Report on the Impact of Data Protection Principles on Judicial Data in Criminal Matters including in the framework of Judicial Co-operation in Criminal Matters (2002)

FOREWORD

1. During its 74th meeting, the European Committee on Legal Co-operation (CDCJ) adopted the draft revised terms of reference of the Project Group on Data Protection (CJ-PD) for 2001 and 2002. The Committee of Ministers subsequently adopted these revised terms of reference, as they appear in document CJ-PD (2000) 3 rev 4, at its 740th meeting. According to these adopted terms of reference, the CJ-PD is instructed:

> "*to consider, before the end of 2001, the impact of data protection principles, on the one hand on judicial co-operation, and on the other hand on police co-operation, in criminal matters, in particular, by the Working Party on data protection and police and judicial co-operation in criminal matters (CJ-PD/GT-CP).*"

2. In order to specify and more clearly define the subjects to be dealt with, taking into account that exchanges of data by the judiciary within the framework of judicial co-operation in criminal matters by mutual assistance are one particular aspect of information processing and this does not, therefore, cover all activities involving the processing of personal data in the judicial field, the CJ-PD decided to slightly change the name of the new working party to the "Working Party on data protection and police and judicial data in criminal matters" (CJ-PD/GT-PJ) [see docs CJ-PD-GC (2001) RAP 7 and CJ-PD (2001) RAP 39]. The CDCJ and its Bureau were informed about this change of name (see paragraph 35 of document CDCJ-Bu (2002) 8) The CJ-PD also underlined that when the CJ-PD/GT-PJ examined the impact of data protection principles on judicial co-operation in criminal matters, it should pay particular attention to the common principles that should be taken into account in answering mutual legal assistance requests from countries that do not have an adequate level of data protection.

3. According to the above-mentioned terms of reference, the CJ-PD was also instructed to "*prepare the evaluation of Recommendation No. R (87)15 on the use of personal data in the police sector, which shall be transmitted to the Committee of Ministers by 2002, at its request and through the CDCJ*".

4. In view of the close links between the tasks of the Working Party and the content of Recommendation No. R (87)15, the CJ-PD entrusted the CJ-PD/GT-PJ with the preparation of a draft report on the third evaluation of this Recommendation to be submitted to the CJ-PD at its 40th plenary meeting in 2002 for revision and approval. The CJ-PD instructed its Working Party to take account of the following in the preparation of this draft report: the previous two evaluations; the Regional Seminar on "Data Protection in the Police Sector" organized by the Council of Europe in 1999 in the framework of its "Activities for the Development and Consolidation of Democratic Stability" (ADACS) and as a contribution to the Stability Pact for South-East Europe; the results of the "Fight Against Crime and Personal Data Protection Project" (FALCONE Programme) which was launched on the initiative of the Italian and Portuguese Data Protection Commissions and approved and sponsored by the Commission of the European Communities; as well as any developments since the last evaluation, in particular with regard to the case law of the European Court of Human Rights in this matter.

5. In accordance with the above-mentioned instructions, the CJ-PD/GT-PJ prepared both the present draft report on the impact of data protection principles on judicial data in criminal matters,

including in the framework of judicial co-operation in criminal matters, and the preliminary draft report on the third evaluation of Recommendation No. (87)15 regulating the use of personal data in the police sector. Both reports were submitted to the CJ-PD at its 40th plenary meeting from 7 to 9 October 2002 for examination and approval.

6. The CJ-PD examined and revised the draft report on the impact of data protection principles on judicial data in criminal matters including in the framework of judicial co-operation in criminal matters during its 40th plenary meeting. The CJ-PD unanimously adopted this report, except paragraph 34 (under the Principle of Proportionality) where a dissenting opinion was expressed by the Swedish delegation in relation to the deletion of the excessive data which in its opinion are contrary to the Swedish constitutional rules on the rights of access to public documents. The CJ-PD invited the CDCJ to approve, subject to any amendments it might wish to make, the draft report on the impact of data protection principles on judicial data in criminal matters including in the framework of judicial co-operation in criminal matters and to authorise the publication of this report on the Council of Europe's data protection website.

7. In view of the multidisciplinary composition[1] of the Working Party (CJ-PD/GT-PJ) which prepared the draft of this report, as well as the issues concerned (police and judicial data in criminal matters), the CJ-PD invited the CDCJ to send the final version of this report for information to the European Committee on Crime Problems (CDPC) and, subject to the agreement of the CDPC, to its relevant subordinate committees, in particular the Committee of Experts on Police Ethics and Problems of Policing (PC-PO) and the Committee of Experts on the Operation of European Conventions in the Penal Field (PC-OC).

* * *

DRAFT REPORT ON THE IMPACT OF DATA PROTECTION PRINCIPLES ON JUDICIAL DATA IN CRIMINAL MATTERS, INCLUDING IN THE FRAMEWORK OF JUDICIAL CO-OPERATION IN CRIMINAL MATTERS

INTRODUCTION

8. Twenty years after the opening for signature of the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* [ETS No. 108] of the Council of Europe (henceforth Convention 108), questions arise about the practical impact of data protection principles in the judicial context (the processing of data by judicial authorities including their processing in the context of mutual co-operation). A recent institutional reflection started within the European Union during the negotiations of the *Convention on Mutual Assistance in Criminal Matters between the*

[1] The following four experts were appointed by the CJ-PD :
- Mr Marc BUNTSCHU, Switzerland (Deputy Head of the Secretariat of the Swiss Data Protection Officer)
- Mr Giovanni BUTTARELLI, Italy (Secretary General of the *Garante per la Protezione dei Dati Personali*)
- Mr Alexander PATIJN, Netherlands (Legal Adviser at the Ministry of Justice)
- Ms Kinga SZURDAY, Hungary (Senior Legal Counsellor at the Ministry of Justice).

