Guide to the preparation of contractual clauses governing data protection during the transfer of personal data to third parties not bound by an adequate level of data protection (2002)

Prepared by the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) in 2002

Table of contents

Appendices

I. BACKGROUND

1) Introduction

1. The Council of Europe's *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal data* [ETS No.108] (hereinafter Convention 108) was opened for signature on 28 January 1981 and has the purpose of securing in the territory of each Party respect for the rights and fundamental freedoms of every individual, whatever his/her nationality or place of residence, and in particular his/her right to privacy, with regard to automatic processing of personal data relating to him/her.

2. In principle, it should make no difference to data subjects whether data processing operations take place in one or several countries. The same fundamental rules should apply and data subjects should be given the same safeguards for the protection of their rights and interests. In practice, however, the protection of an individual's data is weakened when the geographic area is widened. Therefore it became necessary to establish mechanisms which provide an adequate protection to individuals when data concerning them flow across borders.

3. If any changes in the processing of personal data deserve mention since Convention 108 was adopted, they are those that derive from the advances made in information technology, combined with the developments in telecommunications, which have opened up new possibilities for processing data on an international scale. The developments in electronic data processing and in the setting up of extensive data banks have increasingly facilitated the dissemination of information in several countries. They help to overcome the various barriers to communication between different States: distance, time, language and cost. As a result, the free international flow of information may enhance cultural and economic relationships worldwide.

4. Nevertheless, as the personal data protection principles laid down in Convention 108 are not yet enshrined in the legislation, common law and social practices of the great majority of third countries, potential risks to the rights of data subjects of the countries that are Party to Convention 108 may arise when the processing of personal data of those individuals is carried out in such third countries. Therefore, it is important to find specific legal solutions that seek to maintain the balance between the requirements of the effective protection of personal data and the principle of free flow of information, regardless of frontiers, notwithstanding that the former is a fundamental right of the individual and therefore deserves specific legal protection.

5. These solutions may be of the utmost importance where there is a controller or a processor that is committed to applying the data protection principles of Convention 108 in a country that does not yet recognise those principles as part of their legal system; but this does not prevent that controller or processor from voluntarily accepting to be bound by them. This may also enhance social and commercial respect for those principles, which may be the source of customary law. However the use of contractual clauses should not be seen as a long-term substitute for domestic law protecting personal data.

2) The Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data

6. Article 12 of Convention 108 was drafted with the aim of finding a balance between the protection of personal data and the free flow of information in the context of transborder flows of these data:

> ***"****Article 12 – Transborder flows of personal data and domestic law*
>
> *1. The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.*
>
> *2. A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.*
>
> *3. Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:*
>
> > *a. insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;*
> >
> > *b. when the transfer is made from its territory to the territory of a non Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph."*

7. Article 12 specifies the notion set out in the Preamble of Convention 108 which states "[…] Reaffirming at the same time their commitment to freedom of information regardless of frontiers; Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples […]". In summary, this provision on transborder data flows has as its primary objective the protection of privacy without posing an excessive burden on the free flow of information so as to avoid negative effects on international relations, be they cultural, economic or of another kind.

8. Therefore, Article 12 establishes the principle of the free flow of personal data between Contracting States, but goes on to grant each Party to Convention 108 the right to prohibit or restrict transfrontier flows in respect of certain categories of data covered by specific regulations, except where the regulations of the recipient state provide equivalent protection. At the same time, it provides for the restriction or prohibition of the flow of personal data across national borders into non Contracting States passing through the intermediary of a Contracting State.

9. However, this provision does not provide a full solution to the need to protect the fundamental rights and freedoms of the data subject as regards the processing of his/her personal data in connection with transborder data flows as the spectacular increase in such data flows which has occurred during the last decade will probably increase in the near future. The transfer of personal data across borders is facilitated by the existence of

digital communication systems and is rendered inevitable by the internationalisation of the economy.

3) The model contract of 1992 to ensure equivalent data protection in the context of transborder data flows

10. In order to prevent the level of privacy protection from being reduced as a result of automated processing of personal data in third countries, the Council of Europe's Consultative Committee of Convention 108 started to reflect in 1989 on the possibility of using contractual techniques to ensure the protection of the individual's privacy in the context of transborder data flows. This contractual technique had already been referred to in several sectorial recommendations on data protection adopted by the Committee of Ministers (e.g. Recommendation No R (86) 1 on the protection of personal data used for social security purposes; Recommendation No R (89) 2 on protection of personal data used for employment purposes).

