

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Strasbourg, 2 March / mars 2022

T-PD(2022)1Mos

**CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION  
OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING**

**OF PERSONAL DATA COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION  
DES PERSONNES A L'ÉGARD DU TRAITEMENT AUTOMATISÉ  
DES DONNÉES A CARACTÈRE PERSONNEL**

**CONVENTION 108+**

**Compilation of Comments on  
Standard Contractual Clauses for Transborder Flows**

**Compilation des commentaires sur les  
Clauses contractuelles types relatives aux flux transfrontières de données**

## TABLE OF CONTENT / TABLE DES MATIÈRES

EUROPEAN UNION – EUROPEAN COMMISSION (EC) / UNION EUROPÉENNE – COMMISSION EUROPÉENNE (CE).....	3
EUROPEAN UNION – EUROPEAN DATA PROTECTION SUPERVISOR (EDPS) / UNION EUROPÉENNE – CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES (CEPD) .	17
FINLAND / FINLANDE .....	24
FORMER CHAIR OF THE COMMITTEE / ANCIEN PRÉSIDENT DU COMITÉ.....	26
GERMANY / ALLEMAGNE .....	31
INTERNATIONAL COMMITTEE OF THE RED CROSS (ICRC) / COMITÉ INTERNATIONAL DE LA CROIX ROUGE (CICR) .....	32
ITALY / ITALIE .....	37
SWEDEN / SUÈDE .....	42
TURKEY / TURQUIE.....	43
UNITED KINGDOM / ROYAUME-UNI .....	44
UNITED KINGDOM – INFORMATION COMMISSIONER'S OFFICE (ICO) / ROYAUME-UNI – BUREAU DU COMMISSAIRE DE L'INFORMATION (ICO).....	46

## EUROPEAN UNION – EUROPEAN COMMISSION (EC) / UNION EUROPÉENNE – COMMISSION EUROPÉENNE (CE)

(...)

Term/Duration: Start date [MM/DD/YEAR] - End date [MM/DD/YEAR]

(...)

**Commented [A1]:** This makes sense mainly for the controller-processor relationship, but will in most cases not fit C-C transfers

**NOTE:** These contractual clauses provide an appropriate level of protection for the transfer of personal data to a ~~Third non-state Party country~~ under Article 14.23 b) of Modernized Convention 108.

**Commented [A2]:** The legal nature of these clauses, and their legal effects in the domestic law of the Parties, will have to be discussed. In our view, this should be a model contract that Parties to the Convention CAN approve under Article 14.3 b)

### STANDARD CONTRACTUAL CLAUSES

Contractual clauses for ~~transborder flows of data international transfers~~ from controller to controller

(...)

**Commented [A3]:** This is the wording of the "heading" of Article 14 of Conv108+, but in the text the (correct) term "transfer of personal data" (to a State not Party to the Convention) is used; see also below Clause 1

### PART I - GENERAL CLAUSES

#### Clause 1. Purpose and scope

1.1. The aim of these standard contractual clauses is to ensure compliance with the requirements for the transfer of personal data to a ~~Third non-state Party country~~ under Convention 108+ (hereinafter the Convention). ~~These contractual clauses provide an appropriate level of protection for the transfer of personal data under Article 14(2)(b) of the Convention~~

**Commented [A4]:** Since this will be used first of all by private entities, perhaps better to say "to a [country/state] that is not Party to [Convention 108+/full title of the Convention]"

[OPTION] This Agreement sets forth the terms and conditions governing the transfer of personal data to a Third country from an entity subject to Convention 108+ (hereinafter the Convention).

**Commented [A5]:** See comment above on the legal nature/effect of the clauses

(...)

**Commented [A6]:** Why is this an option and how does this relate to the previous sentence?

#### Clause 2. Definitions

(...)

**Commented [A7]:** Not clear what is meant here: the data exporter as such will not be an "entity subject to Convention 108+" (only States are)

**Convention:** ~~Modernized Protocol CETS No 223 amending Convention for the Protection of Individuals with regard to the processing of Personal Data (CE=TS No. 108) amending Protocol to the Convention for the Protection of Individuals with Regard to the Processing of Personal Data~~, adopted by the Committee of Ministers at its 128th Session in Elsinore on 18 May 2018.

**Commented [A8]:** But the Amending Protocol is not Convention 108+... this should rather read something like "Convention 108... as amended by Protocol..."

**Clauses:** Standard contractual clauses approved under the Convention.

**Commented [A9]:** Convention 108+ does not use the term "standard contractual clauses", but rather speaks of "approved standardised safeguards provided by legally binding and enforceable instruments"

**Data processing:** any operation or set of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data. ~~Where automated processing is not used, Data processing means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria.~~

[Source: Article 2 of the Convention]

**Commented [A10]:** Can this be relevant for data transferred?  
**Commented [A11]:** To be considered how to identify defined terms (and whether there is really a need to "visually" identify them)

**Data importer:** is the ~~natural or legal person, [public authority, service, agency or any other body], located in a Third non-state Party country, to which is the Recipient of a transfer of the~~ personal data ~~is transferred~~ from ~~a the~~ Data exporter.

**Data exporter:** is the ~~natural or legal person, [public authority, service, agency or any other body]~~ which, alone or jointly with others, ~~has decided~~ to transfer personal data to a ~~Third country non-State Party.~~

**Data subject:** an identified or identifiable individual whatever his or her nationality or residence.

[Source: Article 2 of the Convention]

(...)

**Commented [A12]:** To be discussed – perhaps one could instead refer to the controller/processor in a non-Party to whom the data exporter transfers the data?  
If the terms controller/processor are not used, it will be important to have a sufficiently broad definition here (e.g. the data importer might not always be a natural or legal person)  
**Commented [A13]:** See above: one could again refer instead to the controller/processor transferring the personal data  
**Commented [A14]:** Since these are C-C clauses, this is correct, but in our view it would be better to have a more "generic"/factual definition that refers simply to the fact of the transfer (rather than who took the decision to do so)  
**Commented [A15]:** Would merge this into the definition of "personal data" (as is done in Article 2)

**Data breach:** Any ~~non-authorized non-authorized~~ ~~access to, destruction, loss, use, modification or disclosure access or disclosure~~ of Personal Data due to a violation of the principle of data security, ~~in which sensitive, protected data or confidential data is copied, transmitted, viewed, stolen or used by an individual or entity unauthorized to do so.~~

[Source: Article 7 of the Convention]

(...)

**Commented [A16]:** This is too narrow: Article 7(1) also refers to "accidental"  
**Commented [A17]:** TBD (Article 7(1) of course stipulates security obligations to avoid data breaches, but not sure whether this means the violation of such obligations has to be made part of the definition of data breach)  
**Commented [A18]:** Not clear where this is coming from, or why it would be needed – would suggest deleting

~~Transborder flows of data~~ **International transfers of personal data**: transfer of personal data to a ~~Recipient located in a Third country~~ a jurisdiction of another State or to an international organization.

[Source: Article 14.1 of the Convention, Par. 102. of Explanatory Rep]

(...)

**Onward transfer**: when Personal data transferred to another state-Party is ~~likely to be~~ further transferred to a Party located in a jurisdiction without an appropriate level of protection being ensured [OR which is not considered adequate].

[Source: Par. 106 of Explanatory Report]

(...)

**Processor**: means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf [and under the instructions] of the Controller.

[Source: Article 2 of the Convention]

(...)

**Sensitive data**: ~~personal data that is~~ (i) ~~related to~~ Genetic data, ~~or~~ (ii) personal data relating to offences, criminal proceedings and convictions, or related security measures; ~~or~~ (iii) Biometric data uniquely identifying a person; or (iv) personal data for the information they revealing data relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life.

[Source: Article 6 of the Convention]

**Supervisory authority/ies**: One or more authorities responsible for ensuring compliance with the provisions of the Convention and the Applicable law.

[Source: Article 15 of the Convention]

~~Third country~~ **Non-state Party**: a country that has not ratified the Convention or where it is not fully in force.

**Third Party Beneficiary**: the Data subject whose Personal data is the object of ~~an transborder flow(s) of data~~ International transfer.

**Commented [A19]**: Why do we need this (defined) term (which Convention 108+ only uses in the headings of Article 14)? If necessary, one could include a definition of "transfer of personal data", namely "the disclosure or making available to a recipient subject to the jurisdiction of a non-Party State or international organisation"

**Commented [A20]**: shouldn't it be clear that this is about further transfers by the importer?

**Commented [A21]**: This does not seem to make sense: the question of the level of protection concerns whether an onward transfer can be allowed, but not the definition of what is an onward transfer. For the latter, the only thing that should matter is that the recipient of the original transfer further transfers (or perhaps just: discloses) the data. One could exclude further transfers to recipients located in the jurisdiction of the original data exporter (and perhaps also in the jurisdiction of a Party to the Convention, although this would not work for the EU Member States to which Article 14(1), first sentence, will not apply)

**Commented [A22]**: What about the clauses themselves (which for the purposes here is the most important)? Also, in most (if not all) Parties the Convention itself is probably not directly applicable, but rather "transposed" by domestic ("applicable") law, which also means the supervisory authority/ies will not (be able to) ensure compliance with the Convention as such

**Commented [A23]**: Not clear – what does "not fully" mean? how would this be applied in practice (by a company)?

**Commented [A24]**: See above: "... of a transfer of personal data based on/under these clauses"

However, does this mean that data subjects would be third party beneficiaries for ALL the clauses? Even those that are only concern the data exporter/importer?

**Clause 3. General clauses**

**3.1. Invariability of the Clauses**

These Clauses set out appropriate safeguards, including enforceable data subject rights, obligations for data controllers and effective legal remedies, pursuant to Article 14(2)(b) of the Convention and, with respect to data transfers from controllers to controllers, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Annexes.

**Commented [A25]:** See above on the legal nature/effect of the clauses

**Commented [A26]:** Not clear what this is supposed to mean (in any event, those are supposed to be C-C clauses)

**Commented [A27]:** The text does not seem to contain modules

This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental human rights or fundamental freedoms of data subjects recognized in the Convention.

These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of the Convention and the Applicable law.

**Commented [A28]:** See earlier comment: in most (if not all) Parties the Convention will not be directly applicable

**Interpretation**

Where these Clauses use terms that are defined in the Convention, those terms shall have the same meaning as in the Convention and its Explanatory Report.

**Commented [A29]:** This might go too far (the ER is not binding law), but perhaps one could say something like: "interpreted in the light of...?"

These Clauses shall be read and interpreted in the light of the provisions of the Convention and the Applicable law.

**Commented [A30]:** Not sure this would be a good idea: those are supposed to be model clauses developed based on the Convention, and their interpretation should not vary according to domestic (applicable) law

These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in the Convention and the Applicable law.

**Commented [A31]:** See earlier comments on the effect of the Convention. Perhaps one could say something like "...rights and obligations provided for in the Convention as incorporated into Applicable law?" or "...provided for in Applicable law incorporating the Convention?"

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Capitalized terms used but not defined in these Clauses (including the Annexes) have the meanings given to them in the agreement into which these Clauses are incorporated.

**Commented [A32]:** Those are supposed to be model clauses that should not be modified, and they have been/will be developed independently of what can be found in the different domestic laws of the Parties. If there is a need to define terms (in the light of the second paragraph of this clause on interpretation in the light of the Convention), that should be done in the Clauses

**Clause 4. Accession clause**

An entity that is not a Party to these Clauses may, with the agreement of the other Parties, accede to these Clauses at any time, either as a Data exporter or as a Data importer, by completing and signing the form available in Annex 2.

Once it has completed and signed the form of Annex 2, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a Data exporter or Data importer in accordance with its designation in the form Annex 2.

(...)

### Clause 5. Third Party Beneficiaries

The Parties agree and acknowledge that (a) any Data subject whose Personal data ~~was part of an international data~~ transferred under these Clauses shall be entitled to assert rights and remedies hereunder as a Third-party beneficiary with respect to any provisions of these Clauses affording a right, action, claim, benefit or privilege to such Data subject and (b) the jurisdiction established in Clause 25 is for the benefit of the Data Subject and the Parties shall not challenge such recognition of jurisdiction.

**Commented [A33]:** As "rights" might be (mis-)understood as referring only to the specific rights (access, etc.), it might be better to say something like: "...entitled to invoke the [safeguards/guarantees] set out in these Clauses"

**Commented [A34]:** This is perhaps clear for the specific rights (which refer specifically to the data subject), but is it also sufficiently clear for the principles and obligations? It might be better/safer to either list (positively or negatively) the provisions that afford third party beneficiary rights, or to use a formulation like "... any provisions of these Clauses that are intended to protect the interests of the Data subject", or "for which the Data subject falls within the zone of interests to be protected"

**Commented [A35]:** Not entirely clear to us what this means – would be good to better understand the objective behind this. Perhaps the last part ("is for the benefit of the Data Subject and the Parties shall not challenge such recognition of jurisdiction") could be deleted?