In accordance with the terms of reference from the CJ-PD, the European Committee on Crime Problems (CDPC) and its relevant subordinate committees could also participate in the composition of the CJ-PD/GT-PJ. Therefore, the other three experts of the CJ-PD/GT-PJ were appointed by the following committees:
- The European Committee on Crime Problems (CDPC) appointed Mr Hughes BRULIN, Belgium (Deputy Legal Adviser, Directorate General on Penal and Human Rights Legislation, Ministry of Justice).
- The Committee of Experts on Police Ethics and Problems of Policing (PC-PO) appointed Ms Elenor GROTH, Sweden (Legal Adviser, Ministry of Justice)
- The Committee of Experts on the Operation of European Conventions in the Penal Field (PC-OC) appointed Mr Philippe BIJU-DUVAL, France (Bureau de Droit Pénal Européen et International, S.A.E.I., Ministry of Justice).

member States of the European Union of 29 May 2000 (Official Journal of the European Communities, Series C 197, 12/07/2000). At the same time, the seminars organised in the framework of the "Fight Against Crime and Personal Data Protection Project" (FALCONE Programme), which was launched on the initiative of the Italian and Portuguese Data Protection Commissions and approved and sponsored by the Commission of the European Communities, also dealt with the impact of the data protection principles on data held by judicial authorities. Furthermore, during the *Conference on protecting society from organised crime* organised by the Council of Europe, the Italian anti-Mafia Directorate and the University of Naples II (8-10 September 2000, Caserta (Italy)), the European prosecutors stressed the need for every European state to set up a central data bank in matters of organised crime where information supported by evidence would be gathered; but they went on to note that restrictions had to be imposed on the exchange of information across borders, in order to respect individual rights, particularly concerning personal data. They asked the Council of Europe to establish a committee of experts to consider these issues and make appropriate recommendations. The need for specific provisions in this field was also recalled during the discussions setting up Eurojust in the framework of the European Union[2].

9. Therefore, the issue of the impact of data protection principles on data held by judicial authorities, including the exchange of information across borders in the framework of mutual legal assistance, is at present a topical issue which needs further examination. With this aim, the Project Group on Data Protection (CJ-PD) set up a working party to examine these issues.

10. Under Article 3 of Convention 108 "The Parties undertake to apply this Convention to automated personal data files and automated processing of personal data in the public and private sectors". Therefore, the Convention applies to the personal data of persons involved in the judicial procedure which are automatically processed by the judiciary if the Party to the Convention has not excluded these categories of automated personal data files from the scope of application of the Convention in accordance with Article 3.2.a of Convention 108. Furthermore, Convention 108 will also apply to the personal data of persons involved in the judicial procedure which are not processed automatically by the judiciary if the Party to the Convention has made the declaration mentioned in Article 3, paragraph 2, littera c.

11. However, only recently has the possible application of the data protection principles to personal data held by the judiciary become an issue. This can be explained in practical terms by the specific rules of information management observed in the judicial field for many years and, more particularly, by the existence of national codes of criminal procedure. Since the majority of these codes were drafted at a time when computer systems were unknown or limited to technical sectors, the combination of national rules on prosecution with respect for the principle of a fair trial naturally led prosecutors, magistrates and judges of European countries to process data essentially in manual files or dossiers. Convention 108, which was drafted to apply to the collection and processing of information which would be consulted frequently, was not drafted in view of the classical "handling" of information only on the occasion of an investigation or a trial, above all taking into account that the automatic processing of personal data has only recently been introduced in the judicial field.

12. Even if Convention 108 was intended to apply to the judicial field, it is true that the data protection principles are not often applied in this field. There are, however, some specific legal provisions that could serve the same aim, although they are not data protection provisions *per se*.

[2] The Commission of the European Communities is currently considering bringing forward European Union legislation on the issue of data protection in the context of police and judicial co-operation with a view to making a proposal.

For example, although national criminal codes are not specifically designed with data protection in mind, many of their rules, such as safeguards for accused persons, rules for collecting evidence, balance of interests in a fair trial, can have the same effects as data protection principles. Furthermore, when national codes of criminal procedure have been adopted or substantially reviewed during the last two decades they have often included specific provisions for protecting the personal data held by judicial authorities.

13. For almost fifteen years, the development of new information technologies in every sector of society has increased parallel to the interest of law enforcement agencies in the prosecution of organised crime at the international level. Consequently, the judicial authorities of European states have created contacts and co-operate by means of the new information technologies: for instance, consulting legal or case law databases; using ad hoc "paragraph libraries" in order to draft judgments and decisions; storing specific data when conducting an investigation; exchanging information (or even letters rogatory) at international level by e-mail.

14. The above-mentioned reasons underline the need to examine the impact of data protection principles in the judicial sector. This applies in particular to the processing of information collected on the basis of intrusive methods (such as telecommunication interceptions) or using methods facilitating the use of DNA tests.

15. Therefore, the Project Group on Data Protection (CJ-PD) prepared this report. The report is divided into two main parts: the first part analyses the impact of data protection principles on data processed in the judicial field, in particular in relation to specific questions raised in practice at a national level (I. THE IMPACT OF DATA PROTECTION PRINCIPLES ON JUDICIAL DATA IN CRIMINAL MATTERS). The second part analyses the impact of data protection principles on international judicial co-operation in criminal matters (II. THE IMPACT OF DATA PROTECTION PRINCIPLES ON MUTUAL LEGAL ASSISTANCE IN CRIMINAL MATTERS).

16. It should be remembered that, to the extent that the report refers to safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, as established by Articles 5, 6 and 8 of Convention 108 and Article 8 of the ECHR, derogations from such rights, in accordance with Article 9 of Convention 108, which were elaborated on the basis of Article 8 of the ECHR, are possible where they are provided for by law and constitute a necessary measure in a democratic society in the interests of :

a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;
b. protecting the data subject or the rights and freedoms of others.

I. THE IMPACT OF DATA PROTECTION PRINCIPLES ON JUDICIAL DATA IN CRIMINAL MATTERS

Preliminary remarks:

The approach of the Project Group

17. In accordance with its terms of reference, the CJ-PD was instructed "to consider, before the end of 2001, the impact of data protection principles, on the one hand on judicial co-operation, and on the other hand on police co-operation, in criminal matters […]". Taking into account these terms of reference, the CJ-PD examined the impact of the data protection principles in the judicial field and reached some conclusions on this issue.

