

4



28 JANUARY 1981-2021
CONVENTION 108
ON DATA PROTECTION



Strasbourg, 15 September 2022

T-PD(2022)1rev1Mos

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

Model Contractual Clauses for Transborder Data Flows of Personal Data

REVISED VERSION OF THE ONE SENT FOR COMMENTS ON 07.07.2022

Table of Contents

FINLAND.....	2
GERMANY	18
UNITED KINGDOM / ROYAUME UNI.....	5
COMMISSAIRE A LA PROTECTION DES DONNEES DU CONSEIL DE L'EUROPE.....	16
EUROPEAN COMMISSION	41
EUROPEAN DATA PROTECTION SUPERVISOR	57

FINLAND

COUNCIL OF EUROPE CONVENTION 108+

Model Clauses for Transborder Data Flows of Personal Data STANDARD CONTRACTUAL CLAUSES

Agreement number [xx/2022]

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

Data ~~e~~Exporter information

~~Company~~Name:

Address:

City, Country, zip code:

Email:

Data importer information

~~Name~~Company:

Address:

City, Country, zip code:

Email:

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

Data ~~e~~Exporter

By ~~Name~~:

Signature Date [MM/DD/YEAR]

Data importer

By ~~Name~~:

~~Title~~: [xxxx]

NOTE: These ~~Model~~~~contractual~~ clauses provide an appropriate level of protection for the personal data to non-Parties of Modernised Convention 108 following the standards established by Article 14(3) (b) of Modernised Convention 108⁺.

STANDARD-MODEL CONTRACTUAL CLAUSES

~~Contractual-Model~~ clauses for transborder flow of personal data from controller to controller

The Data Exporter and the Data importer (hereinafter, the Parties) agree to these ~~standard~~~~Model~~~~contractual~~ clauses (hereinafter the Clauses):

PART I - GENERAL CLAUSES

Clause 1. Purpose and scope

1.1. The aim of these ~~standard~~~~contractual~~model clauses is to ensure compliance with the requirements for the transfer of personal data to a non-Party under Convention 108+ (hereinafter the Convention).

When adopted and implemented by the persons involved in the transfer and further processing,
~~These contractual-Model~~ clauses provide an appropriate level of protection for the transfer of personal data following Article 14(3)(b) of the Convention.

(...)

Model Clauses ~~(or Standard contractual clauses)~~: Approved standardised safeguards provided by legally binding and enforceable instruments as required under Article 14(3)(b) of the Convention.

(...)

[Source: Article 7 of the Convention]

(...)

[Source: Article 26.3 of the Convention]

(...)

Special categories of data: ~~(or Sensitive data):~~ (i) Genetic data, (ii) personal data relating to offences, criminal proceedings and convictions, or related security measures; (iii) Biometric data uniquely identifying a person; or (iv) personal data for the information they reveal 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 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(3)(b) of the Convention, provided they are not modified, except to add or update information in the Annexes.

(...)

Interpretation

(...)

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. 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~~ prevail over these Clauses.

Commented [A1]: FINLAND : It is difficult to decide whether the deletion is ok. Just to note that an option of transfers from controller to processor has been added at the end of the clauses. Also, the definitions of « data exporter » and « data importer » include both the controller and the processor.

In any case, it is important to keep in mind that the adequate protection of personal data should be guaranteed in all cross-border transfers, and cannot be undermined by transferring data to a processor (or sub-processor).

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 Annex 2, and, if required, updating the ~~data~~ description of the transfer of Annex 1.

(...)

The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

~~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 8. Transparency of processing

(...)

8.2. Paragraph 1 shall not apply where the Data subject already has the relevant information.

~~8.3. Paragraph 1 shall not apply when the Personal data are not collected from the data subject~~ where the processing is expressly prescribed by law or this proves to be impossible or involves disproportionate efforts.

[Source: Article 8 of the Convention]

Clause 9. Accuracy and data minimisation

(...)

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.

(...)

Commented [A2]: Is this part really necessary – in my opinion it could be deleted, but it is also ok for me to leave it.

Commented [A3]: I think, this does not apply to this part, does it?

The Data importer shall ~~notify~~ notify, without delay, at least the Data Exporter, who will notify the competent Supervisory Authority of those data breaches which may interfere with the rights and fundamental freedoms of data subjects.

In case where a Data breach has occurred that may seriously interfere with the human rights and fundamental freedoms of the individual (e.g. the disclosure of data covered by professional confidentiality, Special categories of sensitive data, or which may result in financial, reputational, or physical harm or humiliation) the Data importer shall notify without delay the Data Exporter and the relevant Supervisory Authority/es 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.

[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 where applicable, and also the Data Exporter, shall notify the Data subjects involved in the Data breach and ~~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.

In specific circumstances, where the notification would require unreasonable time, effort or resources, the Data importer may seek the cooperation or the assistance of the Data exporter to produce the notifications and measures in the previous paragraph.

[Source: Article 7 of the Convention & Paragraph 66 of the Explanatory Report]

(...)

Clause 12. Special categories of data

Where the transfer involves ~~Sensitive~~ Special categories of data, the Data importer shall apply additional safeguards adapted to the risks at stake and the interests, rights and freedoms to be protected.

(...)

The Parties have agreed on the safeguards as set out in Annex 4~~The Parties shall set out these~~
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 non-Party unless the third party ensures an appropriate level of protection in line with Article 14 of the Convention-108+.

(...)

Clause 14. Processing under the authority of the Data importer

(...)

Clause 15. Documentation and compliance

(...)

The Data importer guarantees that it has paid due regard to the impact the intended data processing might have on the rights and fundamental freedoms of Data subjects prior to the commencement of such processing according to the circumstances of the specific transfer and has taken the necessary technical and organisational measures to comply with the clause. 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 has designed the data processing in such a manner as to prevent or minimize the risk of interference with those rights and fundamental freedoms.

Clause 16 – Rights of the Data subjects

(...)

Clause 17. Redress for the Data subject

(...)

The alternative mentioned in the paragraph above does not exclude or alter the right of the Data subject afforded by these Clauses, the Convention and the Applicable law to lodge a claim complaint at the Supervisory Authority/ies or at the courts of the applicable jurisdiction. The Data importer shall abide by a decision that is binding under the Applicable law.

(...)

Commented [A4]: FINLAND : The clause is about documentation and compliance. The clause could be made more concise as proposed, but this part of the text has apparently changed the meaning (technical and organisational measures which take into account the implications ...). Appropriate technical and organisational measures are usually required to guarantee the protection of personal data at all stages of processing. Those must be documented so that the controller is able to demonstrate compliance with that requirement.

Clause 19. Supervisory authority

(...)

The Parties hereby consent that the supervisory authority is entitled to request that any of the Parties demonstrates the effectiveness of the safeguards ~~or including~~ 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]

(...)

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

Clause 20. Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in ~~the country of destination~~~~the non-Party 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. This should include full and joint liability for any material and non-material damages made by the Parties, or which occurred to the data subject in relation of the use of the Clauses.

(b) This is based on the understanding that specific exceptions to these Clauses based on applicable law(s) that respect the essence of the 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.

(...)

- ii) the laws and practices ~~in the country of destination~~~~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;

(...)

- (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 issued and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

Commented [A5]: including those going beyond the mere risks that may arise with the data transfer

(...)

- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the ~~non-Party~~ country of destination – or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(...)

Clause 21. 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, and to the extent possible - the Data subject promptly (if necessary, with the help of the data exporter) if it:

(...)

- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, on the request of 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.).

(...)

SECTION IV – FINAL PROVISIONS

Clause 22. Non-compliance with the Clauses and termination

- (a) ~~Each Party shall promptly inform each other party if it is unable to comply~~ ~~Both Parties shall promptly inform each other if they are unable to comply~~ with these Clauses, for whatever reason.

(...)

[OPTION 1]

Any dispute, controversy or claim between the Parties arising under, out of or relating to these Clauses including, without limitation, its formation, validity, binding effect, interpretation, performance, breach or termination, as well as non-contractual claims, shall 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]~~the country of the Data Exporter.

[WIPO CLAUSE - Arbitration clause only for B2B conflicts]

[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/

The alternative mentioned in the paragraph above does not exclude or alter the right of the Data subject afforded by these Clauses, the Convention and the Applicable law to lodge a ~~claim~~ complaint of any kind at the Supervisory Authority/ies or at the courts of the applicable jurisdiction.

[OPTION 2]

(...)

The alternative mentioned in the paragraph above does not exclude or alter the right of the Data subject afforded by these Clauses, the Convention and the Applicable law to lodge a complaint ~~claim~~ of any kind at the Supervisory Authority/ies or at the courts of the applicable jurisdiction.

(...)

Annex 1
Information about the transfer

Description of the transfer: [...]

Purpose(s) of the transfer: [...]

Additional information: [...]

Annex 2
Accession form

Agreement number [xx/2022]

Designation: [Data Exporter] or [Data importer]

Company name:

Address:

City, Country, zip code:

Email:

By the signatures of their authorized representatives below, [Company name] agrees to become, with immediate effect, a Party to and agrees to be bound by the terms of the Contractual clauses for transborder flow of personal data [from controller to controller] OR [from controller to processor].

By Name:

Title: [xxxx]

Signature Date [xxxx]

Annex 3

Security measures

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

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Annex 4

Measures for ~~sensitive~~ Special categories of data]

[These safeguards may include, for instance, alone or cumulatively

- i) the data subject's explicit consent for the processing of ~~sensitive~~ Special categories of 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 Special categories of~~Sensitive~~ data, and
- vi) additional restrictions with respect to further disclosure according to the nature of the data].

Annex 5

LIST OF SUB-PROCESSORS

[ONLY FOR MODULE 2 & 3 to be drafted after concluding model C2C - This annex has to be completed by the Parties if they agree to pre-authorize sub processors]

GERMANY

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION
OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING
OF PERSONAL DATA
CONVENTION 108

Model Contractual Clauses for Transborder Flows of Personal Data

Commented [A6]: The term « data » appears twice, therefore we suggest to delete the term « data » in « Transborder Data Flows » so that the modified title of the document would be.
Model Contractual Clauses for Transborder Flows of Personal Data.
This would also be in line with the « definition » given in Clause 2 of this draft document.

Commented [A7]: In our view, the SCC of the EU Commission are a very good example for future Model Contractual Clauses (MCC). They are the most used transfer tool by data exporters falling under the scope of the GDPR. The wide spread use of MCC with similar requirements would promote further global convergence of data protection enabling thus the free flow of personal data and guaranteeing the protection of personal travels with the data.
In this light, we refer to the COM SCC in the following comments and suggest further alignment.

**COUNCIL OF EUROPE
CONVENTION 108+
Model Clauses for Transborder Flows of Personal Data**

Agreement number [xx/2022]

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

Data exporter information

Name:

Address:

City, Country, zip code:

Email:

Data importer information

Name:

Address:

City, Country, zip code:

Email:

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

Data exporter

By:

Signature Date [MM/DD/YEAR]

Data importer

By:

Signature Date [MM/DD/YEAR]

NOTE: These Model clauses provide an appropriate level of protection for the transfer of personal data to non-Parties of Modernised Convention 108 following the standards established by Article 14(3) (b) of Modernised Convention 108.

Commented [A8]: see previous comment, which says : The term « data » appears twice, therefore we suggest to delete the term « data » in « Transborder Data Flows » so that the modified title of the document would be.
Model Contractual Clauses for Transborder Flows of Personal Data.
This would also be in line with the « definition » given in Clause 2 of this draft document.

MODEL CONTRACTUAL CLAUSES

Model clauses for transborder flow of personal data from controller to controller

The Data Exporter and the Data importer (hereinafter, the Parties) agree to these Model clauses (hereinafter the Clauses):

PART I - GENERAL CLAUSES

(...)

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 of, either directly or through the Data exporter:

Commented [A9]: editorial

(...)

- g. any necessary additional information in order to ensure fair and transparent processing of the personal data.

Commented [A10]: Amendment in line with Art. 8 (1) of Convention 108+

(...)

8.3. Paragraph 1 shall not apply when the Personal data are not collected from the data subject where the processing is expressly prescribed by law or this proves to be impossible or involves disproportionate efforts.

[Source: Article 8 of the Convention]

Commented [A11]: Is this part really necessary – in my opinion it could be deleted, but it is also ok for me to leave it.

(...)

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.

Commented [A12]: I think, this does not apply to this part, does it?

In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the

risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(...)

The Data importer shall notify, without delay, at least the Data Exporter, who will notify the competent Supervisory Authority of those data breaches which may interfere with the rights and fundamental freedoms of data subjects.

(...)

Clause 13. Onward transfers

The Data importer shall not disclose the personal data to a third party located in a non-Party unless the third party ensures an appropriate level of protection in line with Article 14 of the Convention.

(...)

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

Clause 20. Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the 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. This should include full and joint liability for any material and non-material damages made by the Parties, or which occurred to the data subject in relation of the use of the Clauses. 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 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.

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

- 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

Commented [A13]: To specify the standards to be applied to TOMs.

Commented [A14]: On this point, it has been noticed that a notification chain is implemented in case of data breaches, which is different from those of the COM's SCC. In the current text, the data importer notifies the data exporter, who in turn notifies the CSA. In the case of the SCC (Module One: Clause 8.5 (e)), the data importer notifies both in parallel. BfDI suggests to change the wording into the SCC wording.