11. Taking into account the above mentioned considerations, the Council of Europe jointly with the Commission of the European Communities and the International Chamber of Commerce, prepared a study in 1992 which contains a "model contract to ensure equivalent data protection in the context of transborder data flows" (see the data protection web site of the Council of Europe at the following address: http://www.coe.int/dataprotection). As mentioned in this study, the obligations of the licensor and licensee under the model contract were based on the guarantees established by the Council of Europe's Convention 108, which also appear in the OECD Guidelines on the protection of privacy and transborder flows of personal data. The objectives of the model contract to ensure equivalent data protection in the context of transborder data flows were as follows:

> to provide an example of one way of resolving the complex problems which arise following the transfer of personal data subjected to different protection regimes;
>
> to facilitate the free circulation of personal data in the respect of privacy;
>
> to allow the transfer of data in the interest of international commerce;
>
> to promote a climate of security and certainty of international transactions involving the transfer of personal data.

12. The clauses of the model contract were designed to allow the transfer of personal data between independent economic entities and it was left to the Parties whether to use the clauses or not; the clauses were optional. Parties should adapt the clauses to specific conditions. The clauses could serve as a basis for the establishment and development of appropriate rules e.g. for transfers within the same group of firms or between a file controller and a data processing service. The study also mentioned that Parties were free to choose the law applicable to the contract between licensor and licensee. They should always stipulate explicitly the law which they have chosen. When the applicable domestic law ensures a better protection of the personal data, the licensor was recommended to check whether he/she must complete the clauses accordingly.

4) The Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows

13. This "model contract" prepared in 1992 was the first step for the preparation of similar model contractual clauses in another international forum. However, the need to improve "the application of the principles set forth in the Convention [which] has become necessary because of the increase in exchanges of personal data across national borders between states which are Parties to the Convention and states or entities which are not"[1] was one of the reasons for the preparation of the *Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS No.108] Regarding Supervisory Authorities and Transborder Data Flows* [ETS No. 181] which was opened for signature on 8 November 2001.

14. The Explanatory Report of this Additional Protocol to Convention 108 states that the "increase in the flow of data across national borders is a consequence of the ever-growing volume of international exchanges on a global scale, together with technological progress and its numerous applications. At the same time, therefore, a constant effort is needed to improve the effective protection of the rights guaranteed by the Convention. Effective protection in turn requires international harmonisation not only of the basic principles of data protection but also, to a certain extent, of the means of implementing them in such a rapidly changing, highly technical field and of the conditions in which the transfers of personal data can be made across national borders. […] The flow of information is at the very core of international co-operation. However, the effective protection of privacy and personal data also means that there should in principle be no transborder flows of personal data to recipient countries or organisations where the protection of such data is not guaranteed"[2].

15. As said above, Article 12 of Convention 108 establishes the principle of the free flow of personal data between the Parties subject to the possibilities for derogation provided for in sub-paragraph 3. Article 2 of the Additional Protocol to Convention 108 establishes the principle that transborder flows of data to a recipient which is not under the jurisdiction of a Party to Convention 108 are subject to the condition of an adequate level of protection in the recipient country or organisation. However, Parties to Convention 108 have the possibility to determine derogations from the principle of an adequate level of protection. One of these derogations concerns the provision of safeguards by the controller responsible for the transfer and can in particular result from contractual clauses (see Article 2, paragraph 2, littera b. of the Additional Protocol of Convention 108).

16. The problematic issue is to define the meaning of an "adequate level of protection". The Explanatory Report of the Additional Protocol to Convention 108, in particular the paragraphs concerning Paragraph 1 of Article 2, gives some indications of when it could be considered that an adequate level of data protection exists in a third country. This can be established via a general assessment or via an assessment on a case-by-case basis.

17. The adequacy of the level of data protection can be established by a general assessment: Paragraph 28 of the Explanatory Report of the Additional Protocol states that

[1] See paragraph 3 of the Explanatory Report of the Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS No.108] Regarding Supervisory Authorities and Transborder Data Flows [ETS No. 181].

[2] Ibid. paragraphs 4 and 6 of the Additional Protocol to Convention 108.

"an assessment of adequacy can similarly be made for a whole state or organisation thereby permitting all data transfers to these destinations. In that case, the adequate level of protection is determined by the competent authorities of each Party".