18. Under criminal procedure, the same personal data may be processed, at the same time, even in identical documents, by the police and the judicial authorities. Telephone tapping provides an illustration of the mixed nature of some data: a judge may authorise telephone tapping but the data are then collected by the police before the data are transferred again to a judicial authority. In these cases there is the risk of a grey area where some police data go to the judicial sector and some judicial data remain in the police sector. This can give rise to confusion in qualifying data as judicial or police data. This must not be used as a loophole for not applying the data protection principles in these sectors, or for avoiding determining who is controller of the file or the degrees of responsibility for each processing operation. It is however clear that each level of authority must respect its own rules.

19. Criteria must be found to determine which specific rules are to be applied. To this end, in accordance with Article 2.d of Convention 108, the controller of the file "means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them". Therefore, national law should clearly determine whether the controller of the data file is the police or the judicial authority. Furthermore, the purpose of processing can also serve as a complementary criterion.

20. Taking the above considerations into account, the following conclusion was reached:

In order to make a distinction between judicial and police data, it should be advisable to make explicit who is the controller of the file in the sense of Article 2, paragraph 2, littera d. of Convention 108 with regard to judicial data and police data. The controller of the file in this sense need not necessarily be the same as the authority who, according to the code of criminal procedure, is responsible for making decisions on or conducting criminal investigations. Special care should be taken to avoid loopholes in responsibility, in particular when personal data are collected and used by the police following an order from the judiciary to use intrusive surveillance methods such as interception of telecommunications.

21. The CJ-PD also underlined that exchanges of data by the judiciary in the framework of judicial co-operation in criminal matters by mutual assistance are one particular aspect of the processing of information and this does not therefore cover all activities involving the processing of personal data in the judicial field. The principles below therefore also apply to other activities involving the processing of personal data by the judicial authorities.

22. The CJ-PD examined the application of the main data protection principles in the framework of mutual legal assistance in criminal matters (see the second part of this report)**.**

23. The scope of application of this examination is limited to the processing of personal data in judicial procedures in criminal matters and does not include the processing of personal data in the framework of civil or administrative judicial matters. The impact of data protection principles on the processing of information by police services is contained in the report devoted to the third evaluation of Recommendation No. (87) 15 regulating the use of personal data in the police sector.

Data protection and criminal procedure: a common aim?

24. It is possible that the data protection principles are not yet fully applied in the judicial field (since they may not be applicable). As mentioned above, there are, however, some specific legal provisions that could serve the same aim, although they are not data protection provisions *per se*.

For example, although national criminal codes are not specifically designed with data protection in mind, many of their rules, such as safeguards for accused persons, rules for collecting evidence, balance of interest in a fair trial, can have the same effects as data protection principles.

Data protection principles

a) Principle of lawfulness of processing

> *Personal data undergoing(…) processing shall be*
> *a. obtained and processed fairly and lawfully;*
> (Convention 108, Art. 5.a)

25. This principle requires that the public authorities only process personal data if they have been authorised to do so by law.

26. In relation to the processing of personal data by judicial authorities, it should be taken into account that a complete register of criminal convictions may only be kept under the control of the official authority.

27. Having in mind the possible impact of data protection principles in the judicial context, does this principle, combined with the principle of transparency, require that in every case judicial authorities should have specific legal authorisation for processing data in the pursuit of their legitimate purposes?

28. In some countries, legislation on data protection does not apply to pending proceedings; instead there are specific data protection provisions in the code of criminal procedure. More generally, the provisions of national codes of criminal procedure require judicial authorities to accomplish their missions of prosecution or of judgment without explicit references to data processing or to a complete listing of specific purposes. In this respect, it must be acknowledged that traditional provisions in codes of criminal procedure which were not drafted with data protection principles in mind can nevertheless fulfil the data protection requirements of Convention 108, in particular when they specify the purposes of the activities of the judicial authorities, or even when they develop these activities more generally without providing a specific authorisation to set up data processing. Therefore, it would be advisable that national legislators in all the Parties to Convention 108 examine this problem.

29. In relation to the application of the data protection principle of lawfulness to the processing to judicial data, the following conclusion was reached:

There is no need to create specific legal rules authorising the judicial authorities to process personal data, in every case, in order to fulfil the requirements of the lawfulness principle when provisions in criminal procedure codes already provide such rules.

b) Principle of finality/ purpose

> "*Personal data undergoing (…) processing shall be stored for specified and legitimate purposes and not used in a way incompatible with those purposes"* (Convention 108, Art. 5.b)

30. This principle requires that data are not processed subsequently for incompatible purposes.

31. Having in mind the possible application of this principle in the judicial context, the problem is how to define what is compatible and what is not (see for instance Article 23.1.b of the *Convention on Mutual Assistance in Criminal Matters between the member States of the European Union* of 29 May 2000). For example, can a judge re-use data in civil proceedings (e.g. divorce proceedings) that were initially collected in relation to a criminal case on assault between the same married couple?

32. Re-use for the purposes of civil proceedings could present some problems of compatibility of purpose. In many of those civil cases, parties will provide the relevant data themselves. Re-use for administrative purposes might be more problematic. The re-use of data collected for a specific criminal case in an administrative case (e.g. customs, labour inspection and taxation issues, etc.) should be considered incompatible if there is no concrete link. This does not exclude that the exceptions and the derogations of Article 9 of Convention 108 might apply. The Working Party agreed to use the words "directly related" which appear in Article 23.1.b of the *Convention on Mutual Assistance in Criminal Matters between the member States of the European Union* of 29 May 2000.