Commented [A15]: The SCCs of the European Commission allow for data transfers, if the third party agrees to be bound by these Clauses. Why is this aspect not reflected here ? In contrast, the sole reference to Article 14 of Convention 108+ seems to fall a bit short.

Commented [A16]: We would suggest (based on the SCC clause 14(a) sentence 2) to also refer to the practices, as these are also to be considered in the assessment (see ii)

Commented [A17]: Here the enumeration ((a) and (b)) does not match with the one in the SCC, so that, according to our view, the references made in subsequent paragraphs do not quite match. We have adjusted them accordingly.

and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(...)

- (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 [issue] 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.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the country of destination or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

Commented [A18]: See our first comment to this clause. This reference should now be correct.

Commented [A19]: including those going beyond the mere risks that may arise with the data transfer

Commented [A20]: Insofar as the text contained in the comment before is intended to be an addition that is still to be inserted, this goes beyond the wording of the SCC of the COM (clause 14 c). But could possibly be included as a clarification.

Commented [A21]: See our first comment to this clause. This reference should now be correct.

Commented [A22]: See our first comment to this clause. This reference should now be correct. Not only a) is part of the warranty. See SCC COM clause 14 (e)

Commented [A23]: See our comment before.

(...)

Clause 21. 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, and to the extent possible the Data subject promptly (if necessary with the help of the data exporter) if it:

(...)

- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, on the request of the data exporter, 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.).

(...)

SECTION IV – FINAL PROVISIONS

(...)

Commented [A24]: Why « where applicable, and to the extent possible » ? We prefer only « where possible »

Commented [A25]: This means, that the data importer provides information to the exporter only when the exporter makes a request. We would prefer the previous wording ("at regular intervals for the duration of the contract"). It is not comprehensible why the importer cannot inform the exporter on a regular basis, but should only act upon request of the exporter. Regular information of the exporter about applications made accordingly, especially with regard to possible developments (e.g. increase of applications in total or only of certain authorities) is useful for the assessment as well as in terms of transparency and for effective data protection. Alternatively, we would suggest the wording from SCC clause 15.1 (c).

UNITED KINGDOM / ROYAUME UNI

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION

OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING

OF PERSONAL DATA

CONVENTION 108

Model Contractual Clauses for Transborder Data Flows of Personal Data

COUNCIL OF EUROPE

CONVENTION 108+

Model Clauses for Transborder Data Flows of Personal Data

Commented [A26]: What is the intended vision for these Clauses? Is the document intended to be a final set of Clauses Members to recognise and adopt domestically, without any amendments? Or is the intention for these to be more flexible, for Members to modify and draw inspiration from?

T-PD(2022)1rev1Mos

Agreement number [xx/2022]

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

Data exporter information

Name:

Address:

City, Country, zip code:

Email:

Data importer information

Name:

Address:

City, Country, zip code:

Email:

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

Data exporter

By :

Signature Date [MM/DD/YEAR]

Data importer

By :

Signature Date [MM/DD/YEAR]

NOTE: These Model clauses provide an appropriate level of protection for the transfer of personal data to non-Parties of Modernised Convention 108 following the standards established by Article 14(3) (b) of Modernised Convention 108.

MODEL CONTRACTUAL CLAUSES

Model clauses for transborder flow of personal data from controller to controller

The Data Exporter and the Data importer (hereinafter, the Parties) agree to these Model clauses (hereinafter the Clauses):

PART I - GENERAL CLAUSES

Clause 1. Purpose and scope

(...)

Clause 2. Definitions

(...)

Data importer: The Controller located in a non-Party to whom the Data exporter transfers Personal data.

Data Exporter: The Controller located in a country that is a member of the Convention, that transfers Personal data to a Data importer.

(...)

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 8. Transparency of processing

(...)

8.3. Paragraph 1 shall not apply when the Personal data are not collected from the data subject [\[A1\]](#) where the processing is expressly prescribed by law or this proves to be impossible or involves disproportionate efforts.

[Source: Article 8 of the Convention]

(...)

Commented [A27]: Under Clause 1 of the draft Model Contractual Clauses, the scope of the clauses is set-out. However - the UK remains unclear as to what type of transfers would be captured by the clauses; for example, could the Model Contractual Clauses be used for the transfer of personal data for law enforcement and national security purposes, or for general processing? As the Working Group will be aware, both in the UK and the EU GDPR covers general and national security processing whereas other directives and acts (such as the Law Enforcement Directive and Part 3 of the Data Protection Act 2018 in the UK) regulates law enforcement processing. We'd be grateful to understand the types of transfers under C108+ which would be captured by these draft clauses.

Commented [A28]: We recommend deleting 'Data Processors' from the Definition of 'Data Exporter/Importer' as these seem to be Controller-to Controller clauses.

Commented [A29]: Do we want to use a technical term such as "warrant" – which has a particular meaning?

We would suggest to use a more generic term - For example, "confirms that"

Commented [A30]: In response to the Expert's question (asked in footnote A1) we would keep that whole point '8.3' in.

This provision should be kept in based on Art 8 (3)

Clause 11. Data security

The Data importer and, during transmission also the Data exporter shall ensure that the Controller, and where applicable the Processor^[A2], takes appropriate security measures against risks such as accidental or unauthorized access to, destruction, loss, use, modification or disclosure of personal data.

(...)

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 where the data importer is a processor, each party shall provide that the Controller 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.

(...)

Clause 18. 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 these Clauses and the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the Data exporter under the Applicable law.

(...)

The Data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability. The Data Importer remains responsible for the processing also where a processor is processing the data on his or her behalf.

[Source: Para. 22 of the Explanatory Report]

(...)

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

Clause 20. 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 [A31]: We previously commented as a Priority Comment

“The Data importer may not have any relationship with the data subjects. And both the importer and exporter may be processors.”

Further explanation:

First the data importer may not have any relationship with the data subjects. AND there may be situations where both the importer and exporter may be processors (and therefore seemingly no obligation to report to the DPA)

Clearly this will be a difficult clause for the importer to fulfil if it has no relationship to the DS. Furthermore this may contradict with Art 7.2 of C108+ which states that it is the controllers obligation to inform and no mention is made of the processors obligations.

We suggest to modify this way: “... the data importer, and where the data importer is a processor, each party shall provide that the controller 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 [A32]: We previously commented that 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.

Indeed it provides legal certainty and clarity in particular for data subjects and small businesses.

Commented [A33]: We had previously commented here and would like to clarify our comment: we wonder if this reflects the Convention?

In particular we would suggest to mirror the wording in para 22 of the explanatory report to C108+ and add: “the Data Importer remains responsible for the processing also where a processor is processing the data on his or her behalf.”

Commented [A34]: We previously already made a comment which we’d like to clarify.

We note that best practice in regard to transfer risk assessments is still developing and changing. We would therefore suggest that these Clauses should be relatively flexible in their interpretation of the risk assessment, allowing room for evolving practices and providing organisations flexibility in conducting the assessments. The focus of our approach in the upcoming TRA, Transfer Risk Assessment in the UK will be on human rights and risks more generally just to give an example. We have indicated in grey in the text areas that we think could be omitted to give DPAs more flexibility.

Our proposed NEW text would read:

- 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 relevant laws and practices in the 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.

(...)

Clause 21. Obligations of the data importer in case of access by public authorities

Notification

- (a) In so far as local laws allow and it is reasonable to do so, the Data importer agrees to notify the Data exporter and, where applicable and to the extent possible the Data subject promptly (if necessary, with the help of the data exporter), if it:

(...)

- (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.

(...)

Review of legality and data minimisation

(...)

SECTION IV – FINAL PROVISIONS

Clause 22. Non-compliance with the Clauses and termination

(...)

- (b) In the event that the Data importer is in breach of these Clauses or unable to comply with these Clauses, and there is a real and serious risk that the transfer would lead to circumventing the provisions of the Convention, the data exporter may suspend the

Commented [A35]: We suggest adding "relevant" here, as current wording suggests Parties would need to take into account all the laws and practices of the destination country (not reasonable or proportionate).

Commented [A36]: The UK has substantive concerns around this section, in its current form.

National security is rightly outside the scope of C108+, which is governed by the domestic legislation of each Party. However, this Clause places significant and specific obligations on businesses in terms of how they interact with domestic national security agencies.

We understand that this is the approach taken in the EU SCCs (Clause 15.1 & 15.2), which these Clauses have drawn inspiration from. However, for these model contractual clause have the potential for use by C108+ Parties, all members must be comfortable with its provisions and it must be within the scope of processing under C108+. Given the diversity of Party membership, we would therefore ask that the specificity of this section is significantly reduced to allow for differing approaches, and to ensure these Clauses do not stray into remit not occupied by C108+.

We have provided several comments that bring Clause 21 closer to acceptable for the UK - but we will provide further comments on the next draft.

Commented [A37]: We previously already made a comment which we'd like to clarify.

We suggest adding

"in so far as local laws allow and it is reasonable to do so". This is to prevent a legal conflict in this area and provide additional legal certainty - i.e. in cases where domestic laws prohibit businesses from disclosing public authority access requests.

Commented [A38]: We previously already made a comment which we'd like to clarify.

We suggest that the importer should not necessarily be bound to seek a waiver in every circumstance - for example, if they assess the request to be lawful. We suggest adding this wording "**The legality of the request should be reviewed**" at the start of para b— or wording of the EU SCCs (15.2) and Clause 23.2 IDTA as the same approach is taken there.

Commented [A39]: Is this intended to be its own Clause? All other bolded headlines are Clause or Section titles.

transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 20(f).

(...)

- (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 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. The same shall apply to any copies of the data.

(...)

Clause 26. General Provisions

[These are standard clauses in contracts. These may be merged with the general clauses of the first section of the model clauses in order not to have two general sections]

Term. This Agreement will remain in force and effect during the Term until terminated by either party in accordance with clause 22.

OPTION: Term. This Agreement will remain in force and effect and renew automatically until terminated by either party in accordance with clause 22.

(...)

Commented [A40]: We previously already made a comment which we'd like to clarify. We would welcome further discussion on whether suspension is necessary in all cases - for example, where there is only a minimal risk of direct/indirect damage to data subjects. In some cases it causes more harm to suspend the transfer to the data subject.

Indeed Article 14(1) C108+ refers to a "real and serious risks that the transfer to another Party, or from that other Party to a non-party, would lead to circumventing the provisions of the Convention" And according to para 106 of the explanatory note – parties cannot rely on it "where the risk is either hypothetical or minor". Clear and reliable evidence is required that the transferring the data to another party could significantly undermine the protections afforded to the data under the convention and that the likelihood of that happening is high.

Change suggested:
We would ask to replace 'shall' by 'may'

Commented [A41]: We previously already made a comment which we'd like to clarify. We still suggest this addition: ***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. Consider whether the clauses should continue until all data has been deleted.

Commented [A42]: We previously already made a comment which we'd like to clarify. You may need to consider how the Term works when the importer needs to retain data to comply with local law.

Suggested wording to replace the current text: ***"Where the data importer must retain transferred personal data in order to comply with a local law, the term will remain in force in respect of any retained data for as long as the personal data is retained."***

This is in keeping with Eg. section 31.1 IDTA in the UK and clause 16 EU SCCs in case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data

Annex 1

Information about the transfer

Description of the transfer: [...]

Purpose(s) of the transfer: [...]

Additional information: [...]

Annex 2

Accession form

Agreement number [xx/2022]

Designation: [Data Exporter] or [Data importer]

Company name:

Address:

City, Country, zip code:

Email:

By the signatures of their authorized representatives below, [Company name] agrees to become, with immediate effect, a Party to and agrees to be bound by the terms of the Contractual clauses for transborder flow of personal data [from controller to controller] OR [from controller to processor].

By Name:

Title: [xxxx]

Signature Date [xxxx]

Annex 3

Security measures

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

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

]

Annex 4

Measures for Special categories of data]

[These safeguards may include, for instance, alone or cumulatively

- i) the data subject's explicit consent for the processing of Special categories of 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 Special categories of data, and
- vi) additional restrictions with respect to further disclosure according to the nature of the data].

Annex 5

LIST OF SUB-PROCESSORS

[ONLY FOR MODULE 2 & 3 to be drafted after concluding model C2C - This annex has to be completed by the Parties if they agree to pre-authorize sub processors]

[A1](#) Is this part really necessary – in my opinion it could be deleted, but it is also ok for me to leave it.

[A2](#) I think, this does not apply to this part, does it?

[A3](#) including those going beyond the mere risks that may arise with the data transfer

COMMISSAIRE A LA PROTECTION DES DONNEES DU CONSEIL DE L'EUROPE

COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION
DES PERSONNES A L'ÉGARD DU TRAITEMENT AUTOMATISÉ
DES DONNÉES A CARACTÈRE PERSONNEL
CONVENTION 108

Clauses contractuelles types relatives aux flux transfrontaliers
de données à caractère personnel

CONSEIL DE L'EUROPE

CONVENTION 108+

Clauses types relatives aux flux transfrontaliers
de données à caractère personnel

Accord n° [xx/2022]

Délai/Durée : date de début [JJ/MM/AAAA] – date de fin [JJ/MM/AAAA]

Coordonnées de l'~~Exportateur~~exportateur de données

Nom :

Adresse :

Ville, pays, code postal :

Courrier électronique :

Coordonnées de l'~~Importateur~~importateur de données

Nom :

Adresse :

Ville, pays, code postal :

Courrier électronique :

Par la signature de leurs représentants autorisés, les parties s'engagent à respecter les conditions énoncées dans le présent accord.