## SECTION II – RIGHTS AND OBLIGATIONS OF THE PARTIES

### Clause 6. Data protection safeguards

(...)

The Data exporter represents that it has the right to transfer the personal data to the Data Importer in accordance with this Agreement and the Applicable law.

**Commented [A36]:** Not entirely clear to us what this means, especially the reference to "this Agreement" (which is not a defined term)

### Clause 7. Purpose limitation

The Data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex 1.

Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes.

[Source: Article 5(4) (b) of the Convention]

**Commented [A37]:** This would not work: either there is a principle of compatible processing in the first sentence (as in Article 5(4)(b) of the Convention), or one applies a principle of strict purpose limitation, in which case processing for ARS purposes would have to be added to the first sentence as an allowed (not: compatible) purpose (e.g. "may not process ... for (an)other purpose(s) than the one/those in Annex 1, or for archiving..., subject to appropriate safeguards"

**Commented [A38]:** Article 5(4)(b) allows processing for a compatible purpose, but of course this doesn't mean that one could not impose strict purpose limitation in a transfer context

### Clause 8. Transparency of processing

8.1. In order to enable Data subjects to effectively exercise their rights pursuant to these Clauses, the Data importer shall inform them, either directly or through the Data exporter of:

(...)

b. the legal basis and the purposes of the intended processing;

(...)

d. the recipients or categories of recipients of the personal data, if any; and

(...)

**Commented [A39]:** What does this refer to? The legal basis under the law of the importer? Wouldn't the importer be processing the data on the basis of the clauses (and only for the purposes set out in the clauses)?

f. of the right to obtain a copy of these Clauses;

**Commented [A40]:** This is only about providing information about this right, but the right itself does not seem to be established anywhere in the clauses

8.2. Paragraph 1 shall not apply where the Data subject already has the relevant information or where the processing is expressly prescribed by law ~~binding the data subject~~ or this notification proves to be impossible or involves disproportionate efforts.  
[Source: Article 8 of the Convention]

**Commented [A41]:** Is this really relevant in the case of a commercial contract based on the Clauses?

### Clause 9. Accuracy and data minimisation

(...)

~~If from time to time~~ the Data importer is informed by the Data Exporter of corrections made by Data Exporter to the Personal Data, the Data importer will promptly implement ~~all those~~ corrections.

**Commented [A42]:** Shouldn't there also be an obligation for the Data importer to inform the Data exporter of corrections (made by the Data importer)?

(...)

### Clause 11. Data security

The Data importer, and, during transmission also the Data exporter, shall adopt appropriate security measures against risks such as accidental or unauthorized access to, destruction, loss, use, modification or disclosure of personal data.

In particular, the Data importer shall adopt ~~specific~~ appropriate security measures, both of a technical and organizational nature, for each processing, taking into account in particular: the potential adverse consequences for the individual, the nature of the personal data, the volume of personal data processed, the degree of vulnerability of the technical architecture used for the processing, the need to restrict access to the data, the potential adverse consequences of any data breach for the individual, and the current state of the art of data-security methods and techniques in the field of data processing, ~~requirements concerning long-term storage, and so forth.~~

**Commented [A43]:** Not clear what is meant here (and there shouldn't be a suggestion that "long-term storage" is generally fine) – would suggest deleting

~~The security measures mentioned above should take into account the current state of the art of data-security methods and techniques in the field of data processing.~~ Their cost should be commensurate with the seriousness and probability of the potential risks. Security measures should be kept under review and updated where necessary.

**Commented [A44]:** Already covered by the next paragraph

The Parties have agreed on the technical and organizational measures set out in Annex 3. The Data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security, and shall update them where this is no longer the case.

(...)

~~Each Party shall provide that the Controller notifies, without delay, at least the competent Supervisory Authority of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects.~~



T-PD(2022)1Mos

In case where a Data breach has occurred that may seriously interfere with the ~~fundamental human~~ rights and ~~fundamental~~ freedoms of the individual (e.g. ~~for instance~~, the disclosure of data covered by professional confidentiality, sensitive data, or ~~data~~ which may result in financial, reputational, or physical harm or humiliation) the Data importer shall notify ~~without [undue] delay~~ the Data Exporter and the ~~relevant~~ Supervisory Authority/ies of (i) -the incident including a complete description of the Data Breach, and (ii) of any measures taken and/or proposed to address the breach and its potential consequences.

**Commented [A45]:** The standard in Article 7(2) is "without delay"

[Source: [Article 7\(2\), point 65](#) of the Explanatory Report]

~~If the data breach is likely to result in a significant risk for the rights and freedoms of individuals, (such as discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage), the Data importer, and also if necessary with the assistance of the Data Exporter, shall notify the Data subjects ~~involved in (potentially) concerned by~~ the Data breach and provide them with adequate and meaningful information on, notably, the contact points and possible measures that they could take to mitigate the adverse effects of the Data breach.~~

**Commented [A46]:** We understand that this is based on para 66 of the Expl Report, but it is nevertheless a bit odd that the Clauses would apply two different (ly worded) standards ("seriously interfere", "significant risk") together with different explanations ("e.g. for instance, the disclosure of data covered by professional confidentiality, sensitive data, or data which may result in financial, reputational, or physical harm or humiliation"; "such as discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage") for the notification to the DPA and to the individual

[Source: Paragraph 66 of the Explanatory Report]

~~If the Data importer does not spontaneously inform the Data subject of the Data breach, the supervisory authority, having considered the likely adverse effects of the breach, should be allowed to require the controller to do so. Notification to other relevant authorities such as those in charge of computer systems security may also be desirable.~~

**Commented [A47]:** These are Clauses concluded between two (private) Parties, they cannot impose duties on public authorities (and in any event, since the supervisory authorities are those of the Data exporter, which will come from a jurisdiction subject to Convention 108+, there is no need to repeat the Convention/ER)

[Source: [Article 7 of the Convention & Paragraphs 62 to 66](#) of the Explanatory Report]

~~[It might be useful to indicate that, where not all the relevant information is available, notification can happen "in stages", with more information to be provided as soon as possible]~~

## Clause 12. Sensitive data

(...)

~~Such safeguards must guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject [notably a risk of discrimination].~~

**Commented [A48]:** We understand that this is the wording of Article 6(2) of the Convention, but all of this is already covered by the first paragraph (we would be agnostic as to whether to use "adapted to" or "guard against")

These safeguards may include, for instance, alone or cumulatively (i) ~~requesting~~ the data subject's explicit consent for the processing of sensitive data; (ii) ~~applying rules ensuring~~ professional secrecy ~~obligation~~; (iii) ~~measures following a risk analysis~~; (iv) a particular and qualified organizational or technical security measure (e.g. data encryption, pseudonymisation), (v) limiting the personnel permitted to access the Sensitive data, ~~and or~~ (vi) additional restrictions with respect to further disclosure according to the nature of the data.

**Commented [A49]:** It might be better to say that the Parties shall set out these measures in Annex X, and then to include these examples there as a "chapeau"

[Source: [Article 6 of the Convention and Paragraphs 56 to 61](#) of the Explanatory Report]

### Clause 13. Onward transfers

The Data importer shall not disclose the personal data to a third party located in a ~~Third country~~ non-state Party unless the third party is or agrees to be bound by these Clauses.

**Commented [A50]:** To be noted that for the EU Member States this will not work, as also (onward) transfers to non-EU Parties will require safeguards

An Onward transfer by the Data importer may ~~only~~ take place only- if:

(i) the ~~recipient is subject to the jurisdiction law of that~~ State or international organization ~~whose where the Personal data is transferred law~~, including the applicable international treaties or agreements, ~~provide secure~~ an appropriate level of protection ~~in accordance with a~~ Article 14(2),(3)(a) of the Convention;

**Commented [A51]:** This formulation suggests that joining the Clauses is the only option, whereas the next sentence (with the list of (i) to (v)) makes clear that there are also other alternatives. Therefore, the next sentence should start differently, for instance: "Otherwise, an onward transfer ..."

(ii) the third party enters into a binding instrument with the Data importer ensuring the same level of data protection as under these Clauses, and the ~~d~~Data importer provides a copy of these safeguards to the ~~d~~Data exporter;

**Commented [A52]:** To be discussed whether these Clauses should even cover any (onward) transfers to international organisations

(...)

**Commented [A53]:** TBD: this raises the important question WHO would determine that the third country ensures an "appropriate level of protection"

(vi) where none of the other conditions apply, the ~~d~~Data importer has obtained the explicit consent of the ~~d~~Data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of ~~an~~ appropriate ~~level of~~ data protection ~~safeguards~~. In this case, the ~~d~~Data importer shall inform the ~~d~~Data exporter ~~of the onward transfer based on consent~~ and, at the request of the latter, shall transmit to it a copy of the information provided to the ~~d~~Data subject.

(...)

### Clause 14. Processing under the authority of the ~~d~~Data importer

(...)

### Clause 15. Documentation and compliance

(...)

In particular, the ~~Data importer-exporter~~ shall keep appropriate documentation of the processing activities carried out under its responsibility.

**Commented [A54]:** We believe that in a C-C contract the reference should be to the Data importer (which will process under its own responsibility)

The ~~Data importer-exporter~~ shall make such documentation available to the competent Supervisory authority/~~ies~~ on request.

**Commented [A55]:** Same here

The Data importer shall take all appropriate measures to comply with the obligations of these Clauses and be able to demonstrate ~~such compliance~~ to the competent Supervisory authority/~~ies~~ mentioned in Clause 20, ~~that the data processing under these Clauses is in compliance with the provisions of the Convention and the Applicable law~~.

**Commented [A56]:** In our view the Clauses should only regulate compliance with "themselves"

~~The Data importer guarantees that it has examined the likely impact of intended data processing on the rights and fundamental freedoms of Data subjects prior to the commencement of such processing, and processing and has designed the data processing in such a manner as to prevent or minimize the risk of interference with those rights and fundamental freedoms.~~

**Commented [A57]:** This appears a bit exaggerated (it seems to suggest the need for a privacy impact assessment in each and every case; moreover, compliance with the Clauses should itself "minimize the risk of interference", whereas it will never be possible to "prevent" any such risk)

~~The Data importer shall implement technical and organizational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing.~~

~~The Data importer shall comply with the duties mentioned in the paragraphs above having regard to the risks arising for the interests, rights and fundamental freedoms of the data subjects, adapt the application of the mentioned duties according to the nature and volume of the data, the nature, scope and purpose of the processing and, where appropriate, the size of the controller or processor.~~

**Commented [A58]:** This is already sufficiently covered by the security clause

~~[Source clause 10 of the Convention]~~

#### Clause 16. Use of sub-processors

~~[PENDING FOR MODULE 2 Transfers from controller to processor]~~

**Commented [A59]:** Does this mean that there will be a "MODULE 2"? It seems indeed important to have clauses on the controller/processor relationship.

#### Clause 17 – Rights of the Data subjects

The Data importer, if required with the assistance of the Data exporter, shall deal with any enquiries and requests it receives from a Data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.

As for the C-C contract, it might still be good to have rules on what the Data importer should do in case it engages a processor (at least an obligation to properly select such a processor and ensure that it only acts upon instructions, and perhaps based on a contract setting out essential elements of the service and requiring the processor to cooperate with the controller)

The Data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the ~~e~~Data subject shall be in an intelligible and easily accessible form, using clear and plain language.

In particular, upon request by the Data subject, the Data importer, ~~or the Data exporter, where applicable,~~ shall provide, free of charge, the following rights:

**Commented [A60]:** Not clear what is meant here – the rights towards the Data exporter will be set out in the domestic (applicable) law, in line with the Convention

a) not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration;

**Commented [A61]:** 'ensure'? Or perhaps this provision could be draft differently, by saying that the data subject has the right ... (a) – (h)

b) to obtain, on request, at reasonable intervals ~~and without excessive delay,~~ confirmation of the processing of Personal data relating to him or her, the communication in an intelligible form of the data processed ~~and transfer,~~ all available information on their origin, on the preservation period as well as any other information that the ~~controller~~ Data importer is required to provide in order to ensure the transparency of processing in accordance with these Clauses;

**Commented [A62]:** The text should be harmonised (in other parts the formulation is "his/her")

(...)