33. In relation to the application of the data protection principle of finality to the processing of judicial data, the following conclusion was reached:

When considering if the re-use of personal data collected in the framework of a judicial criminal case is compatible with the original purpose, special consideration could be given to whether:
1) the judicial criminal case and the judicial civil case for which the data are re-used are directly related;
2) the judicial criminal case and the administrative case for which the data are re-used are directly related.
If the purpose for which the data are to be re-used is not compatible with the purpose for which the data were collected, the exceptions under Article 9 of Convention 108 could be applied.

c) Principle of proportionality

> "*Personal data undergoing (…) processing shall be adequate, relevant and not excessive in relation to the purposes for which they are stored "* (Convention 108, Art. 5.c)

34. The need for each category of data to be collected and further processed should be examined according to the purposes for which they will be processed. The principle of proportionality, which is very closely related to the principle of necessity, implies that data undergoing processing must not be excessive with regard to the purposes for which they are collected and used subsequently.

35. It is not advisable to transpose the principles of necessity and proportionality to collection of data by judicial authorities without first clarifying the real meaning of these terms. In the case law of some national data protection commissions, "necessary" is strictly interpreted as something which is indispensable (in order to be collected, for instance). However, information which may be considered necessary at the time of its collection by a judicial authority may subsequently be found to be irrelevant in the light of developments of the inquiry.

36. These principles of necessity and proportionality should then be assessed in a global way, keeping in mind the different processing operations performed during the whole procedure

(prosecution and judgment of a criminal offence), with the establishment of the truth during a fair trial as the main goal. This includes the preservation of possibly exculpatory evidence and information about the process of gathering data. In many cases, the decision on necessity or proportionality of data can only be taken at a later stage, after the data have already been collected. If the judicial authority is of the opinion at the time of collection that the data are excessive they should be deleted; if not, they may be kept and the question of the length of storage should then be examined.[3]

37. The question of the spontaneous exchange of information between judicial authorities (of the same country or of different countries) was raised as a particular application of the principle of proportionality. According to some opinions on mutual judicial assistance in criminal matters, this principle was already presupposed on the basis of Article 21 of the *European Convention on Mutual Assistance in Criminal Matters* [ETS. No. 30] of 20 April 1959. The spontaneous exchange of judicial information is explicitly mentioned in Article 7 of the *Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union* of 29 May 2000.

38. In relation to the application of the data protection principle of proportionality to the processing of judicial data, the following conclusion was reached:

The principle of proportionality with respect to the processing of data should also be applied to the judicial field. However, this principle should be assessed with due flexibility, with a global view of all the processing operations performed during the prosecution and judicial criminal proceedings. The exigencies of a fair trial and the need to preserve possibly exculpatory data put limits of predictability on the need for information by the authorities conducting these activities.

d) Principle of the length of conservation

> *"Personal data undergoing (…) processing shall be preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored"* (Convention 108, Art. 5.e)

39. According to this principle, data must be kept for no longer than is necessary. This does not mean the shortest period in general but the shortest one in accordance with the purposes of the data collection.

40. Judicial authorities may process personal data for prosecution purposes when they are conducting inquiries with a view to the suppression of criminal offences. In this context, the nature of the data processing (including the length of conservation) is to a certain extent close to that of police services and can follow the common rules set out in Principle 7.1 of Recommendation No. R (87) 15. However the collection and processing of personal data by judicial authorities is often intended to be used as the basis for judicial proceedings (trial) and judicial decision (judgment). In this context, the Working Party considered that files of the judicial authorities could be kept for a longer period because they might be necessary in a review procedure. Where national law provides a time limit for the institution of these review proceedings, this period set by law indirectly determines the length of storage. If national law does not determine any specific time limit, the extension of the period of storage should be considered as the question might always arise of the

[3] The CJ-PD could not reach a unanimous decision in relation to this paragraph. The Swedish delegation indicated a dissenting opinion because they considered that the deletion of excessive data is contrary to the Swedish constitutional rules on the right of access to public documents. The CJ-PD took an indicative vote on this issue. 14 delegations were in favour of keeping the text as it is and 10 delegations were in favour of changing the text.

correction of miscarriages of justice. In this connection, attention should be paid to Council of Europe Recommendation No. R (84) 10 on the criminal record and rehabilitation of convicted persons, and in particular to its paragraph 13 which provides that "rehabilitation implies prohibition of any reference to the convictions of a rehabilitated person except on compelling grounds provided for in national law".

41. In relation to the application of the data protection principle of length of conservation of data to the processing of judicial data, the following conclusion was reached:

Personal data used as the basis for a judicial decision may be stored in files of the judicial authorities for as long as they are necessary to fulfil the requirements of the judicial procedure. When the data are no longer necessary to fulfil the requirements of the judicial procedure for which they were collected, they should only be kept for the purposes of judicial review procedures or for the purposes of historical, scientific or statistical research. Their storage should be accompanied by appropriate safeguards and security measures to prevent their use for other purposes.

e) Principle of transparency

> *"Personal data undergoing automatic processing shall be […] obtained and processed fairly and lawfully" (Convention 108, Art. 5.a)*
>
> *"Any person shall be enabled:*
> *a. to establish the existence of a (…) personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;*
> *b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the (…) data file as well as communication to him of such data in an intelligible form" (Convention 108, Art. 8.a and b).*

42. The principle of transparency can be given effect by providing information to data subjects about the collection and use of their data unless they already know this or it would involve disproportionate effort. The CJ-PD noted that, in practice, third parties are often not correctly informed about their data mentioned in judicial files.

43. This principle should also be respected in the judicial context, and therefore judicial authorities should inform persons whose data are included in a judicial file where this does not involve disproportionate effort, especially where intrusive methods, such as interception of telecommunications or e-mail messages and search and seizure of computer data, have been used. In relation to the communication of this information, account should be taken of the different degree of infringement of the privacy of the different persons involved (suspects, third parties, etc…). Data subjects can be informed on the initiative of a judicial authority, by the notification of the competent data protection supervisory authority or even by providing clear information on the criteria for collecting and processing information. It is also assumed that after the conclusion of a criminal investigation, the information of data subjects can no longer be precluded on the grounds that the investigation might be jeopardised. Although the rules of a fair trial may simultaneously safeguard the data protection rights of the accused person, they do not necessarily also safeguard the rights of other persons involved in the case, such as witnesses or victims.