~~Exportateur~~exportateur de données

Nom :

~~Fonction : [xxxx]~~ Date de la signature [JJ/MM/AAAA]

~~Importateur~~importateur de données

Nom :

Date de la signature [JJ/MM/AAAA]

NOTE : les présentes Clauses contractuelles types offrent un niveau de protection adéquat pour le transfert de données à caractère personnel vers un tiers non-Partie à la Convention 108 modernisée suivant les normes établies par son article 14.3. ~~(b) de la Convention 108 modernisée¹~~.

CLAUSES CONTRACTUELLES TYPES

Clauses ~~contractuelles~~ types relatives aux flux transfrontières de données à caractère personnel entre responsables du traitement des données

L'~~Exportateur~~exportateur de données et l'~~Importateur~~importateur de données (ci-après : les Parties) approuvent les ~~Clauses-clauses~~contractuelles types énoncées aux présentes (ci-après : les Clauses) :

SECTION I – CLAUSES GÉNÉRALES

Clause 1. Finalités et champ d'application

1.1. Les présentes clauses types visent à garantir le respect des exigences relatives au transfert des données à caractère personnel vers un tiers non-Partie à la Convention 108+ (ci-après : la Convention). Une fois adoptées et appliquées par les signataires impliqués dans le transfert et le traitement ultérieur qui en découle, eElles offrent un niveau de protection adéquat pour le transfert de données à caractère personnel au titre de l'article 14.3.(b) de la Convention.

1.2. Description du transfert

Les présentes ~~Clauses-clauses~~ s'appliquent au transfert des données à caractère personnel décrites à l'annexe 1.

(...)

Clause 2. Définitions

[Note : En plus des sources citées pour chaque terme défini, voir aussi le document

T-PD(2020)06rev3, Interprétation des dispositions].

Dans les présentes ~~Clauses~~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 de l'~~Exportateur~~exportateur des données.

(...)

Traitement de données :

(...)

~~Importateur~~importateur de données : le responsable du traitement ou le sous-traitant situé dans la juridiction d'un tiers vers lequel l'~~Exportateur~~exportateur de données transfère des données à caractère personnel.

~~Exportateur~~exportateur de données : le responsable du traitement ou le sous-traitant situé dans la juridiction d'un pays Partie à la Convention qui transfère des données à caractère personnel vers un ~~Importateur~~importateur de données.

(...)

Transfert ultérieur : lorsque des données à caractère personnel sont transférées par un ~~Exportateur~~exportateur de données à un autre responsable du traitement ou à un autre sous-traitant

Partie (ou Parties) : chaque signataire des présentes ~~Clauses~~clauses

(...)

Catégories spéciales de données : (i) données génétiques, (ii) données concernant des infractions, des procédures et des condamnations pénales et des mesures de sûreté connexes ; (iii) données biométriques identifiant un individu de façon unique ; ou (iv) données révélant des informations sur l'origine raciale ou ethnique, les opinions politiques, l'appartenance syndicale, les convictions religieuses ou autres convictions, la santé ou la vie sexuelle (~~ci-après données sensibles~~).

[Source : article 6 de la Convention]

Autorité(s) de contrôle : une ou plusieurs autorités chargées de veiller au respect des dispositions de la Convention, du droit applicable et des présentes ~~Clauses~~clauses.

[Source : article 15 de la Convention]

Tiers bénéficiaire : la personne concernée, dont les données à caractère personnel font l'objet de transferts transfrontières concernés par les présentes ~~Clauses~~clauses

Clause 3. Clauses générales

3.1. Invariabilité des ~~Clauses~~clauses

Les présentes ~~Clauses~~clauses établissent des garanties appropriées, y compris des droits opposables pour la personne concernée, des obligations incombant aux responsables du traitement des données, ~~des obligations incombant aux sous-traitants~~ et des voies de recours effectives, en vertu de l'article 14.3.b de la Convention, à condition qu'elles ne soient pas modifiées, sauf pour ajouter ou mettre à jour des informations dans les annexes.

Cela n'empêche pas les Parties d'inclure les présentes clauses dans un contrat plus large et/ou d'ajouter d'autres ~~Clauses-clauses~~ ou des garanties supplémentaires, à condition que celles-ci ne contredisent pas les ~~Clausesclauses~~, directement ou indirectement, ou qu'elles ne portent pas atteinte aux droits de l'homme et aux libertés fondamentales des personnes concernées conformément à la Convention.

Les présentes ~~Clauses-clauses~~ sont sans préjudice des obligations incombant à l'~~Exportateurexportateur~~ des données au titre du droit applicable.

Interprétation

Lorsque les présentes ~~Clausesclauses~~ utilisent des termes définis dans la Convention, ceux-ci ont la même signification que dans la Convention et sont interprétés à la lumière de son rapport explicatif.

Les présentes ~~Clauses-clauses~~ sont lues et interprétées à la lumière des dispositions de la Convention.

Les présentes ~~C~~clauses ne sont pas interprétées dans un sens contraire aux droits et obligations prévus dans la Convention et transcrites dans le droit applicable.

En cas de contradiction entre les présentes ~~-Clausesclauses~~ et les dispositions d'accords connexes entre les Parties, en vigueur au moment où les présentes ~~C~~clauses sont convenues ou souscrites par la suite, les présentes ~~C~~clauses l'emportent. Une exception existe lorsque les termes en contradiction dans l'accord concerné offrent aux droits de la Personne concernée une plus forte protection, auquel cas ces termes l'emportent sur les présentes ~~Clausesclauses~~.

Clause 4. Clause d'adhésion

Une entité qui n'est pas une Partie aux présentes ~~C~~clauses peut, avec l'accord des autres Parties, y adhérer à tout moment, soit en qualité d'~~Exportateurexportateur~~ de données soit en qualité d'~~Importateurimportateur~~ de données, en remplissant et en signant l'annexe 2 et, si nécessaire, en mettant à jour la description ~~du transfert des données~~ à l'annexe 1.

Après avoir rempli et signé le formulaire de l'annexe 2, l'entité adhérente devient Partie aux présentes Clauses et, ce faisant, elle a les droits et obligations d'un ~~Exportateurexportateur~~ des données ou d'un ~~Importateurimportateur~~ des données selon sa désignation à l'annexe 2.

L'entité adhérente n'a aucun droit ni obligation découlant des présentes ~~Clauses-clauses~~ pour la période antérieure à son adhésion à celles-ci.

Clause 5. Tiers bénéficiaires

Les Parties conviennent de ce qui suit : toute ~~Personne-personne~~ concernée dont les ~~Données données~~ à caractère personnel ont été transférées au titre des présentes Clauses est fondée à

s'appuyer sur les sauvegardes et garanties énoncées aux termes de la section II des présentes Clauses en tant que Tiers bénéficiaire conformément à toute disposition des présentes Clauses lui octroyant un droit, une voie de recours, un droit à réparation, un avantage ou un privilège.

~~La juridiction compétente est désignée à la Clause 25 à l'intention de la Personne concernée et doit permettre l'accès aux droits des tiers bénéficiaires. Les Parties s'abstiennent de contester cette reconnaissance de compétence.~~

SECTION II – DROITS ET OBLIGATIONS DES PARTIES

Clause 6. Garanties en matière de protection des données

L'~~Exportateur~~exportateur de données certifie qu'il a fait toute diligence pour établir que l'~~Importateur~~importateur de données est à même, par l'exécution de mesures techniques et organisationnelles appropriées, de remplir les obligations qui lui incombent au titre des présentes Clauses.

Clause 7. Limitation de la finalité

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

[Source : article 5.4.b de la Convention]

Clause 8. Transparence du traitement

8.1. Afin de permettre aux Personnes concernées d'exercer effectivement les droits que leur confèrent les présentes Clauses, l'~~Importateur~~importateur de données leur communique les informations ci-après, directement ou par l'intermédiaire de l'~~Exportateur~~exportateur de données :

(...)

Clause 9. Exactitude et minimisation des données

Chaque Partie veille à ce que les données à caractère personnel soient exactes et, si nécessaire, tenues à jour. L'~~Importateur~~importateur de données fait toute diligence pour s'assurer que les données à caractère personnel qui sont inexactes, eu égard à la ou aux finalités du traitement, soient effacées ou rectifiées sans délai.

Lorsque l'~~Importateur~~importateur de données est informé par l'~~Exportateur~~exportateur de données de corrections apportées par ce dernier aux données à caractère personnel, il applique rapidement toutes ses corrections.

T-PD(2022)1rev1Mos

| L'~~importateur~~Importateur de données s'assure que les données à caractère personnel sont adéquates, pertinentes et limitées au strict nécessaire eu égard à la ou aux finalités du traitement.

[Source : article 5.4.d de la Convention]

DRAFT DOCUMENT

Clause 10. Limitation de la conservation

L'~~Importateur~~~~importateur~~ de données conserve les ~~Données~~~~données~~ à caractère personnel pendant une durée n'excédant pas celle qui est nécessaire à la ou aux finalités de leur traitement. Il met en place les mesures d'ordre technique ou organisationnel appropriées pour garantir le respect de cette obligation, notamment l'effacement ou l'anonymisation des données et de toutes leurs sauvegardes à la fin de la période de conservation.

Clause 11. Sécurité des données

L'~~Importateur~~~~importateur~~ de données ainsi que, pendant la transmission, l'~~Exportateur~~~~exportateur~~ de données, s'assurent que le Responsable du traitement et, le cas échéant, le Sous-traitant, prennent [\[A2\]](#) les mesures de sécurité appropriées contre les risques tels que l'accès accidentel ou non autorisé aux données à caractère personnel, ainsi que leur destruction, perte, utilisation, modification ou divulgation accidentelle ou non autorisée.

L'~~Importateur~~~~importateur~~ de données doit en particulier prendre des mesures de sécurité appropriées, d'ordre technique et organisationnel, pour chaque traitement, en tenant compte : notamment de la nature des données à caractère personnel, du volume de données à caractère personnel traitées, du degré de vulnérabilité de l'architecture technique utilisée pour la réalisation du traitement et de la nécessité de restreindre l'accès aux données.

Leur coût doit être proportionné à la gravité et à la probabilité des risques potentiels.

Les Parties sont convenues des mesures d'ordre technique et organisationnel énoncées à l'annexe 3. L'~~Importateur~~~~importateur~~ de données vérifie régulièrement que ces mesures continuent d'offrir le niveau de sécurité approprié et les met à jour lorsque ce n'est plus le cas.

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

En cas de violation des données à caractère personnel traitées par l'~~Importateur~~~~importateur~~ dans le cadre des présentes Clauses, celui-ci prend les mesures appropriées à la violation, y compris des mesures pour limiter les éventuels dommages.

L'~~Importateur~~~~importateur~~ de données notifie l'incident sans délai au moins à l'~~Exportateur~~~~exportateur~~ de données qui à son tour notifie à l'Autorité de contrôle compétente les violations de données qui pourraient interférer avec les droits et les libertés fondamentales des personnes concernées.

En cas de violation des 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~~~~spéciales~~~~sensibles~~, ou divulgation pouvant causer un préjudice financier, porter atteinte à la réputation, à l'intégrité physique ou entraîner une humiliation), l'~~Importateur~~~~importateur~~ de données est tenu de notifier sans délai à l'~~Exportateur~~~~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]

Lorsque la violation des données est de nature à engendrer un risque important pour les droits et libertés des ~~Personnes~~~~personnes~~ concernées (par exemple un traitement discriminatoire, un vol ou une usurpation d'identité, des pertes financières, une atteinte à la réputation, une perte de confidentialité des données protégées par le secret professionnel ou tout autre préjudice économique ou social lourd), l'~~Importateur~~~~importateur~~ de données et, le cas échéant, l'~~Exportateur~~~~exportateur~~ de données sont tenus d'informer ces personnes de la ~~Violation~~~~violation~~ des données et de leur fournir des renseignements adéquats et utiles afin qu'elles sachent où s'adresser et quelles mesures prendre pour atténuer les effets néfastes de la violation des données.

Dans ces circonstances spécifiques, si la notification demandait un temps, des efforts et des ressources déraisonnable, l'~~Importateur~~~~importateur~~ des données peut demander la coopération ou l'assistance de l'~~Exportateur~~~~exportateur~~ des données pour produire les notifications et pour les mesures mentionnées au paragraphe précédent.

[Source : article 7 de la Convention et paragraphe 66 du rapport explicatif]

Lorsque la totalité de l'information relative à la ~~Violation~~~~violation~~ des données n'est pas disponible, la notification peut être effectuée « par étape », des informations complémentaires sur l'incident étant fournies dès que les Parties en disposent.

[Source : article 7 de la Convention et paragraphe 62 à 66 du rapport explicatif]

Clause 12. ~~Catégories spéciales de données~~~~données sensibles~~

Lorsque le transfert concerne des catégories spéciales de données ~~sensibles~~~~sensibles~~ sont transférées, l'~~Importateur~~~~importateur~~ de données applique des garanties supplémentaires adaptées aux risques courus ainsi qu'aux intérêts, aux droits et aux libertés à protéger.

Ces garanties doivent être de nature à prévenir les risques que le traitement de ~~catégories spéciales de données~~ ~~sensibles~~ peut présenter pour les intérêts, les droits et les libertés fondamentales de la personne concernée, notamment un risque de discrimination.