18. The adequacy of the level of data protection can be established by an assessment on a case-by-case basis. Paragraph 26 of the Explanatory Report states that "the adequacy of the level of protection must be assessed in the light of all the circumstances relating to the transfer". Paragraph 27 continues "the level of protection should be assessed on a case-by-case basis for each transfer or category of transfer made. Thus the circumstances of the transfer should be examined and, in particular:

> the type of data,
>
> the purposes and duration of processing for which the data are transferred,
>
> the country of origin and the country of final destination,
>
> the general and sectoral rules of law applicable in the state or organisation in question and the professional and security rules which obtain there. "

19. However, according to Paragraph 2 of Article 2 of the Additional Protocol to Convention 108, the transfer of personal data to countries which do not ensure an adequate level of protection is possible if domestic law provides for it because of specific interests of the data subject; or legitimate prevailing interests, especially important public interests; or if safeguards are provided by the controller responsible for the transfer.

20. In that context it is important to examine what the '*legitimate prevailing interests, especially important public interests*' provided for by domestic law could be. Paragraph 31 of the Explanatory Report says that "The parties have discretion to determine derogations from the principle of an adequate level of protection. The relevant domestic law provisions must nevertheless respect the principle inherent in European law that clauses making exceptions are interpreted restrictively, so that the exception does not become the rule. Domestic law exceptions can therefore be made for a legitimate prevailing interest. That interest may be to protect an important public interest, such as is specified in the context of Article 8 paragraph 2 of the European Convention on Human Rights and Article 9 paragraph 2 of Convention ETS No. 108; the exercise or defence of a legal claim; or the extraction of data from a public register. Exceptions may also be made for the specific interest of the data subject as for the fulfilment of a contract with the data subject or in his interest, or for protecting his vital interest or when he has given his consent. In this case, before consenting, the data subject would have to be informed in an appropriate way about the intended transfer".

21. Another option for the situation where the recipient country does not ensure an adequate level of data protection could be safeguards provided by the controller, in particular such as those resulting from contractual clauses. Paragraphs 32 and 33 of the Explanatory Report state "each party may provide for the transfer of personal data to a recipient which is not subject to the jurisdiction of a Party and does not ensure an adequate level of protection, provided that the person in charge of the transfer supplies sufficient safeguards. These safeguards must be found adequate by the competent supervisory authorities according to domestic law. Such safeguards may in particular be the result of contractual clauses binding the controller who makes the transfer and the recipient who is not subject to the jurisdiction of a Party" and "The content of the contracts

concerned must include the relevant elements of data protection. Moreover, in procedural terms, contract terms could be such, for example, that the data subject has a contact person on the staff of the person responsible for the transfer, whose responsibility it is to ensure compliance with the substantive standards of protection. The subject would be free to contact this person at any time and at no cost and, where applicable, obtain assistance in exercising his or her rights".

5) Contractual clauses for protection of personal data in the context of transborder data flows to third countries prepared by other international organisations

22. As mentioned above, the Commission of the European Communities participated, together with the Council of Europe and the International Chamber of Commerce, in the preparation of the model contract of 1992. Afterwards, the Working Party on Protection of Individuals with Regard to the Processing of Personal Data established under Directive 95/46/EC issued guidelines in order to aid with the assessment of the adequate level of protection required in the transfer of personal data to the third countries[3]. Following these guidelines, the European Commission adopted *Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries.* This Commission Decision sets out "standard contractual clauses ensuring adequate safeguards for personal data transferred from the European Union to countries outside the Union. The Decision obliges member States to recognise that companies or organisations using such standard clauses in contracts concerning personal data transfers to countries outside the European Union are offering "adequate protection" to the data. […]Use of these standard contractual clauses will be voluntary but will offer companies and organisations a straightforward means of complying with their obligation to ensure "adequate protection" for personal data transferred to countries outside the European Union which have not been recognised by the Commission as providing adequate protection for such data"[4]. This Commission Decision covers only the transfer of personal data between data controllers. *Commission Decision 2002/16/EC of 27 December 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries* is intended to cover the transfer to data processors.

23. Other international organisations also examined this issue, for instance the Working Party on Information Security and Privacy of the OECD prepared a Report on Transborder Data Flow contracts in the Wider Framework of Mechanisms for privacy Protection in Global Networks in 2000.

24. In 1999, the International Chamber of Commerce prepared a Model Clauses for Use in Contracts Involving Transborder Data Flows. The International Chamber of Commerce and other business organisations are currently preparing a set of proposed standard clauses for the transfer of personal data from the European Union to third countries. These

---

[3] WP 4 (5020/97) 'First orientations on transfers of personal data to third countries working document — possible ways forward in assessing adequacy', a discussion document adopted by the Working Party on 26 June 1997.

