the latter or through the data exporter, and in accordance with the terms of the Framework Contract, the applicable data protection law~~ **and in accordance with the terms of these Ad hoc clauses**;
- (b) That it has implemented and complies with the technical and organisational security measures specified in Appendix 2 of the Ad hoc clauses ~~and in accordance with the applicable data protection law~~;
- (c) To deal promptly and properly with **all** inquiries from the controller or from the data exporter ~~according to the controller's instructions~~, relating to the processing of the personal data ~~subject to the transfer~~ and to abide by the **final decision advice** of the data protection supervisory authority competent according to the applicable data protection law;

Comments: The data importer should respond to requests by the data exporter even if these are not based upon a request made by the data controller. The data exporter has selected a subcontractor and must be able to control contract performance without constraints.

Same comment as under clause 4 e)

We wish to point that such decisions may place the data importers in situations of conflict of laws whereby they may be required to comply with requests from EU authorities which are in conflict with local regulations. The adoption of global data protection standards would limit undesirable situations for businesses.

To avoid repetitions or long sentences we suggest to add at the beginning of the clauses a contractual definition of “personal data” referring to the personal data as specified in Appendix 1.

(d) That it will agree, at the **reasonable written** request of the controller or the data exporter¹³ ~~on behalf of the controller~~, to submit its data-processing facilities for audit of the processing activities covered by the Ad hoc clauses, which shall be carried out by the controller, the data exporter ~~on behalf of the controller~~, or an inspection body composed of independent **and impartial** members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the controller or the data exporter ~~on behalf of the controller~~, where applicable, in agreement with the data protection supervisory authority competent according to the applicable data protection law;

Comments: Same comments as under clause 4f)

Same comment as under clause 5c) above.

(e) That, in the event of sub-processing by the data importer or by a subsequent sub-processor, the processing activity is carried out in accordance with Clause 11 by a subsequent sub-processor providing at least **an equivalent** ~~the same~~ level of protection for the personal data and the rights of data subjects as the data importer under the ad hoc Clauses. The data importer will inform, ~~taken by the controller according to the Framework Contract~~ **the subsequent sub-processor on the authorisation decision relating to sub-processing referred to in Clause 11.1** and will transfer any necessary information to the subsequent sub-processor;

(f) That if the sub-processing carried out by himself or any subsequent sub-processor is allowed by the controller, it shall communicate to the data exporter **upon request by data exporter at reasonable interval** an updated list of any sub-processing agreements which shall be updated at least once a year. The data importer shall send promptly to the data exporter upon request any **clause relating to the processing of personal data specified in** sub-processor agreement concluded according to the Ad hoc clauses and in particular Clause 11;

Comment: Same comment as under Clause 4 p)

¹³ **A request by the data controller or data exporter would be deemed reasonable if it is done in good faith in the course of performance of the agreement and for reasonable justification. Examples of good faith requests are for instance without being exclusive in case of reasonable suspicion of a breach of its security obligations, in case of a request by a competent data protection supervisory authority, if the data controller is under a legal requirement to demonstrate a certain level of compliance with security measures.**

(g) That it will promptly ~~confirm~~ **confirm** to the data exporter upon request ~~having about the effective implementation of~~ the security measures ~~by itself or through and by~~ any subsequent sub-processor, ~~in accordance with the instructions of the controller;~~

(h) **Option 1** That it has no reason to believe that the legislation applicable to it or to any subsequent sub-processor prevents ~~it~~ **the latter(s)** from fulfilling the controller's instructions and **their respective** obligations and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Ad hoc clauses **and the subprocessing agreements, the Framework Contract and the applicable data protection law**, it will promptly inform the data exporter of such changes, as soon as it is aware of it; in which case the controller is entitled to suspend the transfer of data and/or **require the terminateion of the relevant subprocessing agreement the Framework Contract**. If it does so, the data exporter shall suspend the transfer of data and/or terminate the Ad hoc clauses in accordance with the controller's instructions. If the controller or the data importer do so, the data importer shall suspend the transfer of data and/or terminate any sub-processing agreement in accordance with the controller's instructions;

Option 2 **That the Framework Contract the data controller has no reason to believe that the legislation applicable to the data importer and any subsequent sub-processor prevents the latter(s) from fulfilling their respective obligations under the Ad hoc clauses and their sub-processing agreements, and if the data controller becomes aware of such facts, for instance from a notification received from the data importer or a subprocessor or in the event of a change of legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Ad hoc clauses, the data controller (i) will promptly inform the data exporter of such fact, as soon as it is aware about it, and (ii) is entitled afterwards to suspend the transfer of data.**

Comment: Same comment as under clause 4 l)

(i) That it will promptly notify the data exporter about:

- Any legally binding request disclosure of the personal data by a law enforcement authority, unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
- Any accidental or unauthorised access;
- Any request received directly by the data importer or any subsequent sub-processor from the data subjects without responding to that request, unless it has been otherwise authorised to do so **by the controller or data exporter**; and
- In case of sub-processing, any notification of the subsequent sub-processor in accordance with Clause 5 or 113(1);

(j) To make available to the data subjects upon request a copy of the Ad hoc clauses, or any **clauses relating to the processing of personal data included** sub-processing agreement in

those cases where the data subject is unable to obtain a copy from the controller or the data exporter with the exception of Appendix 2 which shall be replaced by a summary description of the security measures, unless the Ad hoc clauses or the **relevant clauses of the** sub-processing agreement contain commercial secret information, in which case it may remove such commercial secret information;

Comment: Same comment as under Clause 4 p)

(k) That it will ensure compliance with Clauses 5(a) to (k). If it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply. In this case, the controller is entitled to suspend the transfer of data and/or terminate the Framework Contract **as appropriate having regard to the nature and consequences of the breach and the ability of the defaulting party or the data exporter to cure it**. If it does so, the data importer shall suspend the transfer of data and/or terminate any sub-processing contract in accordance with the controller's instructions.

Comment: same comment as under 4 Clause q)

Clause 6

Liability

Comment: We believe that this Clause and Clause 3 should be simplified. It could be done by restating at first the following principle : each party/processor can be held liable to the data subjects for the damages suffered as a result of a breach of the Ad hoc Clauses which are caused by said party/processor or any subprocessor it has engaged. Consistency with clause 4b) (15) must be ensured.

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations, referred to in Clause 3 or in Clause 11 by the data exporter, the data importer or any subsequent sub-processor is entitled to receive compensation from the data exporter for the damage suffered, where the controller has factually disappeared or has ceased to exist in law, unless any successor entity has assumed the entire legal obligations of the controller by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The data exporter may not rely on a breach by the data importer or by any subsequent sub-processor of its obligations in order to avoid its own liabilities.

2. If a data subject is not able to bring a claim against the data exporter referred to in paragraph 1, arising out of a breach by the data exporter or data importer or any subsequent sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against

such entity. The data importer may not rely on a breach by its sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by any subsequent sub-processor of any of its obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subsequent sub-processor agrees that the data subject may issue a claim against the subsequent sub-processor as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data, the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce his/her rights against such entity. The liability of the subsequent sub-processor shall be limited to its own processing operations under the Ad hoc clauses.

4. Notwithstanding clause 3.5 and 11, the data exporter shall be liable to the controller for any breach of the Framework Contract, the Ad hoc Clauses or any sub-processing agreement by itself, the data importer or any subsequent sub-processor.

5. Clause 6 is without prejudice of the liability of the controller in accordance to the Framework Contract and the applicable data protection law.

6. The provisions of Clause 6 shall be understood without prejudice to any data exporter's liability, as a data processor according to the provisions of the applicable data protection law.

Clause 7

NOT COMMENTED

Mediation and jurisdiction

1. The data exporter agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Ad hoc clauses, the data exporter will accept the decision of the data subject:

(a) To refer the dispute to mediation, by an independent person or, where applicable, by the Data protection supervisory authority competent according to the applicable data protection law;

(b) To refer the dispute to the court competent according to the applicable data protection law.

2. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Ad hoc clauses, the data importer will accept the decision of the data subject:

(a) To refer the dispute to mediation, by an independent person or, where applicable,

by the Data protection supervisory authority competent for the controller;

(b) To refer the dispute to the court competent for the controller.

3. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Comment: The provision is a comprehensible method of making the supervisory body of the Controller the competent body also for the processor or subsequent sub-processors, though this approach would need additional provisions in order to ensure the cooperation between DPAs (maybe in the Draft Regulation) for better coordination in case of audits launched from multiple countries.

Cooperation with the Data protection supervisory authority competent for the controller

1. The parties agree that the Data protection supervisory authority competent for the controller has the right to conduct an audit of the data exporter, the importer, and of any subsequent sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the controller under the applicable data protection law.

2. The data importer shall promptly inform the data exporter about the existence of any legislation applicable to it or to any subsequent sub-processor preventing the conduct of an audit of the data importer, or any subsequent sub-processor, pursuant to paragraph 1. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(h).

Clause 9

Governing law

The Ad hoc clauses shall be governed by the law of the Member State in which the controller is established.

Comment: Same comment as under clause 1 f)

Clause 10

NOT COMMENTED

Variation of the contract

The parties undertake not to vary or modify the Ad hoc clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Ad hoc clauses.