Les Parties ~~se sont mises d'accord sur les sauvegardes telles que décrites à l'annexe 4.~~
~~décrivent ces mesures à l'annexe 4.~~

[Source : article 6 de la Convention et paragraphes 56 à 61 du Rapport explicatif]

Clause 13. Transferts ultérieurs

L'~~Importateur~~importateur de données ne divulgue pas les données à caractère personnel à un tiers situé dans la juridiction d'un tiers sauf si ce tiers garantit un niveau de protection approprié conformément à l'article 14 de la Convention~~108+~~.

Sinon, un transfert ultérieur par l'~~importateur~~importateur de données peut avoir lieu si :

- (i) le destinataire est soumis à la juridiction d'un État dans lequel la loi, y compris les traités et accords internationaux applicables, garantissent un niveau approprié de protection, conformément à l'article 14(2) et l'article 14(3) (a) de la Convention ;
- (ii) le tiers conclut un acte légal contraignant et opposable avec l'~~Importateur~~importateur de données garantissant le même niveau de protection des données que celui qu'offrent les présentes Clauses, et si l'~~Importateur~~importateur de données communique une copie de ces garanties à l'~~Exportateur~~exportateur de données ;
- (iii) il est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice dans le cadre de procédures administratives, réglementaires ou judiciaires spécifiques ;
- (iv) il est nécessaire à la sauvegarde des intérêts vitaux de la ~~Personne~~personne concernée ou d'une autre personne physique ; ou,
- (v) lorsqu'aucune des autres conditions n'est applicable, l'~~Importateur~~importateur de données a obtenu le consentement explicite de la ~~Personne~~personne concernée en vue du transfert ultérieur dans une situation particulière, après l'avoir informée de la ou des finalités dudit transfert, de l'identité du destinataire et des risques éventuels que ledit transfert lui fait courir en raison de l'absence d'un niveau approprié de protection des données. Dans ce cas, l'~~Importateur~~importateur des données informe l'~~Exportateur~~exportateur des données du transfert ultérieur sur la base du consentement et, à la demande de ce dernier, lui transmet une copie des informations fournies à la ~~Personne~~personne concernée.

Pour tout transfert ultérieur, l'~~Importateur~~importateur de données doit respecter toutes les autres garanties au titre des présentes Clauses, en particulier en matière de limitation de la finalité.

Clause 14. Traitement effectué sous l'autorité de l'~~Importateur~~importateur de données

L'~~Importateur~~~~importateur~~ de données veille à ce que toute personne agissant sous son autorité, y compris un sous-traitant, traite les données uniquement selon ses instructions et conformément aux présentes Clauses.

Clause 15. Documentation et conformité

(...)

L'~~Exportateur~~~~exportateur~~ de données conserve en particulier une trace documentaire des activités de traitement des données menées sous sa responsabilité.

L'~~Exportateur~~~~exportateur~~ de données transmet ces informations à l'Autorité de contrôle compétente lorsque celle-ci en fait la demande.

L'~~Importateur~~~~importateur~~ de données prend toutes les mesures appropriées pour se conformer aux obligations énoncées dans les présentes ~~Clauses~~~~clauses~~ et pour pouvoir le démontrer à l'~~Autorité~~~~l'autorité~~ de contrôle compétente mentionnée à la Clause 19.

~~L'Importateurimportateur de données garantit qu'il a correctement pris en compte l'impact que le traitement de données envisagé pourrait avoir sur les droits et les libertés fondamentales des personnes concernées avant de commencer ce traitement, en fonction des circonstances du transfert particulier et qu'il a pris les mesures techniques et organisationnelles nécessaires pour respecter cette clause, examiné, préalablement au commencement du traitement de données envisagé, les effets potentiels dudit traitement sur les droits et les libertés fondamentales des Personnes concernées, et qu'il a conçu le traitement de données de manière à prévenir ou à minimiser les risques d'atteinte à ces droits et à ces libertés fondamentales.~~

~~L'Importateurimportateur de données prend des mesures d'ordre technique et organisationnel qui tiennent compte des incidences du droit à la protection des données à caractère personnel à tous les stades du traitement des données.~~

~~L'Importateurimportateur de données se conforme aux obligations mentionnées dans les précédents paragraphes au sujet des risques pesant sur les intérêts ainsi que sur les droits et les libertés fondamentales des personnes concernées, il adapte l'exécution desdites obligations en fonction de la nature et du volume des données, de la nature, de la portée et de l'objet du traitement et, s'il y a lieu, de la taille du responsable du traitement ou du sous-traitant.~~

[Source : ~~article~~~~clause~~ 10 de la Convention]

Clause 16. Droits des personnes concernées

L'~~Importateur~~~~importateur~~ de données, au besoin avec l'aide de l'~~Exportateur~~~~exportateur~~ de données, traite dans les meilleurs délais, et au plus tard dans un délai d'un mois à compter de

leur réception, toute demande de renseignements et autres demandes émanant de la ~~Personne~~ personne concernée au sujet du traitement de ses données à caractère personnel et de l'exercice de ses droits au titre des présentes ~~Clauses~~ clauses.

L'~~Importateur~~ importateur de données prend les mesures appropriées pour faciliter la réponse auxdites demandes et l'exercice des droits de la personne concernée. Toute information communiquée à la ~~Personne~~ personne concernée est présentée de manière intelligible et aisément accessible, et formulée en termes clairs et simples.

En particulier, l'~~Importateur~~ importateur de données lui octroie gratuitement les droits suivants :

(...)

- b) obtenir, à sa demande, à intervalle raisonnable, la confirmation d'un traitement de ~~Données~~ données à caractère personnel la concernant, la communication sous une forme intelligible des données traitées et toute information disponible sur leur origine, sur la durée de leur conservation ainsi que toute autre information que l'~~Importateur~~ importateur de données est tenu de fournir au titre de la transparence des traitements, conformément aux présentes clauses ;

(...)

- e) obtenir, à sa demande, sans frais et sans délai excessifs, la rectification de ces données ou, le cas échéant, leur effacement lorsqu'elles sont ou ont été traitées en violation des dispositions de la présente Convention et/ou du ~~Droit~~ droit applicable ;
- f) bénéficier, quelle que soit sa nationalité ou sa résidence, de l'assistance d'une autorité de contrôle au sens des présentes ~~Clauses~~ clauses pour l'exercice de ses droits au titre de ces dernières ;
- g) obtenir une copie des présentes ~~Clauses~~ clauses ;
- h) disposer d'une personne de référence auprès du personnel des deux Parties qui soit chargée de veiller au respect des alinéas a) à g) des présentes ~~Clauses~~ clauses. La ~~Personne~~ personne concernée pourrait s'adresser à elle à tout moment et sans frais à propos du traitement ou des transferts de données et, le cas échéant, obtenir son aide pour l'exercice de ses droits.

[Source : article 9 de la Convention et paragraphe 111 de l'exposé du rapport explicatif de la Convention]

Clause 17. Recours pour la Personne concernée

L'~~Importateur~~ importateur de données informe les personnes concernées, de façon transparente et facilement accessible, au moyen d'une notification individuelle ou sur son site web, d'un point

de contact autorisé à recevoir les demandes de personnes pour l'exercice de leurs droits et traiter les réclamations. Il traite sans délai toute réclamation reçue de la part d'une personne concernée.

[OPTION : L'~~Importateur~~~~importateur~~ de données convient que les ~~Personnes~~~~personnes~~ concernées peuvent en outre introduire une réclamation sans frais auprès d'un organe indépendant de règlement des litiges. Il informe la personne concernée, d'un tel mécanisme de recours et précise qu'elle n'est pas obligée de faire appel à ce dernier ni de suivre une chronologie spécifique pour demander réparation.]

L'~~Importateur~~~~importateur~~ de données ne peut proposer un règlement des litiges indépendant par une instance d'arbitrage que s'il est établi dans un pays qui a ratifié la Convention de New York pour la reconnaissance et l'exécution des sentences arbitrales étrangères.

La disposition alternative énoncée au paragraphe précédent n'exclut ni n'altère le droit de la personne concernée au titre des présentes ~~Clauses~~~~clauses~~, de la Convention et du ~~Droit~~~~droit~~ applicable, de déposer un recours auprès de(s) ~~L'Autorité~~~~l'autorité~~(s) de contrôle ou des juridictions compétentes. L'~~Importateur~~~~importateur~~ de données applique toute décision contraignante prise, conformément à la loi en vigueur.

Clause 18. Responsabilité

Chaque Partie 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~~~~clauses~~.

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

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

(...)

L'~~Importateur~~~~importateur~~ de données ne peut invoquer le comportement d'un sous-traitant ou d'un sous-traitant de sous-traitant pour s'exonérer de sa propre responsabilité.

(Source : paragraphe 22 du rapport explicatif)

Clause 19. Autorité de contrôle

La ou les ~~Autorité~~~~autorité~~ de contrôle chargée de veiller au respect par l'~~Exportateur~~~~exportateur~~ de données des dispositions du ~~Droit~~~~droit~~ applicable et de la Convention relatives au transfert de données agit en tant ~~qu'Autorité~~~~qu'autorité~~ de contrôle compétente.

Les Parties consentent par les présentes à ce que ~~L'Autorité~~~~l'autorité~~ de contrôle puisse exiger d'une quelconque des Parties qu'elle démontre l'effectivité des garanties prises y compris l'existence d'intérêts légitimes existants et que pour protéger les droits et les libertés fondamentales des ~~Personnes~~~~personnes~~ concernées, ~~L'Autorité~~~~l'autorité~~ puisse interdire ou suspendre les transferts ou les soumettre à conditions.

[Source : article 14.6 de la Convention]

Les Parties s'engagent à reconnaître la compétence de ~~L'Autorité~~~~l'autorité~~ de contrôle et à ne contester ni son autorité, ni sa compétence telle qu'établie par le ~~Droit~~~~droit~~ applicable ou les présentes ~~Clauses~~~~clauses~~, ni aucune autre action, y compris toute forme de coopération entre ~~Autorités~~~~autorités~~ de contrôle conformément au ~~Droit~~~~droit~~ applicable et aux articles 15 et 17 de la Convention.

[Source : articles 15 et 17 de la Convention]

L'~~Importateur~~~~importateur~~ de données s'engage à reconnaître la compétence de ~~L'Autorité~~~~l'autorité~~ de contrôle et à coopérer avec elle dans le cadre de toute procédure visant à garantir le respect des présentes ~~Clauses~~~~clauses~~. Il accepte en particulier de répondre aux demandes de renseignements, de se soumettre à des audits et de se conformer aux mesures adoptées par ladite ~~Autorité~~~~autorité~~, notamment aux mesures correctives et compensatoires. Il confirme par écrit à ~~L'Autorité~~~~l'autorité~~ de contrôle que les mesures nécessaires ont été prises.

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

Clause 20. Législations et pratiques locales ayant une incidence sur le respect des Clauses

- a) Les Parties garantissent qu'elles n'ont aucun motif de croire que, dans ~~le pays de destination~~~~, un Tiers de destination~~, la législation et les pratiques applicables au traitement des données à caractère personnel par l'~~Importateur~~~~importateur~~ de données, notamment toute obligation de les divulguer ou toute mesure d'autorisation d'accès des autorités publiques, empêchent l'~~Importateur~~~~importateur~~ de remplir les obligations qui lui incombent au titre des présentes ~~Clauses~~~~clauses~~. Cela devrait inclure la responsabilité pleine et solidaire pour tout dommage matériel et immatériel ou affectant les ~~Personnes~~~~personnes~~ concernées causé par les Parties en relation avec l'~~utilisation~~ des présentes ~~Clauses~~~~clauses~~.

- b) Cette disposition repose sur l'idée que dès lors que des exceptions spécifiques aux présentes ~~Clauses~~clauses qui sont prévues par le ou les ~~Droit~~droit applicable, 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 (1) de la Convention, elles ne contredisent pas les présentes ~~Clauses~~clauses.

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

- i) les circonstances particulières du transfert, parmi lesquelles l'étendue de la chaîne de traitement, le nombre d'acteurs concernés et les canaux de transmission utilisés ; les transferts ultérieurs prévus ; le type de destinataire ; la finalité du traitement ; les catégories et le format des données à caractère personnel transférées ; le secteur économique dans lequel le transfert a lieu et le lieu de stockage des données transférées ;
 - ii) les législations et pratiques 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 ;
 - iii) toute garantie d'ordre contractuel, technique ou organisationnel pertinente, mise en place pour compléter les garanties prévues par les présentes ~~Clauses~~clauses, y compris les mesures appliquées pendant la transmission et relatives au traitement des données à caractère personnel dans le pays de destination.
- c) L'~~Importateur~~importateur de données garantit qu'il a procédé à l'évaluation au titre du paragraphe b) en apportant la diligence et les efforts nécessaires pour fournir à l'~~Exportateur~~exportateur de données des informations ~~[problèmes]~~[A3] pertinentes, et il s'engage à continuer de coopérer avec l'~~Exportateur~~exportateur de données pour veiller au respect des présentes ~~Clauses~~clauses.
- d) Les Parties conviennent de conserver une trace documentaire de l'évaluation visée au paragraphe b) et de mettre cette évaluation à la disposition de l'autorité de contrôle compétente si celle-ci en fait la demande.
- e) L'~~Importateur~~importateur de données accepte d'informer rapidement l'~~Exportateur~~exportateur de données si, après avoir souscrit aux présentes ~~Clauses~~clauses et pendant la durée du contrat, il a des raisons de croire qu'il est ou est devenu soumis à une législation ou à des pratiques qui ne sont pas conformes aux exigences énoncées au paragraphe a), notamment à la suite d'une modification de la législation ~~d'un État tiers~~du pays de destination ou d'une mesure (par exemple une demande de divulgation) indiquant que l'application pratique de ladite législation n'est pas conforme aux exigences du paragraphe a).