**Commented [A63]:** Would suggest deleting as the first paragraph of this Article already includes timing requirements ("without undue delay and at the latest within one month")

e) to obtain, on request, and without excessive delay, rectification or erasure, as the case may be, of such data if these are being, or have been, processed contrary to ~~these Clauses provisions of this Convention and/or the Applicable law;~~

~~f) to have a remedy under these Clauses where his or her rights under this Agreement, the Convention and/or the Applicable law have been violated;~~  
~~g) to benefit, whatever his or her nationality or residence, from the assistance of a Supervisory authority within the meaning of these Clauses, in exercising his or her rights under these Clauses;~~  
h) To be provided with a contact person on the staff of both Parties, whose responsibility it is to ensure compliance with the substantive standards of protection. ~~The Data subject would be free to contact this person at any time and at no cost in relation to the data processing or transfers and, where applicable, obtain assistance in exercising his or her rights.~~

[Source: Article 9 of the Convention & Par. 111 of the Explanatory Memorandum of Convention]

**Clause 18. Redress for the eData subject**

The Data importer shall inform eData subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints. It shall deal promptly with any complaints it receives from a Data subject.

[OPTION: The eData importer agrees that eData subjects may also lodge a complaint with an independent dispute resolution body at no cost to the eData subject. It shall inform the eData subjects, in the manner set out in paragraph (a), of such a redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

The eData importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.]

~~The alternative mentioned in the paragraph above does not. Nothing in this Clause excludes the right of the Data subject afforded by these Clauses, the Convention and the Applicable law to bring a claim at with the Supervisory Authority/ies or at the courts of the applicable jurisdiction.~~

**Clause 19. Liability.**

(...)

Each Party shall be liable to the eData subject, and the eData subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the eData subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the eData exporter under the Applicable law.

Where more than one Party is responsible for any damage caused to the eData subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the eData subject is entitled to bring an action in court against any of these Parties.

The Parties agree that if one Party is held liable under the previous paragraph, it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to ~~its/their/the other Party's/Parties'~~ responsibility for the damage.

(...)

**Commented [A64]:** This should be covered in Clause 18

**Commented [A65]:** This is covered by Clause 20

**Commented [A66]:** Isn't this already covered by Clause 18, first para?

**Commented [A67]:** TBD – while this is mentioned as a possibility in para 111 of the Expl Report, it suggests the need for some kind of compliance officer/DPO, which in particular for SMEs will often not exist. Also, the obligation in para 1 of this Clause (perhaps together with the right to be provided with a contact person) should be sufficient

**Commented [A68]:** Shouldn't this be broader and also cover other requests and the exercise of individual rights under the Clauses?

**Commented [A69]:** Same comment

**Commented [A70]:** This is neither clear, nor does it look sufficient when it comes to **judicial redress**: the "Applicable law" will only bind the Data exporter, and the same applies to the Convention (if it is at all directly applicable). It should therefore be for the Clauses to "create" judicial remedies, for instance by making the Data importer submit to the jurisdiction of the courts of the Data exporter

### Clause 20. Supervisory authority

The Supervisory authority/~~ies~~ with responsibility for ensuring compliance by the ~~eD~~Data exporter with the Applicable law ~~and the Convention~~ as regards the data transfer shall act as competent Supervisory authority/~~ies~~.

~~The Parties hereby consent that the supervisory authority is entitled to request that the person who transfers data demonstrates the effectiveness of the safeguards or the existence of prevailing legitimate interests and that the supervisory authority may, in order to protect the rights and fundamental freedoms of data subjects, prohibit such transfers, suspend them or subject them to conditions.~~

[Source: article 14.6 of the Convention]

~~The Parties agree to submit to the jurisdiction of the Supervisory authorities and not to question its powers, its jurisdiction, or any other action including any forms of co-operation between supervisory authorities as provided by the Applicable law and article 15 and 17 of the Convention.~~

~~[Source: article 15 and 17 of the Convention]~~

The ~~eD~~Data importer agrees to submit itself to the jurisdiction of and cooperate with the competent Supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

### SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

#### Clause 21. Local laws and practices affecting compliance with the Clauses

The Parties warrant that they have no reason to believe that the laws and practices in the ~~third non-state Party country~~ of destination applicable to the processing of the personal data by the Data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses ~~and the Convention~~.

This is based on the understanding that ~~specific exceptions to these Clauses based on applicable law(s) and practices~~ that respect the essence of ~~the fundamental human~~ rights and ~~fundamental~~ freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in 11(1) of the Convention, are not in contradiction with these Clauses.

~~The Parties declare that in providing the warranty stated in the previous paragraph, they have taken due account in particular of the following elements:~~

**Commented [A71]:** See earlier comments: supervisory authorities will (typically) just be competent to ensure compliance with the domestic (applicable) law (which of course should reflect the Convention)

**Commented [A72]:** This does not seem to make sense: it could only be directed against the Data exporter, for which this will however already follow from the domestic (applicable) law (implementing the Convention)

**Commented [A73]:** This is either covered by the next paragraph, or does not seem necessary (what would the effect of "not questioning" powers/jurisdiction?)

**Commented [A74]:** Why the Convention? This does not apply to the data importer. Isn't what matters here compliance with the clauses?

**Commented [A75]:** Not sure this is the right formulation, as the law will of course not contain "exceptions" to these Clauses, but will rather contradict certain obligations.

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(...)

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfill its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation–. The Data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the Data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 23(d) and (e) shall apply.

#### Clause 22. Obligations of the data importer in case of access by public authorities

(...)

### SECTION IV – FINAL PROVISIONS

#### Clause 23. Non-compliance with the Clauses and termination

(...)

(e) Either Party may revoke its agreement to be bound by these Clauses where the Supervisory authority adopts a decision pursuant the Applicable law that covers the transfer of personal data to which these Clauses apply. This is without prejudice to other obligations applying to the processing in question under the Applicable law.

(...)

**Commented [A76]:** To be discussed whether this level of detail would be necessary.

**Commented [A77]:** To be discussed whether this level of detail would be necessary. From our perspective, the main safeguard would be to challenge requests that are unlawful under the legal framework of the country of the data importer.

**Commented [A78]:** What does this mean? What kind of decision would this be?

**Clause 26. Arbitration [OPTIONAL]**

(...)

[The Parties also recognized that the Data Subject has the right to bring a claim under Clauses [xxxx] and the xxx]

[Source Adapted from <https://www.wipo.int/amc/en/clauses/arbitration/index.html> ]

Source [https://www.wipo.int/amc/en/center/specific-sectors/b2b\\_data/](https://www.wipo.int/amc/en/center/specific-sectors/b2b_data/)

[OPTIONAL ICC CLAUSE]

ICC Arbitration. If the Parties are unable to resolve any Dispute pursuant Section 14.2 above and except as otherwise specified in Section 9.3(b)(i), the Dispute shall be finally settled under the Rules of Arbitration (the "Rules") of the International Chamber of Commerce ("ICC") by three (3) arbitrators designated by the Parties. Each Party shall designate one arbitrator. The third arbitrator shall be designated by the two arbitrators designated by the Parties. If either Party fails to designate an arbitrator within thirty (30) days after the filing of the Dispute with the ICC, such arbitrator shall be appointed in the manner prescribed by the Rules. An arbitration proceeding hereunder shall be conducted in London, U.K., and shall be conducted in the English language. The decision or award of the arbitrators shall be in writing and is final and binding on both Parties. The arbitration panel shall award the prevailing Party its attorneys' fees and costs, arbitration administrative fees, panel member fees and costs, and any other costs associated with the arbitration, the enforcement of any arbitration award and the costs and attorney's fees involved in obtaining specific performance of an award; provided, however, that if the claims or defenses are granted in part and rejected in part, the arbitration panel shall proportionately allocate between the Parties those arbitration expenses in accordance with the outcomes; provided, further, that the attorney's fees and costs of enforcing a specific performance arbitral award shall always be paid by the non-enforcing Party, unless the applicable action was determined to be without merit by final, non-appealable decision. The arbitration panel may only award damages as provided for under the terms of this Agreement and in no event may punitive, consequential and special damages (or as otherwise specified in this Agreement, including, without limitation, Section 10.3) be awarded. In the event of any conflict between the Rules and any provision of this Agreement, this Agreement shall govern. Sample 1 Sample 2 Sample 3 See All (10) Save Copy

**Clause 27. General Provisions**

(...)

**Annex 1  
Information about the transfer**

(...)

**Additional information:** [...]

**Commented [A79]:** It is not clear to us what the purpose is of this (the title seems to refer to B2B conflicts) and how it relates to the clause on redress (in particular whether this would somehow limit/exclude the possibility to obtain judicial redress).

**Commented [A80]:** What does this refer to? These provisions do not seem to say anything relevant to dispute resolution

**Commented [A81]:** Why?

**Commented [A82]:** In our view, this entire clause needs to be discussed in more detail. It is not clear to us what the purpose is of these provisions. We are also wondering whether all of them are appropriate in an instrument that is intended to lay down data protection safeguards.

**Commented [A83]:** Shouldn't it be specified (at least with examples) what additional information should be provided? It would e.g. be useful to indicate the (categories) of data transferred, the (categories of) data subjects covered, which (if any) sensitive data is transferred, etc.

**Annex 3**  
**Security measures**

**Commented [A84]:** Perhaps it would be good to give some examples of possible measures

*[This annex has to be completed and updated by the Data importer]*

**Annex 4**  
**LIST OF SUB-PROCESSORS**

**Commented [A85]:** This is only relevant if the data importer is a processor (which is not the case here)

*[This annex has to be completed by the Parties if they agree to pre authorize sub processors]*



# EUROPEAN UNION – EUROPEAN DATA PROTECTION SUPERVISOR (EDPS) / UNION EUROPÉENNE – CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES (CEPD)

## STANDARD CONTRACTUAL CLAUSES

Contractual clauses for transborder flows of data international transfers from controller to controller

(...)

**Commented [A86]:** C to C only then? Not entirely clear as there are some references below to C to P (clause 16).

### PART I - GENERAL CLAUSES

#### Clause 1. Purpose and scope

1.1. The aim of these standard contractual clauses is to ensure compliance with the requirements for the transfer of personal data to a Third non-state Party country under Convention 108+ (hereinafter the Convention). These contractual clauses provide an appropriate level of protection for the transfer of personal data under Article 14(2)(b) of the Convention

**Commented [A87]:** I assume 14(3)(b)?

[OPTION This Agreement sets forth the terms and conditions governing the transfer of personal data to a Third country from an entity subject to Convention 108+ (hereinafter the Convention)].

**Commented [A88]:** Actually, an entity is not subject to 108+ but it is a processing activity. We could get closer to the wording of Art 3-1 of 108+

(...)

#### Clause 2. Definitions

As used in these Clauses, the following terms shall have the following meanings:

**Applicable law:** domestic data protection law of the jurisdiction of the Data exporter.

**Commented [A89]:** Why are we targeting only the applicable law to the exporter? Importer will also be subject to an applicable law so it may be misleading.

**Biometric data:** data resulting from a specific technical processing of data concerning the physical, biological or physiological characteristics of a human person which allows the unique identification or authentication of such individuals.  
[Source: Par. 58 of Explanatory Report].

**Commented [A90]:** Is there a specific reason to define biometric data as I assume these clauses can be used for transfers not implying the processing of biometric data. So, in many cases this definition will be irrelevant and could rather be an option for the parties depending on the specificities of the processing at stake.

(...)

**Clauses:** Standard contractual clauses approved under the Convention.

**Commented [A91]:** I know that Art 14 is rather broad in the wording but would it be able to clarify what we mean by adoption here? I assume that adoption by T-PD would not equate to an adoption of clauses as envisaged in Art 14. Are we requiring the approval by national SAs?

(...)

**Data importer:** is the natural or legal person, public authority, service, agency or any other body, located in a Third non-state Party country, to which is the Recipient of a transfer of the personal data is transferred from a the Data exporter.

**Commented [A92]:** I am not certain that this definition as it conveys the message that if the data is solely made available (access to a server in Europe for instance) by the exporter, it will also qualify as a lawyer. Perhaps it does or perhaps it needs to be reflected under the definition of transborder data flow.

**Data exporter:** is the natural or legal person, [public authority, service, agency or any other body] which, alone or jointly with others, has decided to transfer personal data to a ~~Third country~~non-State Party.

**Commented [A93]:** Do we miss the link in this definition with the jurisdiction of 108+?

(...)

**Genetic data:** all data relating to the genetic characteristics of an individual which have been either inherited or acquired during early prenatal development, as they result from an analysis of a biological sample from the individual concerned including chromosomal, DNA or RNA analysis or analysis of any other element enabling equivalent information to be obtained.  
[Source: Par. 58 of Explanatory Report]

**Commented [A94]:** Same comment as for biometric data

~~Transborder flows of data~~ **International transfers of personal data:** transfer of personal data to a ~~Recipient located in a Third country~~a jurisdiction of another State or to an international organization.  
[Source: Article 14.1 of the Convention, Par. 102. of Explanatory Rep]

**Commented [A95]:** repetition

(...)