44. Taking into account the above-mentioned considerations, the following conclusion was reached:

In principle, people whose data are included in a judicial file should be informed. Notification is particularly important where measures which interfere with privacy have directly affected the data subject.

f) Right of access

> *"Any person shall be enabled:*
> *(…)*
> *b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the (…) data file as well as communication to him of such data in an intelligible form;" (Convention 108, Art. 8.b).*

45. The right of the data subject to have access to his or her personal data is one of the best-known data protection principles. In the context of judicial data, access should be granted to any data subject who requests access to the judicial file, whether on the basis of the provisions of criminal procedure codes or on the basis of data protection legislation.

46. Problems may arise when personal data are transferred to other countries because the same data would be held under different national or international legislation. The exchange of data in international information systems such as Schengen or Europol has already demonstrated the risk of "forum shopping" with regard to this issue: data subjects are naturally led to request access in the country where the transparency of information is the greatest. If national rules require granting the right of access to data, the information which is exchanged comes under different access rules, taking into account that the right of access must be exerted in accordance with the law of the country where access is requested. Therefore judicial authorities should pay attention to the fact that, if data to which data subjects might not have access in their countries are communicated to another country, the regime in that other country might not necessarily be the same. In principle the substantive criterion is the same: the purpose for which the data have been collected should not be jeopardised. However, the application of this principle differs in different countries. This problem has been tackled in, for instance, Article 109, paragraph 1, of the Schengen Agreement, where the authorities of the communicating country must have the opportunity to state their point of view on a request by the data subject for access to his data. This point of view will be taken into account but is not necessarily decisive in the country where the right of access is exerted. Further international co-operation would be necessary if, in case of doubt, this rule became a more general practice.

47. Taking the above considerations into account, the following conclusion was reached:

If a data subject requests access with regard to data about him/her that have been communicated by judicial authorities of another country, the authorities of the originating country should be given the opportunity to state their point of view before the request is granted.

g) Principle of quality of data: right of rectification and erasure

> *"Personal data undergoing (…) processing shall be accurate and, where necessary, kept up to date" (Convention 108, Art. 5.d)*
> *"Any person shall be enabled:*

(…)

c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention " (Convention 108, Art. 8.c)

48. This principle requires that the data processed are accurate and, where necessary, kept up to date, as well as the rectification or erasure of incorrect data.

49. However, the collection of data for criminal proceedings may result in police reports or witness statements containing inaccuracies (even though they respect procedural rules), or even voluntary lies. These reports or statements form an integral part of the proceedings file and, according to national criminal procedure codes, it would be inconceivable for them to be rectified.

50. Such information can be considered correct because the statement in the report corresponds to what was really declared, although it might be wrong in that it refers to something which never happened or is impossible. These data must not be deleted for as long as the judicial files are kept. Moreover, judicial files can also include declarations by magistrates, representatives of law enforcement agencies, witnesses or victims forming a subjective assessment of the suspect. Finally, if data were collected by a judicial authority at a time when they were considered necessary, and have subsequently been found irrelevant, they must also be kept in the judicial dossier.

51. Personal data are also considered to be inaccurate or incorrect in the case where the data as such may be right but nevertheless yield a false picture if they are not completed by other relevant data. For instance, if the data establish that a person has been suspected of a crime, but was not prosecuted because he/she had a valid alibi, the data about the suspicion must be regarded as incorrect if not completed by the facts due to which he/she was subsequently not prosecuted.

52. It would be difficult to envisage correction of data with regard to the convicted person which are relevant for the conviction. This does not affect the fact that data about third persons are in the file. These may not be relevant for the conviction. Their correction may nevertheless be of interest to the data subject if, for instance, the data were used for a directly related administrative proceeding. Moreover, it must not adversely affect the final court decision.

53. Taking the above considerations into account, the following conclusion was reached:

Consideration should be given to whether the data subject's right of rectification and erasure with regard to data contained in judicial files can be granted in accordance with the relevant rules of the criminal procedure legislation. If incorrect data included in a judicial file are challenged by the data subject, he or she should have the right to add a statement to it stating the corrections. This statement should form an integral part of the judicial file.

h) Principle of independent supervision

"Article 1

"1. Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention and this Protocol.

2. a. To this end, the said authorities shall have, in particular, 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 violations of provisions of domestic law giving effect to the principles mentioned in paragraph 1 of Article 1 of this Protocol.

b. Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence.

3. The supervisory authorities shall exercise their functions in complete independence.

4. Decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts " (Additional Protocol to Convention 108, Art. 1, paragraphs1-4)

54. National data protection supervisory authorities have been set up in almost every European country. They are empowered to guarantee the respect of and to give effect in their domestic law to the principles set out in Convention 108, as well as in national data protection laws. They are, therefore, also competent to supervise, check and verify the proper implementation of these principles in different sectors. However, in some countries specific independent data protection supervisory authorities have been set up to control the exchanges of information between and the processing of data by judicial authorities. In these countries it was assumed, on the one hand, that the data protection supervisory authorities generally have no jurisdictional competence and that the principle of the separation of powers (legislative, executive and judicial) does not allow for the control of the activities of the judiciary. On the other hand, it was pointed out that judicial authorities collect and process personal data and this could also be the object of control by the data protection supervisory authorities. Convention 108 and its Additional Protocol will apply to the personal data of the persons involved in the judicial procedure which are processed by the judiciary unless Parties to those international instruments have made a declaration excluding these categories of data from their scope of application in accordance with Article 3.2.a of Convention 108.

55. Practice reveals an empirical separation of competence. For instance, the data protection supervisory authorities are empowered to check the lawfulness of the information systems and to submit proposals or recommendations to the judicial authorities, the former remaining competent to check the content of the information. In any case, both authorities should lead their specific control in a spirit of fair co-operation.