- f) À la suite d'une notification faite en application du paragraphe e), ou si l'~~Exportateur~~~~exportateur~~ de données a des raisons de croire que l'~~Importateur~~~~importateur~~ de données ne peut plus remplir les obligations qui lui incombent au titre des présentes ~~Clauses~~~~clauses~~, l'~~Exportateur~~~~exportateur~~ de données détermine rapidement les mesures appropriées (par exemple des mesures d'ordre technique ou organisationnel permettant d'assurer la sécurité et la confidentialité) qu'il doit adopter et/ou qui doivent être adoptées par l'~~Importateur~~~~importateur~~ de données pour remédier à la situation. L'~~Exportateur~~~~exportateur~~ de données suspend le transfert de données s'il considère qu'aucune garantie adaptée à un tel transfert ne peut être fournie ou si l'autorité de contrôle compétente lui donne pour instruction de le suspendre. Dans ce cas, l'~~Exportateur~~~~exportateur~~ de données est en droit de résilier le contrat pour autant que celui-ci porte sur le traitement de données à caractère personnel dans le cadre des présentes ~~Clauses~~~~clauses~~. Si le contrat concerne plus de deux Parties, l'~~Exportateur~~~~exportateur~~ de données peut exercer son droit de résiliation à l'égard uniquement de la Partie concernée sauf accord contraire entre les Parties. Si le contrat est résilié conformément à la présente ~~Clause~~~~clause~~, les alinéas d) et e) de la ~~Clause~~~~clause~~ 23 s'appliquent.

Clause 21. Obligations de l'~~Importateur~~~~importateur~~ de données en cas d'accès des autorités publiques

Notification

- a) L'~~Importateur~~~~importateur~~ de données convient d'informer sans délai l'~~Exportateur~~~~exportateur~~ de données et, s'il y a lieu et si possible, la Personne concernée (si nécessaire avec l'aide de l'~~Exportateur~~~~exportateur~~ de données) :
- i) s'il reçoit de la part d'une autorité publique, notamment judiciaire, conformément à la législation du pays de destination, une demande juridiquement contraignante de divulgation des ~~Données~~~~données~~ à caractère personnel transférées au titre des présentes ~~Clauses~~~~clauses~~ ; cette notification comprend des informations sur les données à caractère personnel demandées, l'autorité requérante, la base juridique de la demande et la réponse fournie ; ou
 - ii) s'il a connaissance d'un accès direct, quel qu'il soit, des autorités publiques aux données à caractère personnel transférées au titre des présentes ~~Clauses~~~~clauses~~ conformément à la législation du pays de destination ; cette notification comprend toutes les informations dont l'~~Importateur~~~~importateur~~ dispose.

- b) Si la législation du pays de destination interdit à l'~~Importateur~~~~importateur~~ de données d'informer l'~~Exportateur~~~~exportateur~~ de données et/ou la personne concernée, l'~~Importateur~~~~importateur~~ de données convient de tout mettre en œuvre pour obtenir une levée de cette interdiction afin de communiquer autant d'informations que possible, dans les meilleurs délais. Il accepte de conserver une trace documentaire des mesures qu'il a prises afin de pouvoir en apporter la preuve à l'~~Exportateur~~~~exportateur~~ de données si celui-ci en fait la demande.
- c) Lorsque la législation du pays de destination l'autorise, l'~~Importateur~~~~importateur~~ de données accepte de fournir à l'~~Exportateur~~~~exportateur~~ de données, à sa demande~~intervalles réguliers pendant toute la durée du contrat~~, autant d'informations utiles que possible sur les demandes reçues (en particulier le nombre de demandes, le type de données demandées, la ou les autorités requérantes, la contestation ou non des demandes et l'issue de la contestation, etc.).
- d) L'~~Importateur~~~~importateur~~ de données accepte de conserver les informations visées aux paragraphes a) à c) pendant toute la durée du contrat et de les transmettre à l'autorité de contrôle compétente si celle-ci en fait la demande.
- e) Les paragraphes a) à c) sont sans préjudice de l'obligation incombant à l'~~Importateur~~~~importateur~~ de données, conformément à la clause 20.e et à la Clause 22, d'informer sans délai l'~~Exportateur~~~~exportateur~~ de données s'il n'est pas en mesure de respecter les présentes ~~Clauses~~~~clauses~~.

Contrôle de la légalité et minimisation des données

- a) L'~~Importateur~~~~importateur~~ de données accepte de contrôler la légalité de la demande de divulgation, en particulier de vérifier si elle entre dans les limites des pouvoirs conférés à l'autorité publique requérante et de la contester si, après l'avoir attentivement évaluée, il conclut qu'il existe des motifs raisonnables de considérer qu'elle est contraire à la législation du pays de destination, aux obligations applicables en vertu du droit international et des principes de la courtoisie internationale. L'~~Importateur~~~~importateur~~ de données exerce dans les mêmes conditions les possibilités de recours prévues. Lorsqu'il conteste une demande, l'~~Importateur~~~~importateur~~ de données sollicite des mesures provisoires destinées à suspendre les effets de la demande jusqu'à ce que l'autorité judiciaire compétente se soit prononcée sur son bien-fondé. Il ne divulgue pas les données à caractère personnel demandées tant qu'il n'est pas obligé de le faire au titre des règles de procédure applicables. Ces exigences sont sans préjudice des obligations incombant à l'~~Importateur~~~~importateur~~ de données en application de l'alinéa e de la Clause 20.

- b) L'~~Importateur~~~~importateur~~ de données accepte de conserver une trace documentaire de l'évaluation juridique qu'il a effectuée et de toute contestation de la demande de divulgation et, dans la mesure où la législation du pays de destination le permet, de mettre les documents concernés à la disposition de l'~~Exportateur~~~~exportateur~~ de données. Il les met également à la disposition de l'autorité de contrôle compétente si celle-ci en fait la demande.
- c) L'~~Importateur~~~~importateur~~ de données convient de fournir le minimum d'informations autorisé lorsqu'il répond à une demande de divulgation, sur la base d'une interprétation raisonnable de ladite demande.

SECTION IV – DISPOSITIONS FINALES

Clause 22. Non-respect des ~~Clauses~~~~clauses~~ et résiliation

- a) ~~Chaque~~Les Parties s'informent sans délai l'autre si elles n'este-sont pas en mesure de respecter les présentes ~~Clauses~~~~clauses~~, pour quelque raison que ce soit.
- b) Si l'~~Importateur~~~~importateur~~ de données enfreint les présentes ~~Clauses~~~~clauses~~ ou n'est pas en mesure de les respecter, l'~~Exportateur~~~~exportateur~~ de données suspend le transfert de ~~Données~~~~données~~ à caractère personnel vers l'~~Importateur~~~~importateur~~ de données jusqu'à ce que le respect des présentes ~~Clauses~~~~clauses~~ soit de nouveau garanti ou que le contrat soit résilié. La présente disposition est sans préjudice de l'alinéa f) de la ~~Clause~~~~clause~~ 20.
- c) L'~~Exportateur~~~~exportateur~~ de données est en droit de résilier le contrat, pour autant que celui-ci concerne le traitement de données à caractère personnel au titre des présentes clauses, lorsque :
 - i) l'~~Exportateur~~~~exportateur~~ de données a suspendu le transfert de données à caractère personnel vers l'~~Importateur~~~~importateur~~ de données conformément au paragraphe b) et que le respect des présentes ~~Clauses~~~~clauses~~ n'est pas rétabli dans un délai raisonnable et, en tout état de cause, dans un délai d'un mois à compter de la suspension ;
 - ii) l'~~Importateur~~~~importateur~~ de données enfreint les présentes clauses de manière grave ou persistante ; ou
 - iii) l'~~Importateur~~~~importateur~~ de données ne respecte pas une décision contraignante d'une juridiction ou d'une autorité de contrôle compétente en ce qui concerne les obligations lui incombant au titre des présentes ~~Clauses~~~~clauses~~.

Dans ces cas, il informe l'autorité de contrôle compétente de ce non-respect. Si le contrat concerne plus de deux Parties, l'~~Exportateur~~~~exportateur~~ de données ne peut exercer ce droit de résiliation qu'à l'égard de la Partie concernée sauf accord contraire entre les Parties.

- d) Les données à caractère personnel qui ont été transférées avant la résiliation du contrat conformément au paragraphe c) sont immédiatement restituées à l'~~Exportateur~~~~exportateur~~ de données ou intégralement effacées, à la convenance de celui-ci. Il en va de même pour toute copie des données.

L'~~Importateur~~~~importateur~~ de données apporte à l'~~Exportateur~~~~exportateur~~ de données la preuve de l'effacement des données. Jusqu'à ce que les données soient effacées ou restituées, l'~~Importateur~~~~importateur~~ de données continue de veiller au respect des présentes ~~Clauses~~~~clauses~~. Lorsque la législation locale applicable à l'~~Importateur~~~~importateur~~ de données interdit la restitution ou l'effacement des données à caractère personnel transférées, ce dernier garantit qu'il continuera à respecter les présentes ~~Clauses~~~~clauses~~ et qu'il ne traitera les données que dans la mesure où et aussi longtemps que cette législation locale l'exige.

- e) Chaque Partie peut révoquer son consentement à être liée par les présentes ~~Clauses~~~~clauses~~ lorsque l'autorité de contrôle adopte, [en vertu du droit applicable, une décision couvrant le transfert de données à caractère personnel auquel les présentes clauses s'appliquent]. Cela est sans préjudice des autres obligations qui s'appliquent au traitement en question en vertu du ~~Droit~~~~droit~~ applicable.

Clause 23. Droit applicable

Les présentes clauses sont régies par le droit du pays de l'~~Exportateur~~~~exportateur~~ de données sous réserve que ce droit reconnaisse des droits au tiers bénéficiaire.

Clause 24. Choix des juridictions compétentes

Tout litige survenant du fait des présentes clauses est tranché par les juridictions de [____].

En outre, une personne concernée peut engager des poursuites contre l'~~Exportateur~~~~exportateur~~ et/ou l'importateur de données devant les juridictions du pays dans lequel elle a sa résidence habituelle. Les Parties acceptent de se soumettre à la compétence de ces juridictions.

[OPTION Clause 25. Arbitrage]

[OPTION 1]

Tout litige, controverse ou réclamation entre les Parties, découlant des présentes Clauses ou s'y rapportant, et ayant trait notamment mais non exclusivement à sa formation, sa validité, ses effets obligatoires, son interprétation, son exécution, sa violation ou sa résolution, de même que toute réclamation extracontractuelle, sera soumis à arbitrage pour règlement définitif, conformément au Règlement d'arbitrage de l'OMPI. Le tribunal arbitral sera composé [d'un arbitre unique] [de trois arbitres]. Le lieu de l'arbitrage sera [préciser le lieu]. La langue de la procédure d'arbitrage sera [préciser la langue]. Il sera statué sur le litige, la controverse ou la réclamation conformément au droit ~~[préciser le pays/territoire]~~~~du pays de~~ l'~~Exportateur~~~~exportateur~~ des données.

[CLAUSE DE L'OMPI – Clause d'arbitrage uniquement pour des conflits B2B]

[Source : adaptation de <https://www.wipo.int/amc/fr/Clauses/arbitration/index.html>]

Source https://www.wipo.int/amc/fr/center/specific-sectors/b2b_data/

Les alternatives mentionnées au paragraphe ci-dessus n'excluent en rien ni n'altèrent le droit des personnes concernées garanti par les présentes ~~Clauses~~~~clauses~~, par la Convention et le droit applicable de déposer toute plainte auprès de la ou des autorités de contrôle ou des cours de la juridiction concernées.

[OPTION 2]

(...)

Les alternatives mentionnées au paragraphe ci-dessus n'excluent en rien ni n'altèrent le droit des personnes concernées garanti par les présentes ~~Clauses~~~~clauses~~, par la Convention et le droit applicable de déposer toute plainte auprès de la ou des ~~Autorité~~~~autorité~~ de contrôle ou des cours de la juridiction concernées.

Clause 26. Dispositions générales

(...)

Cession. Le présent accord ne peut être cédé par l'~~Importateur~~~~importateur~~ de données ou de plein droit à aucune personne physique ou morale sans l'approbation expresse donnée par écrit de l'~~Exportateur~~~~exportateur~~ de données.

(...)

Divisibilité. Si l'une des dispositions énoncées dans les présentes ~~Clauses~~~~clauses~~ est jugée nulle par la juridiction compétente désignée par les Parties aux présentes ~~Clauses~~~~clauses~~, cette disposition sera considérée comme étant à reformuler pour se rapprocher le plus possible de l'intention initiale dans le respect de la Convention et du ~~Droit~~~~doit~~ applicable, et le reste du présent accord reste en vigueur et de plein effet.

Intégralité de l'Accord. Aucune déclaration de quelque nature qu'elle soit de l'une ou l'autre des Parties qui ne soit pas expressément énoncée dans les présentes n'aura force obligatoire pour la Partie concernée. Les Parties conviennent que les présentes ~~Clauses~~~~clauses~~ constituent l'intégralité du présent accord entre elles et remplacent toute proposition, orale ou écrite, et toute autre communication entre elles liée aux stipulations des présentes.