**Onward transfer:** when Personal data transferred to another ~~state~~-Party is ~~likely~~ to be further transferred to a Party located in a jurisdiction without an appropriate level of protection being ensured [OR which is not considered adequate].  
[Source: Par. 106 of Explanatory Report]

**Commented [A96]:** by the Data Importer? Do we also envisage onward sharing within the same jurisdiction of the importer?

(...)

~~Third country~~**non-state Party:** a country that has not ratified the Convention ~~or where it is not fully in force~~.

**Commented [A97]:** I think it is rather "non-party" that is used in 108+. Non-state party gives the impression that we speak about non-governmental parties (NGOs, IOs, etc). Perhaps the notion of third country was clearer for private parties that would need to sign the contract and that are less familiar with the terminology of 108+.

### Clause 3. General clauses

#### 3.1. Invariability of the Clauses

These Clauses set out appropriate safeguards, including enforceable data subject rights, obligations for data controllers and effective legal remedies, pursuant to Article 14(2)(b) of the Convention and, with respect to data transfers from controllers to controllers, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Annexes.

**Commented [A98]:** 14(3)(b)?

(...)

#### Interpretation

(...)

~~Capitalized~~ terms used but not defined in these Clauses (including the Annexes) have the meanings given to them in the agreement into which these Clauses are incorporated.

**Commented [A99]:** Do we need this while we actually do not know which agreement we are referring to?

#### Clause 4. ~~Accession~~Accession clause

T-PD(2022)1Mos

An entity that is not a Party to these Clauses may, with the agreement of the other Parties, accede to these Clauses at any time, either as a Data exporter or as a Data importer, by completing and signing the form available in Annex 2.

(...)

### Clause 5. Third Party Beneficiaries

The Parties agree and acknowledge that (a) any Data subject whose Personal data was part of an international data transfer under these Clauses shall be entitled to assert rights and remedies hereunder as a Third-party beneficiary with respect to any provisions of these Clauses affording a right, action, claim, benefit or privilege to such Data subject and (b) the jurisdiction established in Clause 25 is for the benefit of the Data Subject and the Parties shall not challenge such recognition of jurisdiction.

**Commented [A100]:** In practice, such docking clauses are often used for sub-processing situations. I.e the importer is the P of the exporter as C and contracts a sub-P. Do we want to cover these situations as well?

**Commented [A101]:** "were transferred"?

## SECTION II – RIGHTS AND OBLIGATIONS OF THE PARTIES

### Clause 6. Data protection safeguards

The Data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

(...)

### Clause 7. Purpose limitation

(...)

Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes.

[Source: Article 5(4) (b) of the Convention]

**Commented [A102]:** It is also a question of assessing the framework of the third country's applicable law and not only through the implementation of technical and organisational measures. This could be further discussed.

**Commented [A103]:** EU SCCs provide different grounds:

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B. It may only process the personal data for another purpose:

- 'where it has obtained the data subject's prior consent;
- (ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iii) where necessary in order to protect the vital interests of the data subject or of another natural person.'

### Clause 8. Transparency of processing

8.1. In order to enable Data subjects to effectively exercise their rights pursuant these Clauses, the Data importer shall inform them, either directly or through the Data exporter of:

a. his or her identity and habitual residence or establishment;

(...)

**Commented [A104]:** If we read later the article on rights of DS, we are not certain whether a request from DS is needed or not. Can we clarify here that such information should be proactively given without any need for a prior request by DS?

8.2. Paragraph 1 shall not apply where the Data subject already has the relevant information or where the processing is expressly prescribed by law binding the data subject or this notification proves to be impossible or involves disproportionate efforts.  
[Source: Article 8 of the Convention]

**Commented [A105]:** I do not understand this addition? Could it be explained or clarified?  
Plus this does not seem fully in line with Art 8(3) of 108+ limiting these cases to cases of indirect collection of data:

"Where the personal data are not collected from the data subjects, the controller shall not be required to provide such information where the processing is expressly prescribed by law or this proves to be impossible or involves disproportionate efforts".

More broadly, the wording of Art 8-3 seem very very broad. For any kind of indirect collection and if the processing is prescribed by law, would we apply these exemption from transparency obligations? That would be problematic for EU countries also bound by GDPR.

**Commented [A106]:** to be deleted?

### Clause 9. Accuracy and data minimisation

(...)

If from time to time the Data importer is informed by the Data Exporter of corrections made by Data Exporter to the Personal Data, the Data importer will promptly implement all the corrections.

(...)

### Clause 11. Data security

The Data importer and, during transmission also the Data exporter shall adopt appropriate security measures against risks such as accidental or unauthorized access to, destruction, loss, use, modification or disclosure of personal data.

**Commented [A107]:** It would be good to refer to encryption and pseudonymisation.

(...)

Each Party shall provide that the Controller notifies, without delay, at least the competent Supervisory Authority of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects.

**Commented [A108]:** Do we mean exporter plus importer?

**Commented [A109]:** Should we make the notification to SA more systematic by comparison to the notification to DS. Perhaps deleting here the word "seriously"? Also can we notify a more precise timeframe?

In case where a Data breach has occurred that may seriously interfere with the fundamental human rights and fundamental freedoms of the individual (e.g. for instance, the disclosure of data covered by professional confidentiality, sensitive data, or which may result in financial, reputational, or physical harm or humiliation) the Data importer shall notify without undue delay the Data Exporter and the relevant Supervisory Authorities of (i) the incident including a complete description of the Data Breach, and (ii) of any measures taken and/or proposed to address the breach and its potential consequences.

**Commented [A110]:** Shall the data importer notify the SA in Europe? this could be clarified.

Moreover does this parag partly overlaps with the previous one?

[Source: 65 of the Explanatory Report]

If the data breach is likely to result in a significant risk for the rights and freedoms of individuals, (such as discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage), the Data importer, and also the Data Exporter, shall notify the Data subjects involved in the Data breach and provide them with adequate and meaningful information on, notably, the contact points and possible measures that they could take to mitigate the adverse effects of the Data breach.

**Commented [A111]:** Do we need a double notification to DS? I am not sure. Moreover, we usually ask the C to notify DS.

Here we might need to better distinguish the situation depending on the controller or processor qualifications (i.e. the C notifies the SA and possibly the DS while the P notifies the C).

[Source: Paragraph 66 of the Explanatory Report]

If the Data importer does not spontaneously inform the Data subject of the Data breach, the supervisory authority, having considered the likely adverse effects of the breach, should be allowed to require the controller to do so. Notification to other relevant authorities such as those in charge of computer systems security may also be desirable.

[Source: Article 7 of the Convention & Paragraphs 62 to 66 of the Explanatory Report

## 12. Sensitive data

(...)

These safeguards may include, for instance, alone or cumulatively (i) the data subject's explicit consent for the processing of sensitive data; (ii) a professional secrecy obligation; (iii) measures following a risk analysis; (iv) a particular and qualified organizational or technical security measure (e.g. data encryption, pseudonymisation), (v) limiting the personnel permitted to access the Sensitive data, and (vi) additional restrictions with respect to further disclosure according to the nature of the data.

[Source: Article 6 of the Convention and Paragraphs 56 to 61 of the Explanatory Report]

## Clause 14. Processing under the authority of the data importer

The Data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions and in compliance with these Clauses.

## Clause 16. Use of sub-processors

[PENDING FOR MODULE 2 Transfers from controller to processor]

## Clause 17 – Rights of the Data subjects

The Data importer, if required with the assistance of the Data exporter, shall deal with any enquiries and requests it receives from a Data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.

(...)

In particular, upon request by the Data subject, the Data importer, or the Data exporter, where applicable, shall provide, free of charge, the following rights:

(...)

**Commented [A112]:** here again is it the exporter or importer?

**Commented [A113]:** Which SA? Does the European SA have jurisdiction over the importer?

**Commented [A114]:** Could you please clarify further which authorities you have mind?

**Commented [A115]:** This clause seems a bit abstract to me. Could we rather impose to the importer to precisely describe these additional safeguards tailored to the processing at stake - in a specific annex. To facilitate the review of the exporter?

**Commented [A116]:** I would delete. It gives the impression that an "external processor" to the importer would be covered by this clause. I assume we rather target mainly the persons working as employee or under the direct instruction of the data importer?

**Commented [A117]:** Do you mean a C/P module will be integrated later on? Do you also envisage a model P to sub-P?

**Commented [A118]:** typo: "deal"

**Commented [A119]:** for indent A) F) and G), no need for a prior request - to be deleted?

b) to obtain, on request, at reasonable intervals and without excessive delay, confirmation of the processing of Personal data relating to him or her, the communication in an intelligible form of the data processed and transfer, all available information on their origin, on the preservation period as well as any other information that the controller is required to provide in order to ensure the transparency of processing in accordance with these Clauses;

**Commented [A120]:** can we be more practical and envisage the right to obtain a copy of the data?

(...)

f) to have a remedy under these Clauses where his or her rights under this Agreement, the Convention and/or the Applicable law have been violated;

**Commented [A121]:** Do we need this here? contractual clauses will never create as such the legal remedy in the third country or the supervisory authority if there is no SA in the third country? Perhaps better to distinguish the rights of DS in this clause and to have a separate clause on redress and supervision?

g) to benefit, whatever his or her nationality or residence, from the assistance of a Supervisory authority within the meaning of these Clauses, in exercising his or her rights under these Clauses.

(...)

#### Clause 18. Redress for the data subject

The Data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints. It shall deal promptly with any complaints it receives from a Data subject.

**Commented [A122]:** we also need redress towards the exporter no??

(...)

#### Clause 19. Liability.

(...)

Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under the Applicable law.

**Commented [A123]:** It is not only breaching the rights if DS but all the clauses, no? For instance on security.

#### Clause 20. Supervisory authority

(...)

The Parties hereby consent that the supervisory authority is entitled to request that the person who transfers data demonstrates the effectiveness of the safeguards or the existence of prevailing legitimate interests and that the supervisory authority may, in order to protect the rights and fundamental freedoms of data subjects, prohibit such transfers, suspend them or subject them to conditions.

**Commented [A124]:** the exporter? both parties?

[Source: article 14.6 of the Convention]

The Parties agree to submit to the jurisdiction of the Supervisory authorities and not to question its powers, its jurisdiction, or any other action including any forms of co-operation between supervisory authorities as provided by the Applicable law and article 15 and 17 of the Convention.

**Commented [A125]:** I understand the objective but I am not sure to understand the consequences of such sentence. For instance, an European SA would not be able to impose a fine on an importer in the third country solely on the basis of these clauses. The hook is rather indeed on the elements mentioned in the paragraph after (possibility to request information, to perform audits, etc). Might be further discussed.

[Source: article 15 and 17 of the Convention]

(...)

### SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

#### Clause 21. Local laws and practices affecting compliance with the Clauses

(...)

The Parties declare that in providing the warranty stated in the previous paragraph, they have taken due account in particular of the following elements:

(...)

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(...)

### SECTION IV – FINAL PROVISIONS

#### Clause 23. Non-compliance with the Clauses and termination

The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(...)

#### Clause 26. Arbitration [OPTIONAL]

(...)

#### Clause 27. General Provisions

(...)

#### Annex 1 Information about the transfer

(...)

**Commented [A126]:**  
It would be important to include the limitation that we have in the EU SCCs (in the footnote 12):

'As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.'

**Commented [A127]:** Pb in the numbering There is no a)

**Commented [A128]:** There is also a reference to ADR in clause 18. Should

we rather merge all these elements in a single clause?

**Commented [A129]:** Not sure we actually need such clauses. The objective of data protection clauses is to provide safeguards in relation to the processing of personal data but not to cover all aspects of contractual law. This is often done in another context and may depend on different factors. Perhaps better to remain silent on these general contractual clauses?

**Commented [A130]:** Annexes are absolutely key in SCCs. They need to be as specific and complete as possible. We would strongly encourage to add more details on Annexes 1 and 3. Perhaps annexes of the EU transfers SCCs could serve as a source of inspiration here.

## FINLAND / FINLANDE

### PART I - GENERAL CLAUSES

(...)

#### Clause 2. Definitions

(...)

**Transborder flows of data of personal data:** transfer of personal data to ~~a~~the ~~a~~-jurisdiction of another State or to an international organization.

[Source: Article 14.1 of the Convention, Par. 102. of Explanatory Rep]

(...)

**Onward transfer:** when Personal data transferred to another state-Party is to be further transferred to a Party located in a jurisdiction without an appropriate level of protection being ensured [OR which is not considered adequate].

[Source: Par. 106 of Explanatory Report]

(...)