WP 7 (5057/97) 'Judging industry self regulation: when does it make a meaningful contribution to the level of data protection in a third country?', working document: adopted by the Working Party on 14 January 1998.

WP 9 (3005/98) 'Preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries', working document: adopted by the Working Party on 22 April 1998.

WP 12: 'Transfers of personal data to third countries: applying Articles 25 and 26 of the EU data protection directive', working document adopted by the Working Party on 24 July 1998, available, in the web-working document site 'europa.eu.int/comm/internal_markt/en/media.dataprot/wpdocs/wp12/en' hosted by the European Commission.

[4] See http://europa.eu.int/comm/internal_market/en/dataprot/modelcontracts

proposed standard clauses are currently being discussed with the Commission of the European Communities.

II. GUIDE TO THE PREPARATION OF CONTRACTUAL CLAUSES GOVERNING DATA PROTECTION DURING THE TRANSFER OF PERSONAL DATA TO THIRD PARTIES NOT BOUND BY AN ADEQUATE LEVEL OF DATA PROTECTION

25. In view of the legislative and technological developments which have occurred in the field of data protection since the preparation of the "Model Contract" in 1992, the Council of Europe's Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD) decided to re-examine the issue of the contractual clauses to be used when transferring personal data to third countries which do not ensure an adequate level of protection. The T-PD instructed an independent expert to prepare a report on this issue. Professor Jerôme Huet prepared a study on "Contracts involving the transfer of personal data between parties to Convention ETS No.108 and third countries not providing and adequate level of protection" as well as some recommendations made in the light of this study. This Study is available on the data protection website of the Council of Europe (http://www.coe.int/dataprotection).

26. On the basis of this Study as well as the new international instruments recently adopted, in particular the Additional Protocol to Convention 108 and the two Commission decisions mentioned above, the T-PD decided to prepare the present Guide. The T-PD agreed that it would not be appropriate at present to revise the "Model Contract to ensure equivalent data protection in the context of transborder data flows" which the T-PD had drafted in co-operation with the Commission of the European Communities and the International Chamber of Commerce in 1992, since to do so might duplicate the European Commission's work on drafting model clauses for the transfer of personal data to third countries under Directive 95/46/EC (cf. Commission Decision of 15 June 2001 and Commission Decision of 27 December 2001).

27. The purpose of this Guide is to assist parties in the drawing up of contractual clauses conforming to the protection requirements deriving from Convention 108 and inform data controllers and data subjects concerned by transborder flows of what they need to look out for as well as to provide assistance for data subjects seeking to assert their rights in the data protection field.

28. The main objective of the principles contained in this Guide is to contribute to ensuring an adequate level of protection when processing personal data in cases of transfer to countries which do not ensure this level.

29. These principles could also supply a useful tool and a supplementary guarantee for specific transfers between countries which ensure an adequate level of protection (e.g. the transfer of a specific category of data or in other cases for specifying the purposes of the processing).

30. Therefore the present Guide does not replace the contractual clauses included in the model contract of 1992 but instead completes or specifies the 1992 contractual clauses and therefore both documents should be read together.

31. The principles contained in this Guide, which are based on the principles of Convention 108, should be primarily taken into account in cases where in the State where the importer is established there is a lack of legislation or other regulations deemed

satisfactory to provide an adequate level of personal data protection. This means that they are intended to be applied where the recipient of data (the importer) :

is established in a State which has not ratified Convention 108 and lacks the legislation providing the adequate level of protection that is envisaged in Article 2 paragraph 1 in fine of the Additional Protocol to Convention 108 regarding supervisory authorities and transborder data flows; or

operates in a sector of activity that is not subject to other regulations deemed satisfactory as regards personal data protection in a State which has not ratified Convention 108[5]; or

is established in a State that has ratified Convention 108 in cases where the State where the exporter of data is established may have applied the derogations referred to in Article 12.3.a) of Convention 108 to certain kinds of transfers.

32. The parties to these transfers are encouraged to apply these principles to any transfers of personal data other than those mentioned above in order to supplement the legal provisions on data protection which govern them. For example, these principles could be useful for specifying the purposes of the processing in cases of data transfers between countries which have ratified Convention 108 or which have an adequate level of protection.