(...)

Annexe 1

Informations sur le transfert

Description du transfert : [...]

Finalité(s) du transfert : [...]

Informations complémentaires : [...]

DRAFT DOCUMENT

Annexe 2

Formulaire d'adhésion

Accord n° [xx/2022]

Désignation : [Exportateur de données] ou [Importateur de données]

Nom de l'entreprise :

Adresse :

Ville, pays, code postal :

Courrier électronique :

Par la signature ci-dessous de ses représentants autorisés, [Dénomination de la Société] indique être d'accord de devenir Partie aux présentes Clauses-clauses avec effet immédiat et s'engage à respecter les Clauses-clauses contractuelles relatives au transfert international de données [de responsable du traitement à responsable du traitement] OU [de responsable de traitement à sous-traitant].

Nom :

Fonction : [xxxx]

Date de signature [xxxx]

Annexe 3

Mesures de sécurité

[La présente annexe doit être complétée et actualisée par l'Importateur de données]

[Exemples de mesures possibles :

Mesures de pseudonymisation et de cryptage des données à caractère personnel

Mesures pour assurer la permanence de la confidentialité, de l'intégrité, de la disponibilité et de la solidité des systèmes de traitement et des services

Mesures pour assurer la possibilité de restaurer la disponibilité des données à caractère personnel et leur accès rapidement dans le cas d'incidents physiques ou techniques.

Procédures pour tester, mesurer et évaluer régulièrement l'effectivité des mesures techniques et d'organisation afin de garantir la sécurité du traitement

Mesures d'identification et d'autorisation

Mesures de protection des données pendant la transmission

Mesures de protection des données pendant au long de la conservation

Mesures pour assurer la sécurité physique des locaux où sont traitées les données à caractère personnel

Mesures pour enregistrer les événements

Mesures de configuration des systèmes, y compris la configuration par défaut

Mesures de gouvernance et de gestion de l'informatique interne et de la sécurité informatique

Mesures de certification/d'assurance des procédures et des produits

Mesures pour assurer la minimisation des données

Mesures pour assurer la qualité des données

Mesures pour assurer la limitation de la conservation des données

Mesures pour assurer la responsabilité

~~Mesures pour permettre la portabilité des données et garantir l'effacement]~~

Annexe 4

Mesures pour les ~~catégories spéciales de~~ données] sensibles

[Ces sauvegardes peuvent inclure, par exemple, seules ou de façon cumulée

- i) le consentement explicite de la personne concernée au traitement des données sensibles ;
- ii) une obligation du secret professionnel ;
- iii) des mesures découlant d'une analyse de risques ;
- iv) une mesure particulière et qualifiée en matière d'organisation ou de sécurité technique (par exemple, cryptage des données, pseudonymisation) ;
- v) retenir le personnel habilité à accéder aux données sensibles ;
- vi) restrictions supplémentaires pour des accès ultérieurs en fonction de la nature des données]

Annexe 5

LISTE DES SOUS-TRAITANTS

*[SEULEMENT POUR LES MODULES 2 ET 3, à rédiger après avoir finalisé le modèle C2C
La présente annexe doit être complétée par les Parties
si elles conviennent d'autoriser préalablement des sous-traitants]*

~~[1] Sans préjudice du fait que les présentes Clauses peuvent, après leur adoption par le Comité de la Convention 108, être soumises à une approbation d'une autorité de contrôle ou tout autre organe ou institution compétent, sur la base de la loi nationale.~~

[A1] Commentaire : cette partie est-elle réellement nécessaire ? mon opinion est qu'elle pourrait être supprimée mais je suis d'accord pour qu'elle reste.

[A2] Je pense que cela ne s'applique pas à ce sujet.

[A3] Y compris ceux qui dépassent les simples risques liés au transfert de données

EUROPEAN COMMISSION

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA CONVENTION 108

Standard Contractual Clauses for Transborder Flows

(...)

STANDARD CONTRACTUAL CLAUSES

(...)

Model Contractual Clauses for Transborder Data Flows of Personal Data

Commented [A43]: We would like to suggest another wording for the title of these clauses. The advantage of doing this is that it makes sure we have a title that differs from EU SCCs so we cannot mix them up with them.. We think sticking to the previous title: "Model clauses" (from 1992) could help.

Option 1: Model Clauses for Transborder Data Flows of Personal Data

Or we could innovate and opt for a new title:
Option 2: Standard Data Protection Clauses for Transborder Data Flows of Personal Data (this is closer to the current title but still distinguishes it from the EU SCCs)

Commented [A44]: Please see comment above which would require a change throughout the document, if accepted.

Commented [A45]: Below you sometimes use "Model Contractual Clauses" and sometimes "Model Clauses" (without "Contractual") – should be aligned across the document

Commented [A46]: Seems a bit redundant ("data flows of ... data"), do we need the "of Personal Data". Also (here and below), do we really need to use this language of "transborder data flows" (below you then also use "transfer", which to me sounds like the better term)

COUNCIL OF EUROPE

CONVENTION 108+

Model Clauses for Transborder Data Flows of Personal Data

Agreement number [xx/2022]

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

Data exporter information

Name:
Address:
City, Country, zip code:
Email:

Data importer information

Name:
Address:
City, Country, zip code:
Email:

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

Data exporter

By:
Signature Date [MM/DD/YEAR]

Data importer

Signature Date [MM/DD/YEAR]

NOTE: These Model clauses provide an appropriate level of protection for the transfer of personal data to non-Parties of Modernised Convention 108 in accordance with Article 14(3) (b) of Modernised Convention 108.

Commented [A47]: We should be careful with the term "Agreement": those are model contract clauses ("the Clauses") that can (and typically will) form part of a wider commercial agreement". "Agreement" is not a defined term under these Clauses.

Commented [A48]: At the very end of these Clauses reference is made to the "Term" of the "Agreement". In case this is considered important for the Clauses, here only the word "term" (and not also "duration") should be used (or everywhere the word "duration" – basically, the language should be harmonised/aligned).

Commented [A49]: Or: "appropriate level of protection for personal data transferred to..."

Commented [A50]: This is not a defined term (as below you defined the modernised Convention as the "Convention")

MODEL CONTRACTUAL CLAUSES

Model clauses for the transborder flow of personal data from controller to controller

The **data exporter** and the data importer (hereinafter, the Parties) agree to these Model clauses (hereinafter the Clauses):

SECTION I - GENERAL CLAUSES

Clause 1. Purpose and scope

1.1. The aim of these model clauses is to ensure compliance with the requirements for the transfer of personal data to a non-Party under Convention 108+ (hereinafter the Convention).

When adopted and implemented by the Parties, these Model clauses provide an appropriate level of protection for the transfer of personal data in accordance with Article 14(3)(b) of the Convention.

1.2. Description of the transfer

These Clauses shall apply to the transfer of personal data described in Annex 1.

1.3. Purpose of the transfer

The purpose and additional details of the transfer of personal data are described in Annex 1.

Clause 2. Definitions

[Note: Apart from the sources cited in each defined term, see also document T-PD(2020)06rev3, [Interpretation of provisions, May 7, 2021](#)].

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.

Biometric data: data resulting from a specific technical processing of data concerning the physical, biological or physiological characteristics of a **human** person that allows the unique identification or authentication of such individual.

[Source: Para. 58 of the Explanatory Report].

(...)

Commented [A51]: Above you changed back to "data exporter" and "data importer" (without capitals) – there should be one uniform way to use defined terms across the document (in my view: without capitals)

Commented [A52]: This is fine, but why do we then still need the "Note" on the top of this page, which says the same? Would delete that "Note"

Commented [A53]: It needs to be decided how to refer to subsections in each clause. Here you use 1.2, 1.3 with subtitles (same in Clause 3), whereas in other places (e.g. Clause 1.1, Clause 8) you only use the numbers without subtitles. Finally, in some Clauses (e.g. 20-22), letters (a, b, etc.) are used instead of numbers. There should be one approach that is applied throughout the text.

Commented [A54]: "natural"?

Data importer: the controller or processor located in a non-Party to whom the data exporter transfers personal data under these Clauses.

Data exporter: the controller or processor located in a country that is a member of the Convention and that transfers personal data to a data importer.

Commented [A55]: Would reverse the order

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

Commented [A56]: Would suggest linking to this to the definition of "personal data"

[Source: Article 2 of the Convention and para. 15 of the Explanatory Report]

(...)

Transborder flows of personal data: the transfer, making available or disclosure of personal data to a recipient subject to the jurisdiction of another State.

Commented [A57]: As indicated above, in my view it would be better to use "transfer" as the defined term (which could be defined as "the disclosure or otherwise making available of personal data..." (see also the definition of "recipient").

[Source: Article 14 of the Convention, Paras 102 to 104 of the Explanatory report, and the legal opinion provided by the Legal Advisor DLAPIL02/2021_JP/DG3]

Non-Party: a country that has not ratified the Convention or where it is not yet in force.

"Transfer" is also the term used throughout the Clauses (e.g. in Clause 1.2 and 1.3), whereas "transborder flows of personal data" is only used to refer to the title of these Clauses. It would therefore make sense to only use "transfer" and define it as above.

[Source: Article 26.3 of the Convention]

(...)

Party (or Parties): each of the signatories of these Clauses.

Commented [A58]: Seems strange: what about simply saying "a country where the Convention is not in force" (or "... that is not bound by the Convention")?

(...)

Commented [A59]: Or: "each signatory" (or: "the data exporter(s) and data importer(s) that are signatories of these Clauses")

Third party beneficiary: the data subject whose personal data is the object of transborder data flows under these Clauses.

Commented [A60]: "a transfer"

Clause 3. General clauses

Commented [A61]: Does this mean that all Clauses create third-party beneficiary rights? The relevance of this definition is not clear

3.1. Invariability of the Clauses

(...)

3.2 Interpretation

(...)

Clause 4. Accession clause

Commented [A62]: Should this always be included, or could it be an optional 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 Annex 2, and, if required, updating the description of the transfer in Annex 1.

(...)

SECTION II – RIGHTS AND OBLIGATIONS OF THE PARTIES

Clause 6. Data protection safeguards

(...)

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.

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

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:

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

(...)

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) (d) of the Convention]

(...)

Commented [A63]: There appears to be no longer any reference to “third-party beneficiary rights” in the text, EXCEPT for the liability clause (which therefore no longer makes sense). The Clauses should make clear that either all or at least certain Clauses create third-party beneficiary rights (and thus can be invoked by the data subject), as they did in previous versions of the document.

In any event, this cross-reference does not seem to be correct, as Clause 25 is about arbitration.

Commented [A64]: Should this be Clause 5?

Commented [A65]: To be considered whether there should a possibility for the importer (in a C-C scenario) to also process for other purposes, e.g. on the basis of consent or where necessary for legal claims.

Commented [A66]: Why this information and not the contact details? Not sure whether knowing the country/place where the importer is located will enable the individual to contact it.

Commented [A67]: Art 5(4)(c) rather says “not excessive”

Clause 11. Data security

(...)

In addition, the data importer shall notify, without delay, at least the data exporter of those data breaches which may interfere with the rights and fundamental freedoms of data subjects, who shall then without delay notify the competent supervisory authority. The Notification shall include (i) a description of the data breach and its likely consequences, (ii) information on any measures taken and/or proposed to address the breach and its likely consequences.

Commented [A68]: Added from the paragraph below, which to a large extent overlaps

In the event of a data breach that may seriously interfere with the rights and fundamental freedoms of data subjects (e.g. data breaches involving the disclosure of data covered by professional confidentiality, or special categories of data, or which may result in financial, reputational, or physical harm or humiliation), the data importer shall notify without delay the data exporter and the relevant supervisory authority/es 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 [A69]: Competent?

[Source: Para. 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 where applicable the data exporter, shall notify the data subjects concerned by the data breach and provide them with adequate and meaningful information on, notably, the contact points, the nature of the data breach and its likely consequences, and possible measures they could take to mitigate these adverse effects.

Commented [A70]: Not clear what is the difference to the previous paragraph, which already foresees notification of the data exporter (that shall then inform the supervisory authority), but for which a lower threshold (interference with the rights and fundamental freedoms) applies. The only difference appears to be that the data importer would have to directly inform the supervisory authority (plus more details on the content of the notification) – is that intended? Perhaps better to delete this paragraph

Commented [A71]: How does this relate to the examples of “serious interference” in the previous paragraph?

Commented [A72]: Not clear WHEN this would be applicable. It might be better to indicate that this is a responsibility of the data importer, “where appropriate together with” the data exporter

In specific circumstances, where the notification would require disproportionate effort or resources, the data importer may seek the cooperation or the assistance of the data exporter to produce the notifications and measures in the previous paragraph.

Commented [A73]: However, also the data exporter might be unable to notify/help with the notification, for instance in cases when it has not collected the data directly from the individuals concerned (whom the data exporter might not know). There should therefore be an exception from individual notification (at least) in case this would involve disproportionate effort – in which case there should instead be some form of public communication whereby data subjects are informed (see Art 34(3)(c) GDPR)

[Source: Article 7 of the Convention & Para. 66 of the Explanatory Report]

(...)

Clause 12. Special categories of data

(...)

Clause 13. Onward transfers

The Data importer shall not disclose the personal data to a third party located in a non-Party unless the third party is subject to the jurisdiction of a State that has been formally recognised,

Commented [A74]: Shouldn't there also be the possibility to use these clauses (i.e. the third party becomes a party to these clauses)?

by the jurisdiction of the Data exporter, as ensuring an appropriate level of protection in line with Article 14(2), (3)(a) of the Convention.