Clause 11

Sub-processing by the data importer

1. The data importer shall not subcontract any of its processing operations performed ~~on behalf of the controller~~ under the Ad hoc clauses without the prior ~~written~~ authorisation of the controller or of the data exporter given on behalf and according to the instructions of the controller. ~~The data importer will warrant that any subsequent sub-processor provides sufficient guarantees, notably in respect of the technical and organizational security measures. Where the data importer subcontracts its obligations under the Ad hoc clauses, with the prior written authorisation of the controller, it shall do so only by way of a sub-processing agreement with the subsequent sub-processor which imposes the same obligations on the subsequent sub-processor as are imposed on the data importer under the Ad hoc clauses including the technical and organisational security measures (specified in Appendix 2 to these Ad hoc clauses) and the duty to process data in accordance with the controller's instructions and will guarantee the respect of those duties¹⁴. Where any subsequent sub-processor fails to fulfil its data protection obligations under such sub-processing agreement, the data exporter shall remain fully liable to the controller for the performance of the sub-processor's obligations under such agreement.~~

To claim the benefit of this authorisation, the data importer :

- must obtain a specific authorisation for each subcontractor,

¹⁴~~This requirement may be satisfied by the subsequent sub-processor co-signing the contract entered into between the data exporter and the data importer.~~

- must inform the data controller or the data exporter prior to the appointment of any subprocessor; failure by the data controller/data exporter to object to the appointment in a timely fashion allows to proceed with the appointment of the subprocessor,
- benefits from a general authorisation to subcontract to entities which belong to the same group as the data exporter within a pre-determined geographical scope, provided that their list is made available to the data controller upon grounded request,
- benefits from a general authorisation to subcontract within a pre-determined geographical scope, provided that the list of subprocessors is made available to the data controller and/or data exporter upon grounded request,
- benefits from a general authorisation to subcontract to the subprocessors identified on a list issued by the data exporter, such list to be provided to the data controller at the time of execution of the Framework Contract and thereafter maintained up to date by the data exporter, who shall provide it to the data controller upon request.

Comment: the parties will select between the options, which are in line with clause 4 g). The data exporter may however decide not to give the possibility to the data importer to subcontract as widely as he himself can.

~~2. The sub-processing agreement concluded between the data importer and the subsequent sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 (1) to (4), for cases where the data subject is not able to bring the claim for compensation referred to in Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third party liability of the subsequent sub-processor shall be limited to its own processing operations under the Ad hoc clauses.~~

~~3. That, in the event of sub-processing by the data importer or the subsequent sub-processor, the data importer has communicated the controller's instructions and will do so throughout the duration of the personal data processing services to any subsequent sub-processor to process the personal data exclusively on the controller's behalf and in accordance with its instruction and with the terms of the Framework Contract, the Ad hoc clauses, any sub-processing agreement and the applicable data protection law.~~

2. The data importer will warrant that any subsequent sub-processor provides sufficient guarantees, notably in respect of the technical and organisational security measures. Where the data importer subcontracts its obligations under the Ad hoc clauses ~~with prior written authorisation of the controller~~ **as authorised under clause 11.1**, it shall do so only by way of a sub-processing agreement with the subsequent sub-processor which imposes the same obligations on the subsequent sub-processor as are imposed on the data importer under the Ad hoc clauses including the technical and organisational security measures (specified in Appendix 2 to these Ad hoc clauses) and, the duty to process data in

accordance with the controller's instructions and will guarantee the respect of those duties¹⁵. Where any subsequent sub-processor fails to fulfil its data protection obligations under such sub-processing agreement, the data exporter shall remain fully liable to the controller for the performance of the subsequent sub-processor's obligations under such agreement.

3. The sub-processing agreement concluded between the data importer and the subsequent sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3(1) to (4), for cases where the data subject is not able to bring the claim for compensation referred to in Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subsequent sub-processor shall be limited to its own processing operations ~~under the Ad hoc clauses~~.

4. That, ~~in the event of sub-processing by the data importer or the subsequent~~ **sub-processors are committed to provide at least an equivalent level of protection for the personal data and the rights of the data subjects as the data importer under the ad hoc Clauses in accordance with the information received from the data importer or the subsequent sub-processor** ~~the data importer, has communicated the controller's instructions and will do so throughout the duration of the personal data processing services to any subsequent sub-processor to process the personal data exclusively on the controller's behalf and in accordance with its instruction and with the terms of the Framework Contract, the Ad hoc clauses, any sub-processing agreement and the applicable data protection law.~~

5. The sub-processing agreement between the data importer and the subsequent sub-processor shall also provide for a third-party beneficiary clause for the benefit of the controller as laid down in Clause 3(5).

6. ~~In case of subcontracting the processing operations referred to in paragraph 1, the provisions on data protection are those of the applicable data protection law.~~

Comment: deleted because addressed in clause 4 above

Clause 12

NOT COMMENTED

Termination of the contract

1. The data exporter shall suspend the transfer of data and/or terminate the Ad hoc clauses according to the instruction of the controller, and notably when the Framework Contract is terminated.