33. This Guide applies to transfers of personal data between controllers. It will be periodically evaluated by the T-PD.

III. PRINCIPLES TO BE TAKEN INTO ACCOUNT WHEN PREPARING CONTRACTUAL CLAUSES GOVERNING DATA PROTECTION DURING THE TRANSFER OF PERSONAL DATA TO THIRD PARTIES NOT BOUND BY AN ADEQUATE LEVEL OF PROTECTION

For the purposes of these principles the terms below will be understood as follows:

"Personal data" means any information relating to an identified or identifiable individual ("data subject")[6]. An individual shall not be regarded as "identifiable" if the identification requires an unreasonable amount of time and manpower.

"Sensitive data" means personal data revealing racial origin, political opinions, religious or other beliefs, as well as personal data concerning health, sexual life or criminal convictions, and other data defined as sensitive by domestic law in the exporter's country.

"Processing" means any operation or set of operations applied to personal data, such as storage, conservation, adaptation or alteration, extraction, consultation, utilisation, communication, matching or interconnection and erasure or destruction.

"Data exporter" means the controller who transfers the personal data.

[5] Such as, e.g., the Safe Harbor system recognized by the EU as offering an adequate level of protection (Commission Decision 2000/520/EC, of 26 July 2000)

[6] Personal data may be not only texts, but also images, photographs, sound, etc.

“Data importer” means the controller who receives personal data from the data exporter.

“Controller” means the natural or legal person, public authority, agency, or any other body which, alone, or in collaboration with others, determines the purposes of and means used in the collection and processing of personal data.

The reference to “contract” in this guide refers exclusively to the relevant contractual clauses for the protection of personal data.

Principle 1 – General Provision

Data transfers are a form of processing personal data within the meaning of Convention 108. They may go ahead only if processing is carried out as specified in the data protection legislation to which the exporter is subject and, in particular, if the planned transfer is lawful under the terms of that legislation.

The contract should be drawn up taking account of the legal situation (concerning the general legislation and, where applicable, any specific legislation on data protection) of the country in which the data importer is located. To enable the exporter to make sure that the importer continues to be able to honour the contract, the contract should include an obligation for the importer to inform the exporter of any relevant legal change in his or her country subsequent to the conclusion of the contract which may significantly adversely affect the safeguards afforded by the contractual clauses.

Explanatory note:

The importer should inform the exporter of the changes about which he/she could reasonably be expected to know.

Principle 2 – Information to the data subject

The exporter of data should take appropriate measures to inform data subjects, before the data transfer takes place, of the identity of the importer, the purposes for which the data are to be processed and any other information insofar as it is necessary to ensure fair processing, unless this information has already been provided by the exporter of the data. In addition, the data subject should, at his/her request, be informed about the existence of a contract. If data subjects so request, the exporter of data should give data subjects a copy of the contractual clauses relating to data protection.

Explanatory note:

Article 5.a (fair collection and processing of data) of Convention 108 sets out the general principle of transparency in data processing. Article 8 sets out the individual’s right to know about the existence of processing of personal data, its principal purposes, as well as the identity and habitual residence or principal place of business of the controller of the file. The principle of transparency is particularly important in connection with personal data transfers to countries that do not offer an adequate level of protection. The domestic law of some Parties to the Convention and certain Council of Europe recommendations require information to data subjects on the possibility of transfer of their data to a third country. Furthermore, some Parties provide for an obligation to notify the transfer and/or the contractual clauses to the national data protection authority. When carrying out this obligation to inform data subjects, account should be taken of the specific circumstances.

Principle 3 – Details of the transfer

The contract should specify all relevant details of the transfer and, in particular:

- the identity of the exporter and importer of data;

- the categories of personal data to be transferred (sensitive data should be specified);

- the purposes for which the personal data are transferred;

- the categories of data subjects whose personal data are transferred;

- the recipients of the data (where necessary, this should be specified for each category of data);

- the storage limit applicable to the data transferred.

Principle 4 – Obligations of the data importer

The contract should specify that the importer undertakes in particular :

- to process the data transferred fairly and lawfully ;

- to process the data only for the purposes for which they have been transferred ;

Explanatory note:

The contract should list all the purposes for which the exporter authorises the importer to process the data transferred. "Process" comprises subsequent use and further transfer.

to make sure that the data transferred remain accurate, adequate, relevant and not excessive in relation to the purposes for which they have been transferred and that they are updated where necessary;

Explanatory note:

The data importer will be able to guarantee that the data are accurate only in relation to the form in which he/she receives them.

to keep the data for no longer than is necessary for the purposes for which the data have been transferred;

to give data subjects a copy of the contractual clauses relating to data protection if they so request.