Otherwise, an Onward transfer by the Data importer may only take place if:

(...)

Clause 14. Processing under the authority of the Data importer

(...)

Clause 15. Documentation and compliance

(...)

The data importer guarantees that it has paid due regard to the impact the intended data processing might have on the rights and fundamental freedoms of data subjects prior to the commencement of such processing according to the circumstances of the specific transfer and has taken the necessary technical and organisational measures to comply with the clause.

[Source article 10 of the Convention]

Clause 16 – Rights of data subjects

(...)

The data subject shall have the following rights, to be granted free of charge:

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

(...)

- e) to obtain, on request, rectification or erasure, as the case may be, of such data if these are being, or have been, processed contrary to the provisions of these Clauses and/or the applicable law;

- f) to obtain a copy of these Clauses.

[Source: Article 9 of the Convention and para. 111 of the Explanatory Memorandum of Convention]

Commented [A75]: Not clear to me why the original text has been changed, and in particular why the text has moved from an obligation ("shall") to a "guarantee". Would suggest reverting back to the earlier text

Commented [A76]: Should there not be a possibility to apply restrictions/exceptions in certain situations, e.g. if allowed under the laws of the country of destination, the essence of the fundamental rights and freedoms are respected and the restriction/exception constitutes a necessary and proportionate measure in a democratic society for the purposes/objectives listed in Article 11(1) of Convention 108+?

Commented [A77]: Should the Clauses also foresee the scenario where automated decision-making is authorised by a law to which the data importer is subject, which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests (Article 9(2) of Convention 108+)?

Commented [A78]: TBD whether this makes sense

Commented [A79]: This cannot be regulated in a contract between private parties (unlike in Art 9 of the Convention)

Commented [A80]: Wouldn't it make sense to allow the Parties to redact (parts of) the annexes if they contain trade secrets or other confidential information (in which case they could still be required to provide a meaningful summary to the individual).

Commented [A81]: It seems to make little sense to regulate this as a right, given that the exercise of this right would already presuppose knowledge of that contact person. I would suggest moving this into Clause 17 (which already covers the contact point)

Clause 17. Redress for the data subject

(...)

The alternative mentioned in the paragraph above does not exclude or alter the right of the data subject afforded by these Clauses, the Convention and the applicable law to lodge a complaint at the supervisory authority/ies or at the courts of the applicable jurisdiction. The data importer shall abide by a decision that is binding under the applicable law.

Clause 18. 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 these Clauses and the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under the applicable law.

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 claim compensation against any of these Parties.

(...)

Clause 19. Supervisory authority

(...)

(...)

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

Clause 20. Local laws and practices affecting compliance with the Clauses

- a) The Parties warrant that they have no reason to believe that the laws and practices in the 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. This is based on the understanding that specific exceptions to these Clauses based on applicable law(s) that respect the essence of the human rights and

Commented [A82]: This is not very helpful: the Convention as such will not create any rights, including the right to judicial redress (it will typically not be directly applicable), and it seems that at least this provision is not creating a right to redress under the Clauses either (as it merely “does not exclude or alter” rights supposedly granted elsewhere). Applicable law, i.e. the law of the data exporter, will normally not give the individual any rights against the data importer (who is situated in another jurisdiction).

Instead, there should be a provision by which the Parties recognise a right to (judicial) redress against the data importer to the data subject. In order to make this work, the data importer should submit itself to the jurisdiction of the supervisory authority and courts in the jurisdiction of the data exporter (as the data subject cannot be expected to effectively exercise his/her rights in the jurisdiction of the data importer; also, only then does the last sentence – “The data importer shall abide by a decision that is binding under the applicable law” – make sense)

Commented [A83]: See earlier comment(s) regarding third-party beneficiary rights – if ALL Clauses create third-party beneficiary rights, it would be sufficient to say “by breaching these Clauses”; otherwise something like “by breaching any of the Clauses that create third-party beneficiary rights” should be used

Commented [A84]: Going to court is the last resort, in case the responsible Party does not pay compensation voluntarily

Commented [A85]: Art 14(6) is a provision specifically for the data exporter (and it covers the various transfer tools under Art 14, not just transfers based on appropriate safeguards ensured through contractual clauses). As regards the data exporter, Art 14(6) is already ensured through its transposition into the Applicable law. Would suggest deleting

Commented [A86]: Not clear what this means, and how it relates to the first sentence (which is about third country laws/practices, not “damages made by the Parties”, and based on a “no reason to believe” standard rather than “objective” liability without fault).

Commented [A87]: Not clear what is meant with “specific exceptions... based on applicable laws” – why not refer again to “laws and practices” as in lit (a)?

fundamental freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 11(1) of the Convention, are not in contradiction with these Clauses.

(...)

- e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the country of destination or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

- f) (...)

Commented [A88]: Above, I have changed the numbering, as otherwise the reference would have to be to paragraph (b)

Clause 21. 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 possible the data subject promptly (if necessary, with the help of the data exporter) if it:

(...)

Commented [A89]: Not clear what is meant with "where applicable" (no criteria are given) – would suggest only using "to the extent possible" (or, better, "where possible", since a notification is either possible or not, rather than being partly possible as suggested by "to the extent")

Review of legality and data minimisation

(...)

SECTION IV – FINAL PROVISIONS

(...)

- (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 [A90]: This will of course only work in case the Applicable law provides for such a decisions (which might not necessarily be adopted by the supervisory authority, as there could be other competent authorities). Would suggest deleting this paragraph

Commented [A91]: What if that is not the case? There should be text addressing this situation.

Would suggest rephrasing this Clause:

[OPTION 1 (in case the Applicable law provides for third-party beneficiary rights):] These Clauses shall be governed by the law of the country of the Data Exporter.

[Option 2 (in case the conditions for OPTION 1 are not fulfilled):] These Clauses shall be governed by the law of _____. The Parties have verified that such law allows for third-party beneficiary rights.

Clause 23. Governing law

These Clauses shall be governed by the law of the country of the data exporter, provided such law allows for third-party beneficiary rights.

Clause 24. Choice of forum and jurisdiction

(...)

The Parties agree to submit themselves to the jurisdiction of such courts.

Commented [A92]: Should this not be a general provision that applies to both sentences? Therefore moved down.

[OPTIONAL Clause 25. Arbitration]

[OPTION 1]

Any dispute, controversy or claim between the Parties arising under, out of or relating to these Clauses including, without limitation, their interpretation, performance, breach or termination, as well as non-contractual claims, shall 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 Governing law.

Commented [A93]: The reference point are "these Clauses"

Commented [A94]: These are model clauses – there should not be any possibility to context their "formation", "validity" or "binding effect" (unless with latter we mean things like the valid signature, then one could leave "binding effect")

Commented [A95]: See above Clause 23 and the comments made

[WIPO CLAUSE - Arbitration clause only for B2B conflicts]

[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/

The alternative mentioned in the paragraph above does not exclude or alter the right of the data subject afforded by these Clauses or the applicable law to lodge a complaint of any kind with the competent supervisory authority or [bring a claim/file a case] in the competent court.

Commented [A96]: Ok if this is included as a clarification, but this should already be clear from the fact that the "WIPO CLAUSE" only refers to controversies/claims "between the Parties".

Commented [A97]: See also our comments on the redress clause.

[OPTION 2]

(...)

The alternative mentioned in the paragraph above does not exclude or alter the right of the data subject afforded by these Clauses, the Convention and the applicable law to lodge a complaint of any kind at the supervisory authority/ies or at the courts of the applicable jurisdiction.

Commented [A98]: See comment above for the WIPO CLAUSE – if kept, the paragraph should be aligned with the above comments on that clause

Commented [A99]: Not clear what this means: those are model contract clauses and the decision should be made now how to formulate them

Clause 26. General Provisions

[These are standard clauses in contracts. These may be merged with the general clauses of the first section of the model clauses in order not to have two general sections]

Commented [A100]: See earlier comment on the word "Agreement" (which is not a defined term and could cause confusion, given that the Clauses will typically form part of a broader commercial agreement). The applicable term is "these Clauses"

Term. This Agreement will remain in force and effect during the Term until terminated by either party in accordance with clause 22.

Commented [A101]: Not sure whether this is really helpful: the "term"/duration of the Clauses will be linked to the length of the overall commercial agreement, but it should be clear that e.g. Clause 22(d) ("Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses") in a way extends beyond termination

OPTION: Term. This Agreement will remain in force and effect and renew automatically until terminated by either party in accordance with clause 22.

Commented [A102]: This needs to be aligned with the indicated "term" at the beginning of the document (since this OPTION is essentially about an unlimited "term")

Assignment. This Agreement may not be assigned by the data importer or by operation of law to any person(s), firm(s) or corporation(s) without the express written approval of the data exporter.

Commented [A103]: If considered important, this should probably be incorporated into the "docking clause"

Notices. All notices and demands hereunder by a Party to the other will be in writing and will be served by personal service, or by email at the address set forth in the Cover Page, or at such different addresses as may be designated by one Party by written notice to the other Party. All such notices or demands by mail will be by certified or registered mail, return receipt requested, or by a nationally recognised private express courier, and will be deemed complete upon receipt.

Commented [A104]: Not sure what "complete" means, and when "receipt" will be assumed

Severability. If any provision of this Clauses is held invalid by a court with jurisdiction over the Parties to these Clauses, such provision will be deemed to be restated to reflect as nearly as possible the original intentions of the Parties in accordance with the Convention and applicable law, and the remainder of the Clauses will remain in full force and effect.

Commented [A105]: This does not work for (pre-approved) model clauses that must not be changed (and if they are, the data exporter can no longer use them as a ground for data transfers)

Authority. Each Party hereby represents and warrants that the execution, as applicable, delivery and performance by such Party of these Clauses is within its corporate powers and has been duly authorized by all necessary corporate action on its part.

Commented [A106]: Again very questionable whether this can be applied to (pre-approved) model clauses. If it would really turn out that something is wrong with the Clauses, a revised set should be approved

Separate Counterparts. These Clauses may be simultaneously executed in separate counterparts, all of which will constitute one and the same instrument and each of which will be, and will be deemed to be, an original.

Commented [A107]: Same as above: this works for a commercial contract, but not for model clauses that in any event must not be changed and lose their effect if changed

All the Annexes to these Clauses, as well as any footnotes therein, form an integral part of these Clauses. Capitalised terms will have the meanings given to them in clause 2.

Commented [A108]: To be considered whether this clause is suitable for model contract clauses

Commented [A109]: Should either be deleted if no capital letters will be used anymore, or it should be ensured throughout the text that there is a consistent approach.

Annex 1

Information about the transfer

Description of the transfer: [...]

Purpose(s) of the transfer: [...]

Additional information: [...]

DRAFT DOCUMENT

Annex 2

Accession form

Agreement number [xx/2022]

Designation: [data exporter] or [data importer]

Company name:

Address:

City, Country, zip code:

Email:

By the signatures of their authorized representatives below, [Company name] agrees to become, with immediate effect, a Party to and agrees to be bound by the terms of the Contractual clauses for transborder flow of personal data [from controller to controller] OR [from controller to processor].

By Name:

Title: [xxxx]

Signature Date [xxxx]

Commented [A110]: Not clear what this means – is this about which position the “acceding” Party will have under the Clauses? If so, it should rather read sth like:

“Designation of the acceding entity under these Clauses: [data exporter or data importer]”

Commented [A111]: Always a company?

Commented [A112]: If this is only about the signature of the acceding entity, it should probably read “signatures of its authorized representative below, ...”. The question is whether there should perhaps be some “counter-signature” by the already existing Parties, to show the agreement on accession

Commented [A113]: But these clauses are only for C-C transfers?

Annex 3

Security measures

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

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability]

Commented [A114]: However, the examples below sometimes go beyond "security measures" (they seem to also cover general "technical and organisational measures" to ensure compliance with the safeguards).

Also, there should be some logical order of the examples

Annex 4

Measures for special categories of data]

[These safeguards may include, for instance, alone or cumulatively

- i) the data subject's explicit consent for the processing of special categories of 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 special categories of data,
- vi) additional restrictions with respect to further disclosure according to the nature of the data].

Commented [A115]: Shorter retention could also be a measure

Commented [A116]: But this is not really a "measure"

Commented [A117]: Not clear what this means

Annex 5

LIST OF SUB-PROCESSORS

[ONLY FOR MODULE 2 & 3 to be drafted after concluding model C2C - This annex has to be completed by the Parties if they agree to pre-authorize sub processors]

[\[A1\]](#) Is this part really necessary – in my opinion it could be deleted, but it is also ok for me to leave it.

[\[A2\]](#) I think, this does not apply to this part, does it?

[\[A3\]](#) including those going beyond the mere risks that may arise with the data transfer

EUROPEAN DATA PROTECTION SUPERVISOR

Strasbourg, 6 July 2022

T-PD(2022)1rev3

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION
OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING
OF PERSONAL DATA
CONVENTION 108

Model Contractual Clauses for Transborder Data Flows of Personal Data

COUNCIL OF EUROPE

CONVENTION 108+

Model Clauses for Transborder Data Flows of Personal Data
STANDARD CONTRACTUAL CLAUSES

Agreement number [xx/2022]

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

Data ~~e~~Exporter information

~~Company~~ **Name:**

Address:

City, Country, zip code:

Email:

Data importer information

~~Name~~ **Company:**

Address:

City, Country, zip code:

Email:

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

Data ~~e~~Exporter

By ~~Name:~~

~~Title:~~ [xxxx]

Signature Date [MM/DD/YEAR]

Data importer

By ~~Name:~~

~~Title:~~ [xxxx]

Signature Date [MM/DD/YEAR]

NOTE: These ~~Model contractual~~ clauses provide an appropriate level of protection for the transfer of personal data to non-Parties of ~~Modernised~~ Convention 108 following the standards established by Article 14(3) (b) of Modernised Convention 108².