**Supervisory authority/ies:** One or more authorities responsible for ensuring compliance with the provisions of the Convention and the Applicable law.

[Source: Article 15 of the Convention]

(...)

### SECTION II – RIGHTS AND OBLIGATIONS OF THE PARTIES

(...)

#### Clause 13. Onward transfers

The Data importer shall not disclose the personal data to a third party located in a non-state Party unless the third party is or agrees to be bound by these Clauses.

(...)

**Commented [A131]:** Does this mean "data importer"/ non-state Party?

**Commented [A132]:** Why would the definition of "onward transfer" only cover those cases where an appropriate level of protection is not ensured?  
(It is a requirement imposed by the Convention that in the case of onward transfers, an appropriate level of protection is ensured.)  
For consideration: Should this definition rather refer to further transfers to any non-state Party? (See draft clause 13 below.)

**Commented [A133]:** Rather: with "these clauses"? (See draft clause 15 below.)

**Commented [A134]:** See the comment above on the definition of onward transfers.



**Clause 15. Documentation and compliance**

(...)

The Data importer shall take all appropriate measures to comply with the obligations of these Clauses and be able to demonstrate, to the competent Supervisory authority mentioned in Clause 20, that the data processing under these Clauses is in compliance with the provisions of the Convention and the Applicable law.

**Commented [A135]:** See the comment above on the definition of supervisory authority.

(...)

**Clause 16. Use of sub-processors**

[PENDING FOR MODULE 2 Transfers from controller to processor]

**Clause 17 – Rights of the Data subjects**

The Data importer, if required with the assistance of the Data exporter, shall deal with any enquiries and requests it receives from a Data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.

(...)

**SECTION IV – FINAL PROVISIONS**

(...)

**Clause 26. Arbitration [OPTIONAL]**

[WIPO CLAUSE]  
Arbitration clause for B2B conflicts

**Commented [A136]:** It would be useful if we could get explanation for the inclusion of the optional WIPO and ICC clauses, and what their relation is with the draft data protection clauses, to be able to assess them.

(...)

## FORMER CHAIR OF THE COMMITTEE / ANCIEN PRÉSIDENT DU COMITÉ

### SECTION I – CLAUSES GÉNÉRALES

(...)

#### Clause 2. Définitions

Dans les présentes Clauses, les termes ci-après doivent être entendus comme suit :

**Droit applicable** : droit ~~interne~~ relatif à la protection des données, ~~en vigueur dans le pays ou territoire – s'appliquant aux traitements de données relevant de la juridiction à laquelle de l'exportateur des données est soumis.~~

**Commented [A137]**: alignement sur l'article 3.1 Convention 108+

(...)

**Importateur de données** : la personne physique ou morale [l'autorité publique, le service, l'agence ou tout autre organisme], située dans un État tiers ou une organisation internationale, à qui l'exportateur des données transfère les données à caractère personnel.

**Exportateur de données** : la personne physique ou morale [l'autorité publique, le service, l'agence ou tout autre organisme], qui décide de transférer, seule ou conjointement avec d'autres, des données à caractère personnel vers un État tiers ou une organisation internationale.

(...)

**Violation des données** : tout accès non autorisé à des données à caractère personnel, leur destruction, perte, utilisation, modification ou divulgation résultant d'une violation du principe de la sécurité des données et ayant entraîné la copie illicite et non autorisée de données ~~sensibles, protégées ou confidentielles~~, leur transmission, consultation, vol ou utilisation par une personne physique ou morale non autorisée à le faire.

**Commented [A138]**: pourquoi se limiter à des données sensibles

[Source : article 7 de la Convention]

(...)

**Flux transfrontières de données à caractère personnel** : transfert de données à caractère personnel vers un destinataire relevant de la juridiction d'un autre État ou d'une autre organisation internationale. Est également un flux transfrontière l'accès autorisé aux données par une personne physique ou morale, une autorité publique .. relevant de la juridiction d'un autre Etat ou d'une organisation internationale que celle de l'exportateur des données.

[Source : article 14.1 de la Convention et paragraphe 102 du rapport explicatif.]

~~OPTION : [].~~

[Source : ort]

**Commented [A139]:** option entre quoi et quoi, pas clair

**Transfert ultérieur :** des données à caractère personnel qui ont été transférées à un autre État partie sont susceptibles d'être de nouveau transférées à une Partie ~~située dans un pays ou territoire~~ où le niveau de protection assuré n'est pas approprié ~~[OU n'est pas considéré comme étant adéquat].~~

[Source : paragraphe 106 du rapport explicatif]

**Commented [A140]:** une Partie à la Convention est soit un Etat ou organisation internationale.

(...)

**Autorité(s) de contrôle :** une ou plusieurs autorités chargées de veiller au respect des dispositions de la Convention et du Droit applicable.

[Source : article 15 de la Convention]

~~État tiers : pays qui n'a pas ratifié la Convention ou dans lequel celle-ci n'est pas pleinement en vigueur.~~

~~Tiers bénéficiaire : la Personne concernée, dont les Données à caractère personnel font l'objet d'un ou de plusieurs flux transfrontières de données.~~

**Commented [A141]:** la Convention 108+ vise non seulement des Etats mais aussi des organisations internationales. Si veut maintenir une telle définition, il faut la revoir

**Commented [A142]:** Quel serait la valeur ajoutée d'une telle définition ?

## SECTION II – DROITS ET OBLIGATIONS DES PARTIES

### Clause 7. Limitation de la finalité

L'Importateur de données traite les données à caractère personnel uniquement pour la ou les finalités spécifiques du transfert, conformément à l'annexe 1.

~~Le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins de statistiques est compatible avec ces finalités à condition que des garanties complémentaires s'appliquent.~~

[Source : article 5.4.b de la Convention]

**Commented [A143]:** pas favorable à prévoir d'emblée une telle possibilité lors de flux transfrontières de données

### Clause 8. Transparence du traitement

(...)

8.2. Le paragraphe 1 ne s'applique pas lorsque la Personne concernée dispose déjà de ces informations (ou lorsque le traitement est expressément prévu par un texte législatif opposable à ladite personne concernée), ou lorsque cette notification s'avère impossible ou exige des efforts démesurés.

[Source : article 8 de la Convention]

**Commented [A144]:** est-ce vraiment le cas ou est-ce hypothétique ?

### Clause 11. Sécurité des données

(...)

Les Parties au contrat sont convenues des mesures d'ordre technique et organisationnel énoncées à l'annexe 3. L'Importateur de données vérifie régulièrement que ces mesures continuent d'offrir le niveau de sécurité approprié.

En cas de modification substantielle des mesures de sécurité adoptées et décrites dans l'annexe 3, les Parties au contrat doivent actualiser l'annexe.

En cas de violation de données susceptible de porter gravement atteinte aux droits de l'homme et aux libertés fondamentales d'une personne physique (par exemple divulgation de données protégées par le secret professionnel ou de données sensibles, ou divulgation pouvant causer un préjudice financier, porter atteinte à la réputation, à l'intégrité physique ou entraîner une humiliation), l'Importateur de données est tenu de notifier dans un délai raisonnable, à l'Exportateur de données et aux Autorités de contrôle compétentes, i) l'incident, en décrivant la violation de données de façon exhaustive, et ii) toute mesure prise et/ou proposée pour remédier à la violation et pallier les conséquences potentielles

En cas de violation de données susceptible de porter gravement atteinte aux droits et aux libertés fondamentales des personnes concernées, chaque Partie au contrat prévoit que le Responsable du traitement est tenu de notifier l'incident à l'Autorité de contrôle compétente dans les meilleurs délais, ce qui est l'exigence minimale.

**Commented [A145]:** de quel responsable parle-t-on, l'exportateur ou l'importateur ? S'il s'agit de l'exportateur encore faut-il qu'il est connaissance de la violation. Il est dès lors plus logique de commencer par le principe sur l'obligation d'informer de l'importateur

~~En cas de violation de données susceptible de porter gravement atteinte aux droits de l'homme et aux libertés fondamentales d'une personne physique (par exemple divulgation de données protégées par le secret professionnel ou de données sensibles, ou divulgation pouvant causer un préjudice financier, porter atteinte à la réputation, à l'intégrité physique ou entraîner une humiliation), l'Importateur de données est tenu de notifier dans un délai raisonnable, à l'Exportateur de données et aux Autorités de contrôle compétentes, i) l'incident, en décrivant la violation de données de façon exhaustive, et ii) toute mesure prise et/ou proposée pour remédier à la violation et pallier les conséquences potentielles.~~

[Source : paragraphe 65 du rapport explicatif]

(...)

#### **Clause 12. Données sensibles**

Lorsque des Données sensibles sont transférées, l'Importateur de données applique des restrictions spécifiques et des garanties supplémentaires adaptées aux risques courus ainsi qu'aux intérêts, aux droits et aux libertés à protéger.

**Commented [A146]:** A quelles restrictions fait-on allusion ?

(...)

T-PD(2022)1Mos

#### **Clause 15. Documentation et conformité**

Chaque Partie au contrat est en mesure de démontrer qu'elle a respecté les obligations lui incombant au titre des présentes Clauses.

(...)

#### **Clause 19. Responsabilité**

Chaque Partie au contrat est responsable devant l'autre ou les autres Parties de tout dommage qu'elle cause à cette/ces dernière(s) du fait de la violation des présentes Clauses.

Chaque Partie au contrat est responsable devant la personne concernée, qui peut prétendre à une réparation, de tout dommage matériel ou moral qu'elle occasionne à la Personne concernée en enfreignant les droits que les présentes Clauses octroient à cette dernière en tant que tiers bénéficiaire. La présente disposition est sans préjudice de la responsabilité de l'exportateur de données en vertu du Droit applicable.

Lorsque plusieurs Parties au contrat sont responsables de tout dommage occasionné à la personne concernée et résultant d'une violation des présentes Clauses, toutes les Parties au contrat sont responsables conjointement et solidairement et la personne concernée est fondée à saisir la justice contre l'une quelconque desdites Parties.

Les Parties au contrat conviennent que si l'une des Parties est tenue responsable en application du précédent paragraphe, elle est en droit de réclamer à l'autre/aux autres Partie(s) la part de la réparation correspondant à sa/leur part de responsabilité dans le dommage.

(...)

#### **Clause 20. Autorité de contrôle**

(...)

Les Parties au contrat consentent par les présentes à ce que l'autorité de contrôle puisse exiger de la personne qui transfère les données qu'elle démontre l'effectivité des garanties prises ou l'existence d'intérêts légitimes prépondérants et qu'elle puisse, pour protéger les droits et les libertés fondamentales des personnes concernées, interdire ou suspendre les transferts ou soumettre à condition de tels transferts de données.

[Source : article 14.6 de la Convention]

Les Parties au contrat s'engagent à reconnaître la compétence de l'Autorité de contrôle et à ne contester ni son autorité, ni sa compétence, ni aucune autre action, en ce compris toute forme de

coopération entre autorités de contrôle conformément au Droit applicable et aux articles 15 et 17 de la Convention.

(...)

### SECTION III – LÉGISLATIONS LOCALES ET OBLIGATIONS EN CAS D'ACCÈS DES AUTORITÉS PUBLIQUES

#### Clause 21. Législations et pratiques locales ayant une incidence sur le respect des Clauses

Les Parties au contrat garantissent qu'elles n'ont aucun motif de croire que la législation et les pratiques applicables, dans un État tiers de destination, au traitement, par l'Importateur de données, des données à caractère personnel, notamment toute obligation de divulguer des données à caractère personnel ou toute mesure d'autorisation d'accès des autorités publiques, empêchent l'importateur de données de remplir les obligations qui lui incombent au titre des présentes Clauses et de la Convention.

La présente disposition repose sur l'idée que dès lors que des exceptions spécifiques aux présentes Clauses qui sont prévues par le ou les droits applicables, respectent l'essence des droits de l'homme et des libertés fondamentales et n'excèdent pas ce qui est nécessaire et proportionné dans une société démocratique pour préserver l'un des objectifs énumérés à l'article 11 de la Convention, elles ne méconnaissent pas les présentes Clauses.

**Commented [A147]:** revoir la rédaction de cette disposition. Ce n'est pas claire

Les Parties au contrat déclarent qu'en offrant la garantie énoncée au précédent paragraphe, elles tiennent dûment compte en particulier des éléments suivants :

(...)

- b) les législations et pratiques ~~de l'Etat ou de l'organisation internationale destinataire du transfert de données du pays tiers de destination~~ – notamment celles qui exigent la divulgation de données aux autorités publiques ou autorisent l'accès de ces dernières aux données – qui sont appropriées au regard des circonstances spécifiques du transfert ainsi que des limitations et des garanties applicables ;

(...)

