



Explanatory Report to 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

Strasbourg, 8.XI.2001

The text of this explanatory report does not constitute an instrument providing an authoritative interpretation of the Protocol, although it might be of such a nature as to facilitate the application of the provisions contained therein. This Protocol has been open for signature in Strasbourg, on 8 November 2001, on the occasion of the 109th Session of the Committee of Ministers of the Council of Europe.

Introduction

1. The purpose of this Protocol is to improve the application of the principles contained in the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No.108, "the Convention") by adding two substantive new provisions, one on the setting up of one or more supervisory authorities by each Party and one on transborder flows of personal data to countries or organisations which are not parties to the Convention.

2. The Consultative Committee set up by virtue of Article 18 of the Convention prepared this draft Protocol at its 15th meeting held from 16 to 18 June 1999. It was submitted to the Committee of Ministers on the proposal of the Consultative Committee for transmission to the Parliamentary Assembly. The Consultative Committee considered the draft in the light of the Opinion adopted by the Assembly, on 5 April 2000, and then adopted the draft Protocol at its 16th meeting, from 6 to 8 June 2000. The Committee of Ministers adopted the additional Protocol on 23 May 2001.

Commentary concerning the provisions of the Protocol

Preamble

3. Improving the application of the principles set forth in the Convention 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.

4. This 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.

5. Effective application of the principles of the Convention necessitates the adoption of appropriate sanctions and remedies (Article 10). Most countries which have data protection laws have set up supervisory authorities, generally a commissioner, a commission, an ombudsman or an inspector general. These data protection supervisory authorities provide for an appropriate remedy if they have effective powers and enjoy genuine independence in the fulfilment of their duties. They have become an essential component of the data protection supervisory system in a democratic society.

6. 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.

Article 1 – Supervisory authorities

Paragraph 1

7. Article 10 of the Convention requires the establishment of appropriate remedies in the relevant legal provisions of each Party in respect of violations of provisions of domestic law giving effect to the principles of the Convention. However, it does not explicitly require the Parties to establish supervisory authorities to monitor compliance on their territory with the measures giving effect to the principles set forth in Chapters II and III of the Convention and in this Protocol. The first article of this Protocol has in this context a dual aim.

8. It aims to enforce the effective protection of the individual by requiring the Parties to create one or more supervisory authorities that contribute to the protection of the individual's rights and freedoms with regard to the processing of personal data. More than one authority might be needed to meet the particular circumstances of different legal systems. These authorities may exercise their tasks without prejudice to the competence of legal or other bodies responsible for ensuring respect of domestic law giving effect to the principles of the Convention. The supervisory authorities should have the necessary technical and human resources (lawyers, computer experts) to take prompt, effective action in a person's favour.

9. The article also aims to achieve improved harmonisation of the rules governing the supervisory authorities already established in respect of Parties to the Convention. In principle, all the Parties to the Convention shall provide in their domestic legislation for the establishment of one or more supervisory authorities. Depending on the national legal system, however, their composition, powers and *modus operandi* differ considerably from one country to another.

10. The aforementioned harmonisation not only aims at improving the level of data protection in the Parties but also aims at achieving closer co-operation between the Parties, without prejudice to the co-operation system set up by the Convention.

Paragraph 2

11. Parties have considerable discretion as to the powers which the authorities should be given for carrying out their task. According to the Protocol, however, they must at least be given powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities any violations of the relevant provisions.

12. The authority shall be endowed with powers of investigation, such as the possibility to ask the controller ⁽¹⁾ for information concerning the processing of personal data and to obtain it. Such information should be accessible in particular when the supervisory authority is approached by a person wishing to exercise the rights provided for in domestic law, by virtue of Article 8 of the Convention.

13. The supervisory authority's power of intervention may take various forms in domestic law. For example, the authority could be empowered to oblige the controller of the file to rectify, delete or destroy inaccurate or illegally collected data on its own account or if the data subject is not able to exercise these rights himself/herself. The power to issue injunctions on controllers who are unwilling to communicate the required information within a reasonable time would be a particularly effective manifestation of the power of intervention. This power could also include the possibility to issue opinions prior to the implementation of data processing operations, or to refer cases to national parliaments or other state institutions. The supervisory authority should have the power to inform the public through regular reports, the publication of opinions or any other means of communication.

14. Whilst contributing to the protection of individual rights, the supervisory authority also serves as an intermediary between the data subject and the controller. In this context, it seems particularly important that the supervisory authority should be able to provide information to individuals or data users about the rights and obligations concerning data protection. Moreover, every person should have the right to lodge a claim with the supervisory authority concerning his/her rights and liberties in respect of personal data processing. For the reasons referred to in paragraph 7 of this Explanatory Report, this lodging of a claim helps to guarantee people's right to an appropriate remedy, in keeping with Article 10 and Article 8 paragraph d. of the Convention. It is recalled that every person has a judicial remedy. However, domestic law may provide for the lodging of a claim with the supervisory authority as a condition of this judicial remedy.

15. The Parties should give to the supervisory authority the power either to engage in legal proceedings or to bring any violations of data protection rules to the attention of the judicial authorities. This power derives in particular from the power to carry out investigations, which may lead the authority to discover an infringement of a person's right to protection. The Parties may fulfil the obligation to grant this power to the authority by enabling it to make judgments.

16. The supervisory authority's competences are not limited to the ones listed in Article 1 paragraph 2. It should be borne in mind that the Parties have other means of making the task of the supervisory authority effective. It could be possible for associations to lodge complaints with the authority, in particular when the rights of the persons that it represents are restricted in accordance with Article 9 of the Convention. The authority could be entitled to carry out prior checks on the legitimacy of data processing operations and to keep a data processing register open to the public. The authority could also be asked to give its opinion when legislative, regulatory or administrative measures concerning personal data processing are in preparation, or on codes of conduct.