56. Moreover, national laws sometimes grant national supervisory bodies judicial powers equal to those of the judicial authorities since they resolve disputes between parties definitively. These laws generally establish the judicial authorities as appeal courts of the decisions given by the data protection supervisory bodies. Such provisions obviously reveal the limits of the powers of the data protection authorities with regard to the judicial authorities.

57. If in accordance with national law, due to the separation of powers, the general data protection authority is not competent with regard to judicial data pending criminal proceedings, the supervisory functions could be fulfilled by a judge.

58. Taking into account the above considerations, the following conclusion was reached:

States are free to appoint different public independent authorities to control and supervise the proper implementation of the rights set out in Convention 108 and in national data protection law. The distribution of competence with regard to these tasks between data protection

supervisory authorities and judicial authorities should be left to national law. These authorities should co-operate.
When data protection supervisory authorities are empowered with judicial powers by law, special attention should be paid to respect of the individual's rights, in particular the right to a fair trial.

i) Principle on security measures

> *"Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination" (Convention 108, Article 7).*

59. The principle of transparency requires that details about a file should be public, but this transparency does not necessarily include the personal data contained in the file.

60. In relation to this principle, the question of the publication of criminal verdicts on the Internet and on CD-ROM was raised. In some countries the names of the persons concerned are published on the Internet, in others they are made anonymous to prevent them from being digitally searchable. The new technological possibilities provided by the information society entail potential risks for the rights and fundamental freedoms of individuals. It was considered that, even though it may make people identifiable from details in the verdict, at least the compilation of verdicts should not enable them to be digitally searchable on the Internet or on CD-ROM. Legislative measures are necessary if these precautions do not flow from a general duty to protect personal data.

61. Taking into account the above considerations, the following conclusion was reached:

Judicial authorities should take into account the increased risk of infringement of the private life of data subjects when publishing judgments on Internet or making them available on CD-ROM. The necessary measures should be implemented to prevent unlawful digital search.

*** * ***

II. THE IMPACT OF DATA PROTECTION PRINCIPLES ON MUTUAL LEGAL ASSISTANCE IN CRIMINAL MATTERS

Preliminary provisions in mutual legal assistance treaties having an impact on data protection

62. Although the first explicit data protection provision in a treaty on mutual assistance appears in the *Convention on Mutual Assistance in Criminal Matters between the member States of the European Union* of 29 May 2000 there are some provisions in previous international instruments on this matter that have an impact on the protection of personal data.

63. In the context of the Council of Europe, issues related to mutual assistance are based on the *European Convention on Mutual Assistance in Criminal Matters* [ETS No. 30] of 20 April 1959 (henceforth European Mutual Assistance Convention). As there was no automated processing of personal data at that time, it is understandable that this European Mutual Assistance Convention

contains no data protection provision. Article 6, however, reflects the understanding by the drafters of an analogous situation: " […] Any property, as well as original records or documents, handed over in execution of letters rogatory shall be returned by the requesting Party to the requested Party as soon as possible unless the latter Party waives the return thereof".

64. *Recommendation No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of Letters rogatory for the interception of telecommunications* of 25 June 1985 makes explicit that "the evidence contained in the records resulting from the interception will not be used by the authorities of the requesting Party for purposes other that those underlying the letters rogatory in respect of which assistance has been granted" (item 4.d. of the Appendix to this Recommendation).

65. A third preliminary provision that precedes explicit data protection provisions is contained in Articles 8 and 9 of the United Nations *Model Treaty on Mutual Assistance in Criminal Matters* adopted by the General Assembly on 14 December 1990 (A/RES/45/117). Article 8 deals with limitation on use: the information or evidence shall not be used for other investigations or proceedings than those stated in the request. Article 9 deals with the protection of confidentiality which might also have as a result the protection of personal data. On 20 January 1999, the General Assembly of the United Nations adopted a Resolution on *Mutual Assistance and International Co-operation in Criminal Matters* (A/RES/53/112) which contains complementary provisions for the *Model Treaty on Mutual Assistance in Criminal Matters.*

Explicit data protection provisions in the mutual legal assistance treaties

66. The *Convention on Mutual Assistance in Criminal Matters between the member States of the European Union* of 29 May 2000 contains the first explicit data protection provisions. Article 23 of this Treaty contains a data protection provision of a general nature:

> *"Article 23 – Personal Data Protection*
>
> *1. Personal data communicated under this Convention may be used by the Member State to which they have been transferred:*
> *for the purpose of proceedings to which this Convention applies;*
> *for other judicial and administrative proceedings directly related to proceedings referred to under point (a);*
> *for preventing an immediate and serious threat to public security;*
> *for any other purpose, only with the prior consent of the communicating Member State, unless the Member State concerned has obtained the consent of the data subject.*
> *2. This Article shall also apply to personal data not communicated but obtained otherwise under this Convention.*
> *3. In the circumstances of the particular case, the communicating Member State may require the Member State to which the personal data have been transferred to give information on the use made of the data.*
> *4. Where conditions on the use of personal data have been imposed pursuant to Articles 7(2), 18(5)(b), 18(6) or 20(4), these conditions shall prevail. Where no such conditions have been imposed, this Article shall apply.*
> *[…] »*

67. Specific data protection provisions are contained in Article 7 (2) concerning spontaneous exchange of information (spontaneous exchange of information can be subjected to conditions on the use of such information by the receiving authority); in Article 13 concerning joint investigation

teams (there is a limitation in paragraph 10 on the use of information gathered by a joint team to the purpose for which the team was set up); in Articles 18 (5) and (6) and Article 20 on the interception of telecommunications which allow states to set conditions to the use of intercepted materials.