## GERMANY / ALLEMAGNE

### COUNCIL OF EUROPE CONVENTION 108+ STANDARD CONTRACTUAL CLAUSES

#### PART I - GENERAL CLAUSES

##### Clause 1. Purpose and scope

1.1. The aim of these standard contractual clauses is to ensure compliance with the requirements for the transfer of personal data to a non-state Party under Convention 108+ (hereinafter the Convention). These contractual clauses provide an appropriate level of protection for the transfer of personal data under Article 14(2)(b) of the Convention

(...)

##### Clause 2. Definitions

(...)

**non-state Party:** a country that has not ratified the Convention or where it is not fully in force.

(...)

##### Clause 3. General clauses

###### 3.1. Invariability of the Clauses

These Clauses set out appropriate safeguards, including enforceable data subject rights, obligations for data controllers and effective legal remedies, pursuant to Article 14(2)(b) of the Convention and, with respect to data transfers from controllers to controllers, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Annexes.

(...)

##### Clause 4. Accession clause

An entity that is not a Party to these Clauses may, with the agreement of the other Parties, accede to these Clauses at any time, either as a Data exporter or as a Data importer, by completing and signing the form available in Annex 2.

(...)

### Annex 1 Information about the transfer

**Commented [A148]:** General remarks:  
-Germany has not yet concluded an in depth analysis.

-It would be helpful to include an introductory text or guidelines on the use of the proposed SCC.

-Article 23 (g) foresees that the Convention Committee once Convention 108+ has entered into force can develop or approve models of standardised safeguards referred to in Article 14. Convention 108 does not foresee this for its Consultative Committee. It would be helpful to clarify the procedural steps to be taken and the legal quality of this document.

**Commented [A149]:** State might be misleading as it could also be an International Organisation.  
Alternatively: "to a recipient who is subject to the jurisdiction of a State or international organisation which is not Party to the Convention"  
Non-state Party might also be misunderstood as only meaning Parties who are "non-state". Possible alternative: "Non-Party"

**Commented [A150]:** It could be considered to only define those terms that are not already defined by the Convention or the ER.

**Commented [A151]:** See above

**Commented [A152]:** The SCC rarely refer to them: Is it planned to add them later on?

**Commented [A153]:** The description of the data processing would also need to be updated.

**Commented [A154]:** Similar to the EU SCC the annexes could be more detailed.

## INTERNATIONAL COMMITTEE OF THE RED CROSS (ICRC) / COMITÉ INTERNATIONAL DE LA CROIX ROUGE (CICR)

### PART I - GENERAL CLAUSES

#### Clause 1. Purpose and scope

1.1. The aim of these standard contractual clauses is to ensure compliance with the requirements for the transfer of personal data to a ~~Third non-state Party or an international organisation country~~ under Convention 108+ (hereinafter the Convention). ~~These contractual clauses provide an appropriate level of protection for the transfer of personal data under Article 14(2)(b) of the Convention~~

(...)

#### Clause 2. Definitions

(...)

**Data importer:** is the natural or legal person, [public authority, service, agency or any other body], located in a ~~Third non-state Party, or is an international organisation country, to which is the Recipient of a transfer of the~~ personal data is transferred from ~~a the~~ Data exporter.

(...)

#### Clause 3. General clauses

##### 3.1. Invariability of the Clauses

(...)

##### Interpretation

(...).

These Clauses shall be read and interpreted in the light of the provisions of the Convention and the Applicable law.

(...)

**Commented [A155]: ICRC DPC:** international organisations only apply their internal rules and regulations when processing personal data, and not the domestic law of the country where they are based/operate.

This fact should be made explicit throughout these clauses, to avoid any misunderstanding.



### Clause 5. Third Party Beneficiaries

The Parties agrees and acknowledge that (a) any Data subject whose Personal data was part of an international data transfer under these Clauses shall be entitled to assert rights and remedies hereunder as a Third-party beneficiary with respect to any provisions of these Clauses affording a right, action, claim, benefit or privilege to such Data subject and (b) the jurisdiction established in Clause 25 is for the benefit of the Data Subject and the Parties shall not challenge such recognition of jurisdiction.

Commented [A156]: ICRC DPG: See comment to clause 25

## SECTION II – RIGHTS AND OBLIGATIONS OF THE PARTIES

(...)

### Clause 7. Purpose limitation

(...)

Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes.

[Source: Article 5(4) (b) of the Convention]

Commented [A157]: ICRC DPG: What does this mean concretely? What appropriate safeguards does this refer to specifically?  
We suggest having them spelled out in these clauses.

### Clause 10. Storage limitation

The Data importer shall retain the Personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organizational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

Commented [A158]: ICRC DPG: Some personal data received by international organisations might need to be archived in accordance with internal rules and procedures – often archived data cannot be deleted, nor anonymised.

We suggest reflecting this element explicitly in these clauses.

### Clause 11. Data security

(...)

Each Party shall provide that the Controller notifies, without delay, at least the competent Supervisory Authority of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects.

Commented [A159]: ICRC DPG: International organisations only process personal data in accordance with their own internal rules, which generally do not require notification to a national supervisory authority.

In case where a Data breach has occurred that may seriously interfere with the fundamental human rights and fundamental freedoms of the individual (e.g. for instance, the disclosure of data covered by professional confidentiality, sensitive data, or which may result in financial, reputational, or physical harm or humiliation) the Data importer shall notify without undue delay the Data Exporter and the relevant Supervisory Authorities of (i) the incident including a complete description of the Data Breach, and (ii) of any measures taken and/or proposed to address the breach and its potential consequences.

Commented [A160]: ICRC DPG: Same as above

(...)

If the Data importer does not spontaneously inform the Data subject of the Data breach, the supervisory authority, having considered the likely adverse effects of the breach, should be allowed to require the controller to do so. Notification to other relevant authorities such as those in charge of computer systems security may also be desirable.

(...)

**Commented [A161]:** **ICRC DPG:** By virtue of applicable privileges and immunities, as well as the fact that some domestic laws explicitly do not apply to international organisations, national supervisory authorities do not impose obligations on international organisations.

### Clause 13. Onward transfers

The Data importer shall not disclose the personal data to a third party located in a **Third country/non-state Party** unless the third party is or agrees to be bound by these Clauses.

An Onward transfer by the Data importer may only take place only if:

(...)

(iv) it is necessary in order to protect the **vital** interests of the Data subject or of another natural person; or

(...)

**Commented [A162]:** **ICRC DPG:** Onward sharing might be fundamental to ensure the effective performance of the mandate of international organisations (e.g. in the humanitarian sector) – subjecting these transfers to the conclusion of these Clauses with a third party might not be possible in all situations, and could constitute an excessive interference with the neutrality and independence of the international organisation, effectively preventing it from performing its mandate.

**Commented [A163]:** **ICRC DPG:** Important reasons of public interest, such as those related to the effective performance of the mandate of international organisations under international law, should also be included – most onward transfers by international (humanitarian) organisations would be based upon important reasons of public interests.

### Clause 15. Documentation and compliance

(...)

The Data importer shall take all appropriate measures to comply with the obligations of these Clauses and be able to demonstrate, to the competent Supervisory authority mentioned in Clause 20, that the data processing under these Clauses is in compliance with the provisions of the Convention and the Applicable law.

(...)

**Commented [A164]:** **ICRC DPG:** See comment to clause 20 – the processing of personal data by international organisation is governed by its internal rules exclusively, not by the domestic law of the country where the international organisation operates.

### Clause 17 – Rights of the Data subjects

(...)

In particular, upon request by the Data subject, the Data importer, or the Data exporter, where applicable, shall provide, free of charge, the following rights:

(...)

g) to benefit, whatever his or her nationality or residence, from the assistance of a Supervisory authority within the meaning of these Clauses, in exercising his or her rights under these Clauses.

(...)

**Commented [A165]:** **ICRC DPG:** An international organisation will only provide for the rights (and limitations thereof) contained in its internal data protection framework.

**Commented [A166]:** **ICRC DPG:** Linked to the comment above, an international organisation will only offer the possibility for the data subject to have their complaint handled by the "supervisory authority" enshrined in the IO's internal rules, and not the national supervisory authority of the jurisdiction of the data exporter.

**Clause 18. Redress for the data subject**

(...)

The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

The alternative mentioned in the paragraph above does not exclude the right of the Data subject afforded by these Clauses, the Convention and the Applicable law to bring a claim at the Supervisory Authority or at the courts of the applicable jurisdiction.

**Commented [A167]:** **ICRC DPQ:** Not applicable to international organisations. Settlement of data subject complaints will only be offered by international organisations through their own internal rules and mechanisms.

**Clause 19. Liability.**

(...)

Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

**Commented [A168]:** **ICRC DPQ:** by virtue of applicable privileges and immunities, an international organisation is not subject to the jurisdiction of domestic courts unless the IO has expressly waived such immunity (a decision that the international organisation makes independently, based on the circumstances of each situation)

(...)

**Clause 20. Supervisory authority**

(...)

**Commented [A169]:** **ICRC DPQ:** An international organisation, by virtue of applicable privileges and immunities, will not submit itself to the jurisdiction of a national supervisory authority.

**SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

The effective application of the rules on data protection applicable to an international organisation is only monitored by the mechanisms set out in those same rules, and not by domestic authorities under national law.

**Clause 21. Local laws and practices affecting compliance with the Clauses**

(...)

The Parties declare that in providing the warranty stated in the previous paragraph, they have taken due account in particular of the following elements:

**Commented [A170]:** **ICRC DPQ:** we suggest adding, amongst the listed elements, "any applicable privileges and immunities enjoyed by the data importer under national or international law"

(...)

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

**Commented [A171]:** **ICRC DPQ:** Same comment as above regarding national supervisory authorities

(...)

**Clause 22. Obligations of the data importer in case of access by public authorities**

**Notification**

(a) The Data importer agrees to notify the Data exporter and, where applicable, the data subject promptly (if necessary with the help of the data exporter) if it:

(...)

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

**Commented [A172]:** **ICRC DPG:** Same comment as above regarding national supervisory authorities

(...)

## SECTION IV – FINAL PROVISIONS

### Clause 23. Non-compliance with the Clauses and termination

The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(...)

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

**Commented [A173]:** **ICRC DPG:** same comments as above regarding domestic courts and supervisory authorities

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

**Commented [A174]:** **ICRC DPG:** Same comment as above

(...)

### Clause 25. Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of [\_\_\_\_]. The Parties agree that those shall be the courts of [\_\_\_\_].

A Data subject may also bring legal proceedings against the Data exporter and/or Data importer before the courts of the country in which he/she has his/her habitual residence. The Parties agree to submit themselves to the jurisdiction of such courts.

**Commented [A175]:** **ICRC DPG:** An international organisation will not agree to be by default subject to the jurisdiction of domestic courts, in light of their status and applicable privileges and immunities. A waiver of the international organization's immunity from jurisdiction is decided independently by the international organisation, based on the circumstances of each situation.

### Clause 27. General Provisions

(...)

Settlement of disputes is usually guaranteed via arbitration exclusively.

**Commented [A176]:** **ICRC DPG:** In case the importer is an international organisation, a clause should be included specifying that nothing in this Agreement shall be interpreted as a partial or full waiver of the privileges and immunities enjoyed by the international organisation under national or international law

## ITALY / ITALIE

### STANDARD CONTRACTUAL CLAUSES

Contractual clauses for ~~transborder flows of personal data international transfers~~ from controller to controller

(...)

#### PART I - GENERAL CLAUSES

(...)

##### Clause 2. Definitions

(...)

**Data exporter:** is the natural or legal person, [public authority, service, agency or any other body] which, alone or jointly with others, has decided to transfer personal data to an importer located in a Third country/non-State Party.

(...)

**Data breach:** Any ~~non-authorized~~ non-authorized access to, destruction, loss, use, modification or disclosure ~~access or disclosure~~ of Personal Data due to a violation of the principle of data security, in which sensitive, protected data or confidential data is copied, transmitted, viewed, stolen or used by an individual or entity unauthorized to do so.

**Commented [A177]:** IT: Article 7 of 108+ refers to 'accidental or unauthorised access [...]'

[Source: Article 7 of the Convention]

(...)

**Genetic data:** all data relating to the genetic characteristics of an individual which have been either inherited or acquired during early prenatal development, as they result from an analysis of a biological sample from the individual concerned including chromosomal, DNA or RNA analysis or analysis of any other element enabling equivalent information to be obtained.

[Source: Par. 57~~8~~ of Explanatory Report]

(...)

**Onward transfer:** when Personal data transferred to another state-Party is likely to be further transferred to a Party located in a jurisdiction without an appropriate level of protection being ensured [OR which is not considered adequate].