Principle 5 – Sensitive data

The contract should provide all the appropriate additional safeguards when sensitive data are to be transferred.

Explanatory note:

Sensitive data should be transferred only where this is necessary to meet the purposes of the processing. Such transfer, moreover, should be accompanied by additional protective measures, including appropriate security measures such as encoding the data for transfer or listing the conditions governing access to sensitive data.

Principle 6 – Security of the data

The contract should require the importer to take all appropriate technical and organisational security measures for protection of the personal data transferred to him or her, in order to prevent their accidental or unauthorised destruction, as well as to prevent unauthorised access, modification or diffusion of the data. These measures should ensure a level of security appropriate to the potential risks and should take account of the state of technology and the costs involved.

Principle 7 – Rights of access, rectification, erasure and blocking of data

The contract should define the obligations of the exporter and the importer towards the data subject. In particular, the importer of the data should respond to reasonable inquiries regarding the data processing made by the data subjects and should ensure that data subjects have the right of access to data concerning them, including the right of rectification and erasure or the right to block personal data processed in breach of the contract. In relation to these rights, the exporter and the importer should inform each other of requests by data subjects and of the manner in which they have been dealt with.

Principle 8 – Third party beneficiary clause

The contract should include a third-party beneficiary clause enabling data subjects to assert their rights vis-à-vis the exporter and/or the importer.

Principle 9 - Liability

The contract should provide for compensation for data subjects who suffer damage when their data are processed in breach of the contract.

Explanatory note:

An effective compensation system is one which provides for joint and several liability of the importer and the exporter ; other systems, such as a system of insurance, may also be effective. Claims for compensation must arise from a breach of the contractual data protection clauses. Compensation may be sought not only for pecuniary damage but also for non-pecuniary damage.

Principle 10 – Applicable law

The contract should stipulate that the law governing relations under the contract is the law in the exporter's country, provided that the law provides for a third party beneficiary clause. Where such a clause is not permitted by the law of the exporter's country, the contract should stipulate that the law applicable to relations under the contract is the law of a country which is a party to Convention 108 for the protection of individuals with regard to

automatic processing of personal data, whose law provides for the inclusion of a third party beneficiary clause.

Principle 11 –Jurisdiction and mediation

The contract should afford data subjects the right to bring any dispute regarding performance of the contract with the exporter and/or the importer of the data before the competent courts of the country where the exporter is established, without prejudice to the data subject's procedural or substantive right to obtain compensation according to other provisions of national or international law. The contract should also make provision for data subjects, in the event of a dispute not resolved by friendly settlement, to seek an extra-judicial mechanism for settlement of disputes (such as arbitration or mediation).

Explanatory note:

Mediation could also be provided by the competent data protection authority. Data subjects should be able to retain the possibility of recourse to the courts, irrespective of agreements between the parties on the settlement of disputes.

Principle 12 - Disclosure of data

The contract should limit disclosures to third parties of the data transferred to those which are necessary to meet the purposes of the transfer. Such disclosures should be subject to conditions guaranteeing an equivalent level of data protection to that offered by the clauses of the original contract. The transfer could also be made if the data subject gave his or her consent. If such disclosure concerns sensitive data, the explicit consent of the data subject should be required.

Explanatory note :

The disclosure should be made only for the purposes for which the data were transferred. The new importer could accede to the original contract with the original exporter.

Principle 13 – Control and co-operation with supervisory authorities

The contract should authorise the exporter to check compliance with the contractual clauses on data protection or to have it checked. The contract could also provide for the possibility for the importer to supply information concerning the processing of the transferred data to the data protection authority of the exporter's country upon request, as well as the obligation to abide by the opinion of this same authority as regards the processing of the data transferred.

Explanatory note:

The exporter may carry out a check himself or herself. He or she may also entrust this task to an independent and qualified third party. In order to ensure that the data protection authority does not order the contract to be suspended, it is preferable that the importer agree to follow the instructions of this authority with a view to improving compliance with the contractual clauses. "Data protection authority" means the supervisory authority responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated in Convention 108 and its Additional Protocol.

Principle 14 – Termination of the contract

Termination of the contract should be possible, in particular where:

- changes in the importer's national law or any serious event occurring in his or her country make it impossible to abide by the contractual clauses;

- the data protection authority of the exporter's country orders cessation of the data transfer to the importer;

- the importer is insolvent or declared bankrupt.

The contract should provide that when it expires or is terminated, the exporter and the importer remain bound by the obligations and the conditions provided for in the contract with regard to the processing of the data which have been transferred.