¹⁵ **This requirement may be satisfied by the subsequent sub-processor co-signing the contract entered into between the data exporter and the data importer.**

2. The data importer shall suspend the data transfer and/or terminate any sub-processing contract concluded with subsequent sub-processors according to the controller's instructions, and notably when the Ad hoc clauses or the Framework Contract is terminated.

Clause 13

NOT COMMENTED

Obligations after the termination of personal data-processing services

1. On the termination of personal data-processing services or of the Framework Contract, the data exporter shall, at the choice of the controller, return all the personal data processed on behalf of the controller by the data exporter, the data importer or any subsequent sub-processor and the copies thereof to the controller or shall destroy all the personal data and certify to the controller that it has done so, as well as the data importer and any subsequent sub-processor, unless legislation imposed upon data exporter, the data importer or any subsequent sub-processor prevents one of the latter from returning or destroying all or part of the personal data transferred and processed. In that case, the data exporter warrants making full transparency of it towards the controller, and that it, as well as the data importer, and any subsequent sub-processor will guarantee the confidentiality of the personal data transferred and processed and will not actively process the personal data anymore.

2. On the termination of the Ad hoc clauses, the data importer shall, at the choice of the controller that may be expressed on its behalf by the data exporter, return all the personal data processed by the data importer or any subsequent sub-processor and the copies thereof to the controller or to the data exporter on the controller's behalf or shall destroy all the personal data and certify to the controller or to the data exporter on the controller's behalf that it has done so, as well as any subsequent sub-processor, unless legislation imposed upon the data importer or any subsequent sub-processor prevents one of the latter from returning or destroying all or part of the personal data transferred and processed. In that case, the data importer warrants making full transparency of it towards the controller or to the data exporter on controller's behalf and that it, as well as any subsequent sub-processor will guarantee the confidentiality of the personal data transferred and processed and will not actively process the personal data anymore.

3. The data exporter, the data importer and any subsequent sub-processor warrant that upon request of the controller or of the data exporter on behalf of the controller and/or of the Data protection supervisory authority competent for the controller, it will submit its data-processing facilities for an audit of the measures referred to in paragraphs 1 and 2.

On behalf of the data exporter

Name (written out in full):

.....

Position:

.....

Address:

.....

Other information necessary in order for the contract to be binding (if any):

.....

(Stamp of organisation)

Signature:

On behalf of the data importer

Name (written out in full):

.....

Position:

.....

Address:

.....

Other information necessary in order for the contract to be binding (if any):

.....

(Stamp of organisation)

Signature:

Appendix 1 to the Ad hoc clauses

This Appendix forms part of the Ad hoc clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Controller

The controller is *(please list the controller(s) to which the data exporter provides personal data processing services, and specify briefly its/their activities relevant to the transfer)*:

.....
.....
.....

Data exporter

The data exporter is *(please specify briefly your activities relevant to the transfer)*:

.....
.....
.....

Data importer

The data importer is *(please specify briefly activities relevant to the transfer)*:

.....
.....
.....

Data subjects

The personal data transferred concern the following categories of data subjects *(please specify)*:

.....
.....
.....

Categories of data

The personal data transferred concern the following categories of data (*please specify*):

.....
.....
.....

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (*please specify*):

.....
.....
.....

Processing operations

The personal data transferred will be subject to the following basic processing activities (*please specify*) and purposes:

.....
.....
.....

Data subjects' rights

(Please specify the data importer's duties in case the data controller, data exporter or the data importer receives a data subject request concerning information that is processed by the data exporter or the data importer):

.....
.....
.....

Personal data destruction or deletion upon termination

(Please specify the data importer's duties regarding both scenari, depending on the data controller's decision):

.....
.....
.....

DATA EXPORTER:

Name:

.....

Authorised

signature.....

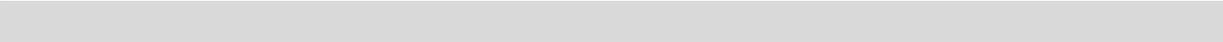
DATA IMPORTER:

Name:

.....

Authorised

signature.....



NOT COMMENTED

Appendix 2 to the Ad hoc clauses

This Appendix forms part of the Ad hoc clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(b) (or document/legislation attached):

.....
.....
.....
.....

ILLUSTRATIVE INDEMNIFICATION CLAUSE (OPTIONAL)

Liability

The parties agree that if one party is held liable for a violation of the Ad hoc clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

- a) The data exporter promptly notifying the data importer of a claim; and
- b) The data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim¹⁶.

¹⁶ Paragraph on liabilities is optional.