(1) Or "controller of the file".

Paragraph 3

17. Supervisory authorities cannot effectively safeguard individual rights and freedoms unless they exercise their functions in complete independence ⁽¹⁾. A number of elements contribute to safeguarding the independence of the supervisory authority in the exercise of its functions. These could include the composition of the authority, the method for appointing its members, the duration of exercise and conditions of cessation of their functions, the allocation of sufficient resources to the authority or the adoption of decisions without being subject to external orders or injunctions.

Paragraph 4

18. As a counterpart to this independence it must be possible to appeal against the decisions of the supervisory authorities through the courts in accordance with the principle of the rule of law when these decisions give rise to complaints.

19. Moreover, in cases where the supervisory authority does not itself have judicial competence, the intervention of a supervisory authority shall not constitute an obstacle to the possibility for the individual to have a judicial remedy.

Paragraph 5

20. Strengthening co-operation between the supervisory authorities must contribute to the development of the level of protection in the Parties' practice under the Convention. This co-operation is in addition to the mutual assistance provided for in Chapter IV of the Convention and the work of the Consultative Committee. Its purpose is to provide improved protection to the people concerned. With increasing frequency people are directly affected by data processing operations which are not confined to one country and therefore involve the laws and authorities of more than one country. The development of international electronic networks and increasing cross-border flows in the service industries and the work environment are examples. In such a context international co-operation between supervisory authorities ensures that people are able to exercise their rights on an international as well as a national level.

Article 2 – Transborder flows of personal data to a recipient which is not subject to the jurisdiction of a Party to the Convention

21. Article 12 of the Convention 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. This implies, in particular, that the principles of the Convention have been implemented.

22. Transborder flows of personal data to a recipient which is not subject to the jurisdiction of a Party are only indirectly concerned. According to Article 12 paragraph 3b, a country may derogate from the principle of the free circulation of data between its territory and a recipient which is not subject to the jurisdiction of a Party via another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party of origin. There is therefore no specific provision on transborder flows of data in respect of states or organisations which are not Parties to the Convention.

(1) In respect of the procedural guarantees set forth in Article 8 of the European Convention on Human Rights, the case law of the organs of this Convention already considers the intervention of an independent body, in certain circumstances, as a guarantee of "effective supervision" of the need for an interference by a public authority with the exercise of the rights provided by Article 8 (cf Gaskin vs United Kingdom, decision of 7 July 1989, series A no. 160, § 49).

23. It follows that the Parties to the Convention might make provision in their legal systems for the explicit authorisation of transfers of personal data to a recipient which is not subject to the jurisdiction of a Party with a different level of protection to the Convention. At the time this Protocol was drafted, even though they were under no explicit obligation to do so, some Parties had introduced rules into their domestic law concerning the transfer of data to a recipient which was not subject to the jurisdiction of a Party. Differences in practice, particularly in the light of the above-mentioned Article 12 paragraph 3b, could lead to substantial restrictions on the free circulation of data between the Parties, which would also be contrary to the purpose of the Convention. It is therefore necessary, in the light of specific provisions in Council of Europe Recommendations on data protection, to establish common rules concerning transborder flows of personal data to a recipient which is not subject to the jurisdiction of a Party.

24. Such a measure is determined on the one hand by the will to guarantee effective protection of personal data outside national borders and, on the other, by the Parties' determination to ensure the free circulation of information between peoples, in accordance with the wording of the Preamble to the Convention.

Paragraph 1

25. Transborder flows of data to a recipient which is not subject to the jurisdiction of a Party are subject to the condition of an *adequate* level of protection in the recipient country or organisation. Paragraph 70 of the explanatory report to the Convention refers to "non-Contracting States (having) a *satisfactory* data protection regime". A recipient which is not subject to the jurisdiction of a Party to the Convention could only be regarded as having a satisfactory data protection regime if it afforded an adequate level of protection.

26. The adequacy of the level of protection must be assessed in the light of all the circumstances relating to the transfer.

27. The level of protection should be assessed on a case-by-case basis for each transfer or category of transfers 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.

28. 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.

29. The assessment of an adequate level of protection must take into account the principles of Chapter II of the Convention and of this Protocol and the extent to which they are met in the recipient country or organisation – as far as they are relevant for the specific case of transfer – and how the data subject can defend his or her interests in case of non compliance in a specific case.

30. The Consultative Committee of the Convention may, at the request of one of the Parties, give an opinion on the adequacy of the level of data protection in a third country or organisation.

Paragraph 2.a

31. 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.

Paragraph 2.b

32. 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.

33. 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.

Article 3 – Final provisions

34. According to the conventional practice of the Council of Europe, an additional Protocol to a Convention can only be signed by the Signatories to the Convention itself. The European Communities, which have participated in the elaboration of the present Protocol, may sign this Protocol after acceding to the Convention under the conditions provided by it.

35. Paragraph 2 of Article 3 only applies to Council of Europe member States and to the European Communities. Paragraph 4 only applies to non-member States of the Council of Europe, which can only accede to the Protocol as well as to the Convention.

36. Paragraph 3 fixes at five the number of ratifications necessary for the entry into force of the Protocol, corresponding to the provisions of Article 22 of the Convention.

37. The provisions in paragraphs 3 to 6 are in conformity with the final clauses of the Convention and with the customary final clauses contained in Council of Europe conventions and protocols.