[Source: Par. 106 of Explanatory Report]

**Commented [A178]:** IT: appropriate

(...)

~~Sensitive-Special categories of data~~: personal data that is (i) related to Genetic data, or (ii) relating to offences, criminal proceedings and convictions, or related security measures; or (iii) Biometric data uniquely identifying a person; or (iv) revealing data relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life.  
[Source: Article 6 of the Convention]

(...)

#### Clause 5. Third Party Beneficiaries

The Parties ~~agrees~~agree and acknowledge that (a) any Data subject whose Personal data was part of an international data transfer under these Clauses shall be entitled to assert rights and remedies hereunder as a Third-party beneficiary with respect to any provisions of these Clauses affording a right, action, claim, benefit or privilege to such Data subject and (b) the jurisdiction established in Clause 25 is for the benefit of the Data Subject and the Parties shall not challenge such recognition of jurisdiction.

## SECTION II – RIGHTS AND OBLIGATIONS OF THE PARTIES

#### Clause 6. Data protection safeguards

(...)

The Data exporter represents ~~that it has the right to transfer the personal data to the Data importer~~ ~~importer in~~ accordance with this Agreement and the Applicable law.

Commented [A179]: IT: not sure it is clear

#### Clause 8. Transparency of processing

8.1. In order to enable Data subjects to effectively exercise their rights pursuant these Clauses, the Data importer shall inform them, either directly or through the Data exporter of:

(...)

f. ~~of~~ the right to obtain a copy of these Clauses;

8.2. Paragraph 1 shall not apply where the Data subject already has the relevant information or where the processing is expressly prescribed by law ~~binding the data subject~~ or this notification proves to be impossible or involves disproportionate efforts.  
[Source: Article 8 of the Convention]

Commented [A180]: IT: Not sure it is clear

#### Clause 9. Accuracy and data minimisation

(...)

If ~~from time to time~~ the Data importer is informed by the Data Exporter of corrections made by Data Exporter to the Personal Data, the Data importer will promptly implement all the corrections.

Commented [A181]: IT: what do we mean?

(...)

### Clause 11. Data security

(...)

If the data breach is likely to result in a significant risk for the rights and freedoms of individuals, (such as discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage), the Data importer, and also the Data Exporter, shall notify the Data subjects involved in the Data breach and provide them with adequate and meaningful information on, notably, the contact points and possible measures that they could take to mitigate the adverse effects of the Data breach.

**Commented [A182]:** IT: at EU level SCC and BCR referential also provide that the data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

(...)

If the Data importer does not spontaneously inform the Data subject of the Data breach, the supervisory authority, having considered the likely adverse effects of the breach, should be allowed to require the controller to do so. Notification to other relevant authorities such as those in charge of computer systems security may also be desirable.

**Commented [A183]:** IT: importer controller or exporter?

**Commented [A184]:** IT: not sufficiently technical

(...)

### Clause 12. Sensitive data

(...)

Such safeguards must guard against the risks that the processing of sensitive special categories of data may present for the interests, rights and fundamental freedoms of the data subject (notably a risk of discrimination).

These safeguards may include, for instance, alone or cumulatively (i) the data subject's explicit consent for the processing of sensitive data; (ii) a professional secrecy obligation; (iii) measures following a risk analysis; (iv) a particular and qualified organizational or technical security measure (e.g. data encryption, pseudonymisation), (v) limiting the personnel permitted to access the Sensitive special category of data, and (vi) additional restrictions with respect to further disclosure according to the nature of the data.

(...)

### Clause 15. Documentation and compliance

(...)

In particular, the Data importer-exporter shall keep appropriate documentation of the processing activities carried out under its responsibility.

The Data importer-exporter shall make such documentation available to the competent Supervisory authority on request.

**Commented [A185]:** IT: isn't this kind of obligations normally on the importer considering that the exporter is bound before the Supervisory authority ?

(...)

### Clause 17 – Rights of the Data subjects

The Data importer, if required with the assistance of the Data exporter, shall ~~deal~~deal with any enquiries and requests it receives from a Data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.

(...)

In particular, upon request by the Data subject, the Data importer, or the Data exporter, where applicable, shall provide, free of charge, the following rights:

- a) not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration;

(...)

### Clause 18. Redress for the data subject

(...)

The alternative mentioned in the paragraph above does not exclude the right of the Data subject afforded by these Clauses, the Convention and the Applicable law to bring a claim at the Supervisory Authority or at the courts of the applicable jurisdiction.

### Clause 20. Supervisory authority

(...)

The Parties hereby consent that the supervisory authority is entitled to request that the person who transfers data demonstrates the effectiveness of the safeguards or the existence of prevailing legitimate interests and that the supervisory authority may, in order to protect the rights and fundamental freedoms of data subjects, prohibit such transfers, suspend them or subject them to conditions.

[Source: article 14.6 of the Convention]

(...)

**Commented [A186]:** IT: Do we need to put in the contract considering that the exporter has already these obligations?

**Commented [A187]:** IT: should we add that the data importer shall abide by a decision that is binding under the applicable law?

**Commented [A188]:** IT ?



**SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

(...)

**Clause 22. Obligations of the data importer in case of access by public authorities**

**Notification**

(a) The Data importer agrees to notify the Data exporter and, where possibleapplicable, the data subject promptly (if necessary with the help of the data exporter) if:  
(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(...)

**Commented [A189]:** IT: "possible" may be more appropriate than "applicable" here

## SWEDEN / SUÈDE

(...)

### PART I - GENERAL CLAUSES

#### Clause 2. Definitions

(...)

**Third country non-state Party:** a country that has not ratified the Convention or where it is not fully in force.

(...)

**Commented [A190]:** SE comment:  
Is this in accordance with article 14?

## TURKEY / TURQUIE

(...)

### SECTION II – RIGHTS AND OBLIGATIONS OF THE PARTIES

(...)

#### Clause 12. Sensitive data

(...)

**Commented [A191]:** Data exporter's data protection authority may determine additional safeguards for processing sensitive data. In such circumstances, it is also important for data importer to apply those safeguards

## UNITED KINGDOM / ROYAUME-UNI

Council of Europe Data Protection committee  
Standard Contractual Clause - draft template  
Feb 2022 v1

### UK draft interventions, by suggested clause:

- In general, the UK suggests it may be worth ensuring consistency around capitalisation - as capitalised words can be used to denote defined terms in other agreements.

### Clause 3

- **Under Interpretation, paragraph 4 (Clause differs from IDTA in that CoE seeks primacy for its SCC ie in the event of a conflict between agreements on data protection standards)**
- (“**In the event of a contradiction...**”: there are occasions where it is desirable for other related agreements to prevail over an SCC agreement - e.g. where they provide greater protection for Data Subjects.
- We therefore recommend adding an exception, e.g. : *“The exception to this is where the conflicting terms of the related agreements provide greater protection for the Data Subject’s rights, in which case those terms will override these Clauses”*.

### Clause 17, Rights of the Data Subject

- **On paragraph 3, which lays out what the Importer/Exporter must provide to the Subject:** information provision (e.g. on the information processed, as in point (b)), may, under circumstances, have a cost - which is not captured in the CoE template. We therefore suggest the text reads *“shall provide, at no greater cost to the Relevant Data Subject than it would be able to charge if it were subject to local domestic legislation, the following rights:”*.
- **On point (h), for Data Subjects to be provided a contact person in both Parties:** The UK recommends that this may place a significant burden on businesses (for example, barriers around shared language with the Data Subject). Given the high level of safeguarding and information already provided to the individual in these Clauses, the UK suggests this point is removed.
- The UK notes that there are no exemptions granted to businesses in responding to requests, other than that requests be “at reasonable intervals”. This may cause excessive burden if, for example, an individual makes excessive or repetitive requests. We would suggest adding exemptions, for example that *“The Importer is not required to respond to requests if (a) it is unable to reasonably verify the identity of an individual making the request”, or (b) the requests are unfounded, excessive or repetitive. In this case, the Importer may refuse the request or may charge the Relevant Data Subject a reasonable fee, or (c) a relevant exemption would be available under the domestic laws of the Exporter”*.

**Clause 18, Redress for the Data Subject**

- On the [optional] clause relating to Data Subjects lodging a complaint with independent dispute resolution bodies: the UK would like to ask whether an “independent dispute resolution body” includes supervisory authorities (e.g. the ICO). If not, what bodies do we envision as acting in this capacity?
- The UK notes that the lodging of complaints may, under certain circumstances, have a cost. We therefore suggest the text reads “Data Subjects may also lodge a complaint with an independent dispute resolution body *at no greater cost to the Data Subject than if they were subject to local domestic legislation*”.

**Clause 22, Obligations of the Data Importer in case of access by public authorities**

- **Paragraph (a) under review of legality and data minimisation, which sets out how businesses should respond to access requests:** the UK would like to clarify whether the paragraph suggests that the Data Importer should review every single request for disclosure. This may add undue burden to businesses, and so the UK suggests amending the paragraph to state: “The Data Importer agrees to review the legality of the request for disclosure *where there are significant grounds to believe it is unlawful*, in particular whether it remains within the powers granted to the requesting public authority. The Data Importer *may* challenge the request if, after careful assessment, it concludes there are reasonable grounds to consider that the request is unlawful...”
- **Under the same paragraph (a), which suggests Importers should always pursue appeal:** The UK notes that it may be operationally difficult for some Importers to pursue appeal themselves, and suggests changing the sentence to “The Data Importer *may*, under the same conditions, pursue possibilities of appeal.”
- **Under paragraph (c), which asks that businesses provide the minimum information responsible in response to requests:** the UK recommends that providing only “the minimum information permissible... based on a reasonable interpretation of the request” in responding to a request adds a significant additional burden to businesses and leaves room for individual interpretation. We recommend changing this to “*The Data Importer may disclose any requested information in so far as it receives an Access Request, based on a reasonable interpretation of the request*”.

## UNITED KINGDOM – INFORMATION COMMISSIONER’S OFFICE (ICO) / ROYAUME-UNI – BUREAU DU COMMISSAIRE DE L’INFORMATION (ICO)

(...)

By the signatures of their authorized representatives below, both parties agree to be bound by the terms of this agreement.

(...)

### PART I - GENERAL CLAUSES

#### Clause 1. Purpose and scope

(...)

[OPTION This Agreement sets forth the terms and conditions governing the transfer of personal data to a Third country from an entity subject to Convention 108+ (hereinafter the Convention)].

(...)

#### Clause 2. Definitions

(...)

**Genetic data:** all data relating to the genetic characteristics of an individual which have been either inherited or acquired during early prenatal development, as they result from an analysis of a biological sample from the individual concerned including chromosomal, DNA or RNA analysis or analysis of any other element enabling equivalent information to be obtained.

[Source: Par. 57 of Explanatory Report]

**Transborder flows of data** ~~International transfers of personal data~~: transfer of personal data to a Recipient located in a Third country ~~recipient subject to the jurisdiction of another State~~ or to an international organization which is not a party to this Convention.

[Source: Article 14.1 of the Convention, Par. 102. of Explanatory Rep]

(...)

**Onward transfer:** when Personal data transferred to nonanother state-Party or y is likely to be further transferred to a Party located in a jurisdiction without an appropriate level of protection being ensured [OR which is not considered adequate].

[Source: Par. 106 of Explanatory Report]

(...)

**Commented [A192]:** For consistency this may need amending to non-state Party

**Commented [A193]:** Changed to para 57 of the explanatory report

**Commented [A194]:** This could be problematic, as a recipient in the same country could also be subject to certain laws of another State.

For these clauses it may be simpler, albeit not perfect, to revert to "located in"

**Commented [A195]:** Should this be simply a further recipient located in a non-state Party?

**Special categories of Sensitive data:** personal data that is (i) related to Genetic data, or (ii) relating to offences, criminal proceedings and convictions, or related security measures; or (iii) Biometric data uniquely identifying a person; or (iv) revealing data relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life.  
[Source: Article 6 of the Convention]

**Commented [A196]:** This is referred to as Special categories of data in Article 6

(...)

**Third Party Beneficiary:** the Data subject whose Personal data is subject to a the object of an transborder flow(s) of dataInternational transfer.

**Commented [A197]:** The word beneficiary suggests data subjects are benefiting from the flow, which is not necessarily the case.  
Would it be better to just state Data Subject?

### Clause 3. General clauses

#### 3.1. Invariability of the Clauses

These Clauses set out appropriate safeguards, including enforceable data subject rights, obligations for data controllers, obligations for data processors and effective legal remedies, pursuant to Article 14(2)(b) of the Convention and, with respect to data transfers from controllers to controllers, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Annexes.

(...)

#### Interpretation

Where these Clauses use terms that are defined in the Convention, those terms shall have the same meaning as in the Convention.

(...)