68. In the context of the Council of Europe, the *Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters* [ETS No. 182] was opened for signature on 8 November 2001. This Second Additional Protocol contains an explicit data protection provision in Article 26:

> "Article 26 – Data Protection
> *1. Personal data transferred from one Party to another as a result of the execution of a request made under the Convention or any of its Protocols, may be used by the Party to which such data have been transferred, only:*
> *(a) for the purpose of proceedings to which this Convention applies or any of its Protocols apply;*
> *(b) for other judicial and administrative proceedings directly related to the proceedings mentioned under (a), and*
> *(c) for preventing an immediate and serious threat to public security.*
> *2. Such data may however be used for any other purpose if prior consent to that effect is given by either the Party from which the data had been transferred, or the data subject.*
> *3. Any Party may refuse to transfer personal data obtained as a result of the execution of a request made under the Convention or any of its Protocols, where*
> *such data are protected under its national legislation, and*
> *the Party to which the data should be transferred is not bound by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, done at Strasbourg on 28 January 1981, unless the latter Party undertakes to afford such protection to the data as is required by the former Party.*
> *4. Any Party that transfers personal data obtained as a result of the execution of a request made under the Convention or any of its Protocols may require the Party to which the data have been transferred to give information on the use made with such data.*
> *[…]"*

69. Paragraph 1 of Article 26 is similar to Article 23 of the *Convention on Mutual Assistance in Criminal Matters between the member States of the European Union* of 29 May 2000. Paragraph 3 provides, however, for the situation where a Party, which has not ratified Convention 108, requires mutual legal assistance.

70. The *Convention on Cybercrime* [ETS No. 185] which was opened for signature on 23 November 2001 was also prepared in the context of the Council of Europe. This Convention has already been signed by thirty-three States, among them four non-member States of the Council of Europe: Canada, Japan, South Africa and the United States of America. Taking into account the worldwide scope of this Convention an explicit data protection provision has not been included. However, Article 28 reproduces the main contents of the United Nations *Model Treaty on Mutual Assistance in Criminal Matters* mentioned above:

> *"Article 28 – Confidentiality and limitation on use*
> *1. When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply*

where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.
2. The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:
kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or
not used for investigations or proceedings other than those stated in the request.
3. If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.
4. Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material".

71. This article allows States which have ratified Convention 108 to limit the use of transferred material to the individual case for which it was communicated. In this respect paragraphs 275 to 278 of the Explanatory Report are relevant:

"Confidentiality and limitation on use (Article 28)

275. This provision specifically provides for limitations on use of information or material, in order to enable the requested Party, in cases in which such information or material is particularly sensitive, to ensure that its use is limited to that for which assistance is granted, or to ensure that it is not disseminated beyond law enforcement officials of the requesting Party. These restrictions provide safeguards that are available for, inter alia, data protection purposes.

276. As in the case of Article 27, Article 28 only applies where there is no mutual assistance treaty, or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties. Where such treaty or arrangement is in force, its provisions on confidentiality and use limitations shall apply in lieu of the provisions of this Article, unless the Parties thereto agree otherwise. This avoids overlap with existing bilateral and multilateral mutual legal assistance treaties (MLATs) and similar arrangements, thereby enabling practitioners to continue to operate under the normal well-understood regime rather than seeking to apply two competing, possibly contradictory, instruments.

277. Paragraph 2 allows the requested Party, when responding to a request for mutual assistance, to impose two types of conditions. First, it may request that the information or material furnished be kept confidential where the request could not be complied with in the absence of such condition, such as where the identity of a confidential informant is involved. It is not appropriate to require absolute confidentiality in cases in which the requested Party is obligated to provide the requested assistance, as this would, in many cases, thwart the ability of the requesting Party to successfully investigate or prosecute crime, e.g. by using the evidence in a public trial (including compulsory disclosure).

278. Second, the requested Party may make furnishing of the information or material dependent on the condition that it not be used for investigations or proceedings other than those stated in the request. In order for this condition to apply, it must be

expressly invoked by the requested Party, otherwise, there is no such limitation on use by the requesting Party. In cases in which it is invoked, this condition will ensure that the information and material may only be used for the purposes foreseen in the request, thereby ruling out use of the material for other purposes without the consent of the requested Party. Two exceptions to the ability to limit use were recognised by the negotiators and are implicit in the terms of the paragraph. First, under fundamental legal principles of many States, if material furnished is evidence exculpatory to an accused person, it must be disclosed to the defence or a judicial authority. In addition, most material furnished under mutual assistance regimes is intended for use at trial, normally a public proceeding (including compulsory disclosure). Once such disclosure takes place, the material has essentially passed into the public domain. In these situations, it is not possible to ensure confidentiality to the investigation or proceeding for which mutual assistance was sought."

72. The question has arisen whether additional conditions could be put on the basis that a transfer of personal data to a country that has not ratified Convention 108 would be regarded by the requested state as conflicting with its essential interest. Article 27, paragraph 4, has been identified as being relevant in this respect. The provision allows states to refuse mutual assistance if this would prejudice their essential interests. Paragraphs 268 and 269 of the draft Explanatory Report read as follows:

"268. Paragraph 4 provides for the possibility of refusing requests for mutual assistance requests brought under this Article. Assistance may be refused on the grounds provided for in Article 25, paragraph 4 (i.e. grounds provided for in the law of the requested Party), including prejudice to the sovereignty of the State, security, ordre public or other essential interests, and where the offence is considered by the requested Party to be a political offence or an offence connected with a political offence. In order to promote the overriding principle of providing the widest measure of co-operation (see Articles 23, 25), grounds for refusal established by a requested Party should be narrow and exercised with restraint. They may not be so expansive as to create the potential for assistance to be categorically denied, or subjected to onerous conditions, with respect to broad categories of evidence or information.