²It is without prejudice to the fact the current clauses may be subject, after its adoption by the Committee of Convention 108, to an approval based on domestic law by a supervisory authority or other competent body or institution

Commented [A118]: I would agree with the deletion of this footnote 1 as the wording was not optimal but I still believe that we should clarify in a document (for instance a FAQ) that these clauses need to be adopted at national or regional level to have some legal effect.

STANDARD-MODEL CONTRACTUAL CLAUSES

Contractual-Model clauses for transborder flow of personal data ~~from controller to controller~~

Commented [A119]: EDPS: C to C only then? Not entirely clear as there are some references below to C to P (Annex 2 in particular).

The Data Exporter and the Data importer (hereinafter, the Parties) agree to these **standard Model contractual** clauses (hereinafter the Clauses):

PART I - GENERAL CLAUSES

Clause 1. Purpose and scope

1.2. The aim of these ~~standard contractual model~~ clauses is to ensure compliance with the requirements for the transfer of personal data to a non-Party under Convention 108+ (hereinafter the Convention).

When adopted and implemented by the persons involved in the transfer and further processing, ~~These contractual-Model~~ clauses provide an appropriate level of protection for the transfer of personal data following Article 14(3)(b) of the Convention.

Commented [A120]: EDPS: The added value of this part is not entirely clear. To be deleted perhaps?

(...)

Clause 2. Definitions

[Note: Apart from the sources cited in each defined term, see also document T-PD(2020)06rev3, [Interpretation of provisions, May 7, 2021](#)].

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 [A121]: EDPS: 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 [A122]: EDPS: 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.

(...)

Model Clauses ~~(or Standard contractual clauses)~~: Approved standardised safeguards provided by legally binding and enforceable instruments as required under Article 14(3)(b) of the Convention.

(...)

Data importer: The Controller or Processor located in a non-Party to whom the Data exporter transfers Personal data.

Data Exporter: The Controller or Processor located in a country that is a member of the Convention, that transfers Personal data to a Data importer.

Data subject: an identified or identifiable individual whatever his or her nationality or residence.
[Source: Article 2 of the Convention and para. 15 of the Explanatory Report]

[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 of the Explanatory Report]

Transborder flows of personal data: the transfer, making available or disclosure of personal data to a recipient subject to the jurisdiction of another State.
[Source: Article 14 of the Convention, Paragraphs 102 to 104 of the Explanatory report, and the legal opinion provided by the Legal Advisor DLAPIL02/2021_JP/DG3]

[Source: Article 26.3 of the Convention]

Onward transfer: when Personal data is transferred by the Data Importer to another Controller or Processor.

(...)

Special categories of data: ~~(or Sensitive data)~~: (i) Genetic data, (ii) personal data relating to offences, criminal proceedings and convictions, or related security measures; (iii) Biometric data

Commented [A123]: EDPS: If these clauses cover only C to C, then I suppose that the reference to processor should be deleted.

Commented [A124]: EDPS: Same comment as for biometric data

Commented [A125]: EDPS: Do we also envisage onward sharing within the same jurisdiction of the importer? This could be further clarified.

uniquely identifying a person; or (iv) personal data for the information they reveal 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, the Applicable law and these Clauses.

[Source: Article 15 of the Convention]

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(3)(b) of the Convention, provided they are not modified, except to add or update information in the Annexes.

(...)

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. 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~~ prevail over these 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 Annex 2, and, if required, updating the ~~data~~ description of the transfer of Annex 1.

(...)

The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

~~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 6. Data protection safeguards

Commented [A126]: EDPS: 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? In particular if we are in a C to C situation only?

Commented [A127]: EDPS: Clause 5 on third party beneficiaries seems to have disappeared? And why was this specific part deleted?

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.

~~The Data exporter represents that it has the right to transfer the personal data to the Data importer in accordance with these Clauses and the Applicable law. (...)~~

Commented [A128]: EDPS: 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.

At least we should add "in particular" or "for instance" through the implementation of...

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:

- a. his or her identity and habitual residence or establishment;
- b. the purposes of the intended processing;
- c. the categories of personal data processed;
- d. the recipients or categories of recipients of the personal data, if any;
- e. the means of exercising the rights set out in these Clauses, as well as any necessary additional information in order to ensure fair and transparent processing of the personal data;
- f. of the right to obtain a copy of these Clauses.

Commented [A129]: EDPS: 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.

~~8.3. Paragraph 1 shall not apply when the Personal data are not collected from the data subject~~
where the processing is expressly prescribed by law or this proves to be impossible or involves disproportionate efforts.

[Source: Article 8 of the Convention]

Commented [A130]: Such new provision will amount to skip transparency obligations in many cases as it might be quite frequent to have a transfer of data that were not collected from the data subjects. Should we delete?

Clause 9. Accuracy and data minimisation

(...)

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.

Commented [A131]: if the clauses are only C to C, then to be deleted.

Commented [A132]: EDPS: It would be good to refer to encryption and pseudonymisation.

(...)

The Data importer shall ~~notify~~ notify, without delay, at least the Data Exporter, who will notify the competent Supervisory Authority of those data breaches which may interfere with the rights and fundamental freedoms of data subjects.

Commented [A133]: EDPS: Can we specify a more precise timeframe?

In case where a Data breach has occurred that may seriously interfere with the human rights and fundamental freedoms of the individual (e.g. the disclosure of data covered by professional confidentiality, Special categories of sensitive data, or which may result in financial, reputational, or physical harm or humiliation) the Data importer shall notify without delay the Data Exporter and the relevant Supervisory Authority/es 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 [A134]: EDPS: 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 where applicable, 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.

In specific circumstances, where the notification would require unreasonable time, effort or resources, the Data importer may seek the cooperation or the assistance of the Data exporter to produce the notifications and measures in the previous paragraph.

[Source: Article 7 of the Convention & Paragraph 66 of the Explanatory Report]

(...)

Clause 12. Special categories of data

Where the transfer involves ~~Sensitive~~ Special categories of data, the Data importer shall apply additional safeguards adapted to the risks at stake and the interests, rights and freedoms to be protected.

(...)

The Parties have agreed on the safeguards as set out in Annex 4. ~~The Parties shall set out these measures in Annex 4.~~

Clause 13. Onward transfers

The Data importer shall not disclose the personal data to a third party located in a non-Party unless the third party ensures an appropriate level of protection in line with Article 14 of ~~the~~ Convention-108+.

(...)

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 15. Documentation and compliance

(...)

~~The Data importer guarantees that it has paid due regard to the impact the intended data processing might have on the rights and fundamental freedoms of Data subjects prior to the commencement of such processing according to the circumstances of the specific transfer and has taken the necessary technical and organisational measures to comply with the clause. 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 has designed the data processing in such a manner as to prevent or minimize the risk of interference with those rights and fundamental freedoms.~~

Clause 16 – 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 related 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~~.

(...)

Clause 17. 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 receive requests to exercise individual rights~~ and handle complaints. It shall deal promptly with any complaints it receives from a Data subject.

(...)

Commented [A135]: EDPS: 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 [A136]: Wouldn't it be appropriate to provide for a possibility to extend the deadline - for instance by two further months where necessary, taking into account the complexity and number of the requests?
This is the solution proposed by the GDPR and often it is imperative for C to benefit from this extension.

Commented [A137]: Would this part rather fit under clause 8 on transparency? Moreover, we are of the opinion that the information should be proactively given to the individual and not only be made available on the website. We could then delete “or on its website”.

Commented [A138]: EDPS: We also need redress towards the exporter no?
Moreover, will this contact point actually handle the complaints? In practice, quite often, the contact point will be the DPO but the responsibility of handling the complaints lies with an oversight mechanism.

So this notion of contact point may create confusion between the handling of the request / complaint by the C and the right to seek redress towards an independent oversight mechanism.

The alternative mentioned in the paragraph above does not exclude or alter the right of the Data subject afforded by these Clauses, the Convention and the Applicable law to lodge a ~~claim~~ complaint at the Supervisory Authority/ies or at the courts of the applicable jurisdiction. The Data importer shall abide by a decision that is binding under the Applicable law.

Clause 18. Liability

(...)

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

[Source: Para. 22 of the Explanatory Report]

Commented [A139]: Rather « the Parties » as it may also be applicable to the Data Exporter.

Clause 19. Supervisory authority

(...)

The Parties hereby consent that the supervisory authority is entitled to request that any of the Parties demonstrates the effectiveness of the safeguards ~~or including~~ 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 as established by the Applicable law or these Clauses, 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],

(...)

Commented [A140]: EDPS: I understand the objective but I am not sure to understand the consequences of such sentence. For instance, a 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 parag after (possibility to request information, to perform audits, etc). Might be further discussed.
Also, there is some overlap with the paragraph after. Actually, I think the parag after is closer to what can be reasonably requested from the data importer.

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

Clause 20. Local laws and practices affecting compliance with the Clauses

- (a) The Parties warrant that they have no reason to believe that the laws and practices in ~~the country of destination~~~~the non-Party 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. ~~This should include full and joint liability for any material and non-material damages made by the Parties, or which occurred to the data subject in relation of the use of the Clauses.~~
- (b) This is based on the understanding that specific exceptions to these Clauses based on applicable law(s) that respect the essence of the 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.
- (...)
- ii) ~~the laws and practices in the country of destination 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;
- (...)
- (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 ~~[issue]~~ and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (...)
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the ~~non-Party~~~~country of destination~~ –or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

Commented [A141]: We are not sure to understand this reference to the liability regime here, also perhaps not 100 % in line with the clause on liability. Can we simply delete the reference here?

Commented [A142]:

EDPS: 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 [A143]: What do you mean here? Do we want to clarify that 'relevant information' is in relation to the 'Local laws and practices affecting compliance with the Clauses'?

(...)

Clause 21. 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, and to the extent possible - the Data subject promptly (if necessary, with the help of the data exporter) if it:

(...)

- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, ~~on the request of 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.).

(...)

SECTION IV – FINAL PROVISIONS

Clause 22. Non-compliance with the Clauses and termination

- (b) ~~Each Party shall promptly inform each other party if it is unable to comply. Both Parties shall promptly inform each other if they are unable to comply~~ with these Clauses, for whatever reason.

(...)

Clause 24. Choice of forum and jurisdiction

(...)

[OPTIONAL Clause 25. Arbitration]

[OPTION 1]

Commented [A144]: EDPS: It would be better to keep 'at regular intervals' to ensure a proactive provision if information.

Commented [A145]: EDPS: There is also a reference to ADR in clause 17. Should we rather merge all these elements in a single clause?

Any dispute, controversy or claim between the Parties arising under, out of or relating to these Clauses including, without limitation, its formation, validity, binding effect, interpretation, performance, breach or termination, as well as non-contractual claims, shall 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]~~the country of the Data Exporter.

[WIPO CLAUSE - Arbitration clause only for B2B conflicts]

[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/

The alternative mentioned in the paragraph above does not exclude or alter the right of the Data subject afforded by these Clauses, the Convention and the Applicable law to lodge a ~~claim~~complaint of any kind at the Supervisory Authority/ies or at the courts of the applicable jurisdiction.

(...)

The alternative mentioned in the paragraph above does not exclude or alter the right of the Data subject afforded by these Clauses, the Convention and the Applicable law to lodge a ~~complaint~~claim of any kind at the Supervisory Authority/ies or at the courts of the applicable jurisdiction.

Clause 26. General Provisions

(...)

Commented [A146]: EDPS: 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?

Annex 1

Information about the transfer

Description of the transfer: [...]

Purpose(s) of the transfer: [...]

Additional information: [...]

Commented [A147]: EDPS: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 such as in the EU SCCs

Annex 2
Accession form

Agreement number [xx/2022]

Designation: [Data Exporter] or [Data importer]

Company name:

Address:

City, Country, zip code:

Email:

By the signatures of their authorized representatives below, [Company name] agrees to become, with immediate effect, a Party to and agrees to be bound by the terms of the Contractual clauses for transborder flow of personal data [from controller to controller] OR [from controller to processor].

By Name:

Title: [xxxx]

Signature Date [xxxx]

Commented [A148]: EDPS: To be clarified : are those clauses covering C to C only or also C to P? See comment above.

Annex 3

Security measures

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

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Annex 4
Measures for ~~sensitive~~ Special categories of data

[These safeguards may include, for instance, alone or cumulatively

- i) the data subject's explicit consent for the processing of ~~sensitive~~ Special categories of 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 Special categories of~~Sensitive~~ data, and
- vi) additional restrictions with respect to further disclosure according to the nature of the data].

Annex 5

LIST OF SUB-PROCESSORS

[ONLY FOR MODULE 2 & 3] to be drafted after concluding model C2C - This annex has to be completed by the Parties if they agree to pre-authorize sub processors]

Commented [A150]: it was not clear to us that the C to C would be module. This could be clarified earlier in the document to get an "easy to navigate through" structure.