### Clause 5. Third Party Beneficiaries

**Commented [A198]:** This section may not be applicable to all jurisdictions. ie Not all jurisdictions do have 3rd party beneficiary rights.

The Parties agree and acknowledge that (a) any Data subject whose Personal data was part of an international data transfer under these Clauses shall be entitled to assert rights and remedies hereunder as a Third-party beneficiary with respect to any provisions of these Clauses affording a right, action, claim, benefit or privilege to such Data subject and (b) the jurisdiction established in Clause 25 is for the benefit of the Data Subject and must allow for third-party beneficiary rights. The Parties shall not challenge such recognition of jurisdiction.

## SECTION II – RIGHTS AND OBLIGATIONS OF THE PARTIES

### Clause 9. Accuracy and data minimisation

(...).

The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.  
[Source: Article 5(4) (c) and (d) of the Convention]

**Commented [A199]:** This includes principles in both Article 5(4)(c) and 5(4)(d)

## Clause 10. Storage limitation

The Data importer shall retain the Personal data in a form which permits identification of data subjects for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organizational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

[Source: Article 5(4)(e) of the Convention]

## Clause 11. Data security

The Data importer and, during transmission also the Data exporter shall ensure that the controller, and where applicable the processor, takes appropriate security measures against risks such as accidental or unauthorized access to, destruction, loss, use, modification or disclosure of personal data.

~~Each party. In particular, the Data importer~~ shall adopt specific security measures, both of technical and organizational nature, for each processing, taking into account: the potential adverse consequences for the individual, the nature of the personal data, the volume of personal data processed, the degree of vulnerability of the technical architecture used for the processing, the need to restrict access to the data, requirements concerning long-term storage, and so forth.

(...)

~~Each Party shall provide that the Controller notifies, without delay, at least the competent Supervisory Authority of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects.~~

In case where a Data breach has occurred that may seriously interfere with the fundamental human rights and fundamental freedoms of the individual (e.g. for instance, the disclosure of data covered by professional confidentiality, sensitive data, or which may result in financial, reputational, or physical harm or humiliation) the Data importer shall notify without undue delay the Data Exporter and the relevant Supervisory Authorities of (i) the incident including a complete description of the Data Breach, and (ii) of any measures taken and/or proposed to address the breach and its potential consequences. This is subject to the exception permitted under Article 11(1) of the Convention.

[Source: Paragraph 65 of the Explanatory Report]

If the data breach is likely to result in a significant risk for the rights and freedoms of individuals, (such as discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage), the Data importer, if necessary in cooperation with the data exporter and also the Data Exporter, shall notify the Data subjects involved in the Data breach and provide them with adequate and meaningful information on, notably, the contact points and possible measures that they could take to mitigate the adverse effects of the Data breach.

[Source: Paragraph 66 of the Explanatory Report]

If the Data importer does not spontaneously inform the Data subject of the Data breach, the supervisory authority, having considered the likely adverse effects of the breach, should be allowed

**Commented [A200]:** Priority Comment 1  
We have concerns that we're asking the importer to notify the SA of the exporter.  
The SAs may not have any jurisdiction or powers to review those data breaches by an importer.

It may be better to state that the importer will notify the Exporter, and (if it has jurisdiction) the Sup Auth.

And if required by Applicable law the Exporter will inform the Sup Auth.

**Commented [A201]:** Priority Comment 2  
The Data importer may not have any relationship with the data subjects. And both the importer and exporter may be processors.

**Commented [A202]:** The supervisory authority may not have jurisdiction. (see Priority Comment 1)



T-PD(2022)1Mos

to require the controller to do so. Notification to other relevant authorities such as those in charge of computer systems security may also be desirable.

[Source: Article 7 of the Convention & Paragraphs 62 to 66 of the Explanatory Report]

### Clause 12. Special categories of Sensitive data

Where the transfer involves special categories of Sensitive data, the parties Data importer shall apply appropriate specific restrictions and additional safeguards in order to prevent adverse effects for the data subjects. For instance this can be the case where there is a potential risk of discrimination or injury to an individual's dignity or physical integrity, sex life or sexual orientation or where processing could affect the presumption of innocence

These appropriate safeguards must be adapted to the risks at stake and the interests, rights and freedoms to be protected.

Such safeguards must guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject [notably a risk of discrimination].

These safeguards may include, for instance, alone or cumulatively (i) the data subject's explicit consent for the processing of special categories of data sensitive data; (ii) a law covering the intended purpose and means of the processing or indicating the exceptional cases where processing such data would be permitted; (iii) a professional secrecy obligation; (iii) measures following a risk analysis; (iv) a particular and qualified organizational or technical security measure (e.g. data encryption, pseudonymisation), (v) limiting the personnel permitted to access the special category Sensitive data, and (vi) additional restrictions with respect to further disclosure according to the nature of the data.

[Source: Article 6 of the Convention and Paragraphs 56 to 61 of the Explanatory Report]

### Clause 13. Onward transfers

The Data importer shall not disclose the personal data to a third party located in a Third country/non-state Party unless the third party is or agrees to be bound by these Clauses.

An Onward transfer by the Data importer may only take place only- if:

(...)

(ii) the third party enters into a legally binding and enforceable instrument with the Data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iii) it is necessary for the establishment, exercise or defence/defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(iv) it is necessary in order to protect the vital interests of the Data subject or of another natural person; or

(...)

(...)

[Source: Article

**Commented [A203]:** As above, the Convention refers to special categories of data

**Commented [A204]:** We find this is not from Article 6 or paras 56-61. We ask to check whether points v and vi should be kept in.

**Commented [A205]:** We think this sentence should be deleted, as according to the list below, they don't need to agree to be bound by these Clauses.

**Commented [A206]:** We would like to see if it's possible to check what the Convention source is of these provisions

### Clause 15. Documentation and compliance

(...)

In particular, the Data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

The Data importer shall make such documentation available to the competent Supervisory authority on request.

The Data importer shall take all appropriate measures to comply with the obligations of these Clauses and be able to demonstrate, to the competent Supervisory authority mentioned in Clause 20, that the data processing under these Clauses is in compliance with the provisions of the Convention and the Applicable law.

(...)

[Source ~~Article clause~~-10 of the Convention]

### Clause 17 – Rights of the Data subjects

The Data importer, if required with the assistance of the Data exporter, shall deal with any enquiries and requests it receives from a Data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.

(...)

[Source: Article 9 of the Convention & Para. 71-83 and 111 of the Explanatory Memorandum of Convention]

### Clause 18. Redress for the data subject

The Data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints. It shall deal promptly with any complaints it receives from a Data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such a redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(...)

**Commented [A207]:** See Priority Comment 1. Does it go to show the exporter has had a breach?

**Commented [A208]:** As above – we have proposed this change throughout this section.

**Commented [A209]:** The Supervisory authority may not have the jurisdiction or power for this.

The underlying principle of transfers is that only relevant protections under the Convention and Applicable law (relevant to the circumstances of the transfer) need to be complied with and these need to be set out in the Clauses.

**Commented [A210]:** We would recommend this passage is clarified.

**Commented [A211]:** We think this time limit is not in the Convention.

**Commented [A212]:** May we ask what the situation would be if it was a processor (or sub-processor)?

**Commented [A213]:** Arbitration would cost the data subject money – in a similar way than going to court. But it may be easier to enforce in the third country

**Clause 19. Liability.**

(...)

Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under the Applicable law.

**Commented [A214]:** We would query whether it is clear which ones those are? (For example, breach of the security requirements)  
It may be better to list which clauses the DS are able to enforce.

Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

**Commented [A215]:** This may need further thought. It means a small exporter is jointly and severally liable with a multinational importer. This could be a class action. Also we would query how this works where there are chains of processors.

(...)

The Data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

**Commented [A216]:** We wonder if this reflects the Convention?

**Clause 20. Supervisory authority**

(...)

The Parties hereby consent that the supervisory authority is entitled to request that the person who transfers data demonstrates the effectiveness of the safeguards or the existence of prevailing legitimate interests and that the supervisory authority may, in order to protect the rights and fundamental freedoms of data subjects, prohibit such transfers, suspend them or subject them to conditions.

**Commented [A217]:** The Data exporter?

**Commented [A218]:** We wonder if this is in the Convention  
This is one of the number of derogations when you wouldn't need the clauses.

[Source: article 14.6 of the Convention]

The Parties agree to submit to the jurisdiction of the Supervisory authorities and not to question its powers, its jurisdiction, or any other action including any forms of co-operation between supervisory authorities as provided by the Applicable law and article 15 and 17 of the Convention.

**Commented [A219]:** See Priority comment 1  
The Supervisory authorities will not have jurisdiction over the importer – unless the underlying Applicable law has extra territorial scope.

[Source: article 15 and 17 of the Convention]

The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent Supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

**Commented [A220]:** See Priority Comment 1

**SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

**Clause 21. Local laws and practices affecting compliance with the Clauses**

The Parties warrant that they have no reason to believe that the laws and practices in the third non-state Party country of destination applicable to the processing of the personal data by the Data

importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses and the Convention.

**Commented [A221]:** The principle of the clauses is not to extend the Convention itself, it's to extend the relevant protections in the circumstances of the transfer.

This is based on the understanding that law(s) and practices that respect the essence of the fundamental human rights and fundamental freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in 11 of the Convention, are not in contradiction with these Clauses.

(...)

## Clause 22. Obligations of the data importer in case of access by public authorities

### Notification

(a) The Data importer agrees, to the extent possible, to notify the Data exporter and, where possible applicable, the data subject promptly (if necessary with the help of the data exporter) if it:

**Commented [A222]:** As above, the exporter and importer may have no relationship with the data subject

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

**Commented [A223]:** We suggest this addition " In so far as local laws allow and it is reasonable to do so".

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

**Commented [A224]:** We suggest this addition again: "In so far as local laws allow and it is reasonable to do so "

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

**Commented [A225]:** What if it is a legitimate request? Should it be required to treat such requests reasonably / as it would for requests for its own data? The Review of legality clause is more reasonable.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

**Commented [A226]:** Instead of providing the information, we suggest an obligation to make and keep a written record of requests.

(...)

### Review of legality and data minimisation

(a) The Data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The Data importer shall, under the same conditions, pursue possibilities of appeal. When making an appeal if reasonable challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 21(e).

T-PD(2022)1Mos

(b) The Data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(...)

**Commented [A227]:** See Priority Comment 1, re supervisory authority jurisdiction and powers

## SECTION IV – FINAL PROVISIONS

### Clause 23. Non-compliance with the Clauses and termination

The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

**Commented [A228]:** Both parties should be under this obligation

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 21(f).

**Commented [A229]:** This will require further consideration. Query whether suspension is necessary in the absence of more than a minimal risk of direct or indirect damage to data subjects.

(...)

(iv) the data importer can no longer comply with clause 21 as there are local laws which prevent it from complying with these clauses and this has more than a minimal risk of direct or indirect damage to data subjects.

**Commented [A230]:** We would recommend this addition.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

**Commented [A231]:** See Priority Comment 1.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.

The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

**Commented [A232]:** The data exporter should be notified of the relevant local law and the required retention period. Only the minimum amount of data should be retained to comply with local law. Processing should stop as soon as permitted by local law upon which the contract will terminate.

(e) Either Party may revoke its agreement to be bound by these Clauses where the Supervisory authority adopts a decision pursuant the Applicable law that ~~covers~~ prohibits the transfer of personal data to which these Clauses apply. This is without prejudice to other obligations applying to the processing in question under the Applicable law.

Consider whether the clauses should continue until all data has been deleted.

### Clause 25. Choice of forum and jurisdiction

(...)

**Commented [A233]:** This jurisdiction must recognise third-party beneficiary rights

**Clause 26. Arbitration [OPTIONAL]**

(...)

Any dispute, controversy or claim between the Parties arising under, out of or relating to these Clauses and any subsequent amendments of this contract, including, without limitation, its formation, validity, binding effect, interpretation, performance, breach or termination, as well as non-contractual claims, ~~shall~~ may be referred to and finally determined by arbitration in accordance with the WIPO Arbitration Rules. The arbitral tribunal shall consist of [a sole arbitrator][three arbitrators]. The place of arbitration shall be [specify place]. The language to be used in the arbitral proceedings shall be [specify language]. The dispute, controversy or claim shall be decided in accordance with the law of [specify jurisdiction].

**Commented [A234]:** We think that this optional clause should be more flexible in its wording: Arbitration should be an option.

(...)

**Clause 27. General Provisions**

(...)

Term. This Agreement will remain in force and effect during the Term until terminated by either party in accordance with clause 23.

**Commented [A235]:** You may need to consider how the Term works when the importer needs to retain data to comply with local law.

(...)