269. In line with this approach, it was understood that apart from those grounds set out in Article 28, refusal of assistance on data protection grounds may be invoked only in exceptional cases. Such a situation could arise if, upon balancing the important interests involved in the particular case (on the one hand, public interests, including the sound administration of justice and, on the other hand, privacy interests), furnishing the specific data sought by the requesting Party would raise difficulties so fundamental as to be considered by the requested Party to fall within the essential interests ground of refusal. A broad, categorical, or systematic application of data protection principles to refuse cooperation is therefore precluded. Thus, the fact the Parties concerned have different systems of protecting the privacy of data (such as that the requesting Party does not have the equivalent of a specialised data protection authority) or have different means of protecting personal data (such as that the requesting Party uses means other than the process of deletion to protect the privacy or the accuracy of the personal data received by law enforcement authorities), do not as such constitute grounds for refusal. Before invoking "essential interests" as a basis for refusing co-operation, the requested Party should instead attempt to place conditions which would allow the transfer of the data (see Article 27, paragraph 6 and paragraph 271 of this report). "

Consistent application of mutual legal assistance treaties

73. The application of the three legal instruments (Convention on Mutual Assistance in Criminal Matters between the member States of the European Union of 29 May 2000, the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters [ETS No. 182] and the Convention on Cybercrime [ETS No. 185]) should be done in a consistent manner.

74. The problem of this consistent application appears when there are countries which although they have concluded a mutual legal assistance treaty between themselves, are not Parties to Convention 108 and therefore are not supposed to have an adequate level of data protection. In this respect, three situations would be distinguished: a) there is a mutual legal assistance treaty between countries which have ratified Convention 108; b) there is a mutual legal assistance treaty between countries that have ratified Convention 108 and countries that have not ratified the Convention or between countries that have not ratified Convention 108; c) and there is no mutual legal assistance treaty between countries which have not ratified Convention 108.

75. The first case presents no problem because the transfer of personal data in the context of mutual legal assistance treaties will be made between countries which are presumed to have an adequate level of data protection. The third case presents no problem because there is no international legal obligation to transfer either under the mutual legal assistance treaty or under Convention 108 and therefore the notion of adequate level of protection in the sense of the Additional Protocol to Convention 108 will be relevant without limitations. The main problem arises in the second case, because States are obliged to transfer data on the basis of the mutual legal assistance treaties, but the problem arises because if the requesting countries have not ratified Convention 108 they are considered third countries and such transfers can in principle only take place if an "adequate level of protection" is ensured in the third country. The problematic issue is to define the meaning of an "adequate level of protection". The explanatory report of the *Additional Protocol to Convention 108 of the Council of Europe on Supervisory Authorities and Transborder Data Flows [ETS 181]*, 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.

76. 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 "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". In general, however, one comes to the conclusion that the Explanatory Report sees the general assessment as the exception rather than the rule.

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 that "*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*".

77. However, according to Paragraph 2 of Article 2 of the *Additional Protocol to Convention 108 of the Council of Europe on Supervisory Authorities and Transborder Data Flows*, 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.

78. 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*".

79. The basis in domestic law (as required by Article 2 (2) a) could be: 1) Provisions in national law: Here criminal procedural acts could come to mind, but also specific legislation outlining the powers of law enforcement and judicial bodies, as well as implementing legislation of international conventions. The possibilities in national law, particularly the possibility to derogate from the principle of adequate protection for reasons of protection of important public interests, deserve closer scrutiny. The prevention of a serious and imminent danger and the suppression of a serious criminal offence may fall under the legitimate prevailing interests referred to in the Additional Protocol, subject to the appropriate safeguards. It would therefore need to be ensured that domestic law enables law enforcement authorities to transfer data in the pursuit of these tasks if the relevant conditions are fulfilled. 2) Provisions in international law (that are applicable in domestic law): These provisions could be embedded in treaties on military co-operation and assistance (e.g. the NATO treaty), in agreements on international police co-operation, in arrangements on co-operation in the field of intelligence services and, last but certainly not least, in mutual legal assistance treaties.

80. Another option for the situation where the recipient 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*". However, the contractual nature of these clauses means that they cannot be applied, in criminal cases, to transfers of data about a given person that take place between two law enforcement agencies. Agreements such as those prepared in the framework of Europol concerning communication of data to third states and third bodies could be used. Sometimes particular conditions on data processing that aim at a different objective (such as confidentiality of information) might have effects that are comparable to measures taken for reasons

of data protection. In that case an examination of the transfer in question could lead to the conclusion that sufficient safeguards are provided. Another possibility to create sufficient safeguards in the meaning of paragraph 32 is any form of agreement between the provider and the recipient. The Explanatory Report provides for Memoranda of Understanding or specific agreements that could be based on general conditions.

81. Despite the controversial issue of the set of conditions to be met in order to establish that a country has an adequate level of data protection or the determination of cases where a transfer is possible although an adequate level of data protection does not exist, the Working Party underlined that the transfer of personal data to third countries which do not have an adequate level of protection but which are bound by a mutual legal assistance treaty could be allowed with certain limitations. A solution for transfers to countries which do not have an adequate level of protection could be examination of transfers on a case-by-case basis and the use limitation clause contained in the mutual legal assistance treaties could be invoked in the sense that the data shall not be used in other cases than those for which the mutual assistance request was made, except with additional consent by the requested state. Both the Second Additional Protocol to the European Mutual Assistance Convention and the Convention on Cybercrime make this possible. This limitation clause limits the use to the individual case for which mutual legal assistance is requested. The knowledge that the personal data are only used for the purposes that are known to the requested country makes it possible to be less restrictive in transferring data. In other cases, the existence of important public interests would be the basis for allowing the transfer, according to Article 2 of the Additional Protocol to Convention 108. Finally there are some cases where an adequate level of protection does not exist and where there is no important public interest which justifies the transfers; however the existence of a mutual legal assistance treaty which obliges the transfers could be considered as a legitimate prevailing interest.

82. Taking into account the above-mentioned considerations, the following conclusions were reached:

An examination of Article 2 of the Additional Protocol shows that there are various options foreseen that allow for the transfer of personal data to third countries which find a balance between data protection principles and other interests.
When Parties transfer personal data following a mutual legal assistance request to a country that does not provide an adequate level of protection, they should, in particular, invoke a use limitation clause, wherever possible, in the sense that the data are not used for another purpose than that for which they have been requested, unless with the prior consent of the transferring state if it is in accordance with national law. It is not necessary to invoke such a clause if the use limitation stems directly from the relevant Treaty.