COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 21 June 2011 T-PD-BUR(2011) 10 en

BUREAU OF THE CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA [ETS No. 108]

(T-PD-BUR)

Report on the consultation on the modernisation of Convention 108 for the protection of individuals with regard to automatic processing of personal data

Drafted by:

Cécile de Terwangne, professor at the Faculty of Law, research director at CRIDS, University of Namur (FUNDP), Belgium, and

Jean-Philippe Moiny, researcher at CRIDS, FNRS doctorate student, University of Namur

crids
CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

Index

Introduction

1. The public consultation organised by the Council of Europe in order to ascertain the reactions of all parties concerned to the idea of modernising Convention 108 met with great success. The Secretariat of the Council of Europe received numerous contributions, most of which were detailed and backed up by arguments and analyses based on the expertise or practical experience of the contributors. Moreover, some of the latter joined forces and presented a joint response to the questionnaire, while certain federations or groups expressed their opinion on behalf of all their members.

2. Every kind of background was represented in the replies – the public sector (governmental authorities, data protection authorities etc.), the private sector (the worlds of banking, insurance, electronic commerce, marketing, audiovisual distribution, socio-economic research etc.), and the academic world and interested associations.

3. There was also a geographic spread. Replies came from various parts of Europe, and not only from European Union countries but also from states outside it such as Albania and Ukraine. It is interesting to compare the replies from states covered by the European data protection directive (European Union area) with those from north America (United States and Canada), Africa (Senegal, Mauritius) and Australia. The International Organisation of La Francophonie also sent comments.

General considerations

4. The replies received sometimes suggest a direction to be followed but do not indicate the means of giving practical effect to that approach. Sometimes, by contrast, commentators present arguments and pointers to one or other direction.

5. In a number of cases, contributors state that in view of the difficulty of the matter, an in-depth study ought to be carried out. This was said, for example, about the exclusion from the scope of the Convention of data processing for personal and household purposes or on the question of the law applicable. In other cases, contributors call for an impact analysis or a study of the effectiveness of the legislative measures envisaged (in particular concerning the introduction of the possibility of class actions and systems of alternative dispute resolution, or concerning the introduction of a duty to report data breaches).

6. A great many contributors argue that the work of modernising the Convention should be carried out from a concern to achieve the greatest possible consistency with the protection rules laid down by the European Union (mainly Directive 95/46). Thus in many cases replies were guided by this concern to align the text of the Convention with that of the European directive. The work of modernising that directive, currently in progress, should be monitored so as to ensure that discrepancies between the texts do not arise. It is interesting to note that this concern is voiced not only by persons from the European Union: it is shared by people outside the EU.

Object and scope of the Convention, definitions

1. Convention 108 has been drafted in a "technologically neutral" approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared ?

7. All those who replied were in favour of keeping the text simple and setting out general principles.

8. In their opinion, this is the only approach which guarantees the long-term viability of the Convention. The past thirty years, with a convention laying down general principles, have shown that this model has stood the test of time.

9. In the same long-term perspective, everyone likewise emphasises the need to ensure the technologically neutral nature of the Convention. The principles formulated must not focus on the existence of a technology, for that would incur the twofold risk that the principles might become obsolete once the technology is outdated or abandoned, and that the principles would not be adaptable to the new technologies that will inevitablyemerge.

10. That being said, the replies state that, while the text of the Convention should not be made too detailed, it is nonetheless necessary to make some additions to the existing text.

11. Several contributors draw attention to the fact that, if the Convention is to have universal validity in the future, it must be realised that too detailed a text will undoubtedly scare away states which might be considering accession to the Convention.

12. Consequently, some commentators take the view that the existing approach should be pursued – keeping the text of the Convention general and simple, and setting out the general principles in detail in specific texts (Committee of Ministers recommendations).

2. Should Convention 108 give a definition of the right to data protection and privacy?

13. Some of those who replied to this question believe that including definitions of the right to data protection and the right to respect for privacy would help to clarify the scope of the text and help the public to understand its subject-matter. In the view of APEP (the Spanish Professional Association for Privacy), this would make it clear that private life and data protection are two different rights, and that personal data may or may not be private.

14. Others consider that, as the concept of privacy appears in several international legal instruments, it would not be opportune to define it in Convention 108. In particular, it is the responsibility of the European Court of Human Rights to define the scope of this concept as set down in Article 8 of the European Convention on Human Rights. The CNIL, for example, considers that these concepts should not be defined but left open to interpretation in an evolutive way. The State Data Protection Inspectorate of Lithuania points out that the international legal instruments which protect private life do not give any definition of it. The same approach could be adopted with regard to data protection.

15. Let us note in passing that a non-uniform perception of what privacy means is discernible in the replies. Some of them refer to the conventional meaning (intimacy, confidentiality), not the more developed one of autonomy and information control as updated by the European Court of Human Rights. The European Banking Association, which believes that Convention 108 should contain the definitions in question, also states that this is particularly important in so far as the Convention is to serve as a basis for countries outside the European Economic

Area, which do not have specific definitions in their own legislation or any knowledge of the concepts of "privacy" and "data protection" in case-law and doctrine in relation to existing European definitions.

16. On the other hand, with regard to the concept of the right to data protection, these and other contributors appreciate the value of a definition while calling for its harmonisation with the one given in the Charter of Fundamental Rights of the European Union. Privacy International emphasises in this connection that it is worthwhile trying to define the right to data protection, in view of the fact that many of the world's constitutions have begun to recognise that data protection is indeed a right.

17. Some replies argue that defining concepts after 30 years' application of the text is not justified. That length of time brings an opposite response from Portugal's Direcçao Geral da Politica de Justiça, which considers that, as the oldest instrument of public international law on the matter, Convention 108, which claims to regulate data protection law, must not demonstrate an inability to define that right itself.

18. The European Newspaper Publishers Association does not state its opinion on the desirability of including such definitions, but says that, if the decision is taken in favour of definition, care should be taken not to make the inference that these rights would prevail over those of freedom of expression and information. Introducing legal uncertainty must also be avoided.

3. Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement agencies. Should this comprehensive approach be retained?

19. There is unanimous agreement that an approach which covers both the private sector and the whole of the public sector, including police and justice system, must be maintained. Given the practical ease and potential of existing technical tools (not to mention those that will emerge in future), it is considered "absolutely vital", to quote many contributors, that law enforcement personnel be required to respect data protection principles.

20. Of course, everyone agrees on the need to adapt these principles to allow for needs arising from the work of these players. The important thing is not to leave the police and justice system outside the protection sphere. The solution generally envisaged is a series of partial exceptions for these players.

21. TechAmerica Europe proposes that thought be given to situations in which partly different rules would apply to public authorities and private entities, while keeping the same basic principles and requirements as to transparency. They ask for consideration to be given to the impact which changes to the Convention might have on the work of law enforcement in order to check that these new measures or new concepts do not give rise to particular difficulties in this sector.

22. Another American contributor asks for special care to ensure that any change made to the Convention continues to allow of a degree of flexibility in exchanges of "police" data between the United States and Europe and permits data sharing for purposes of public safety and prosecution of offences.

23. The Canadian contributors emphasise that their experience of two separate sets of rules for the public and private sectors, as at federal level in Canada, has given rise to criticisms from civil society and from the Federal Privacy Commissioner.

4. Convention 108 does not exclude from its scope data processed by a natural person in the course of a purely personal or household activity. Should this continue to be the case or should a specific exception be introduced (and specifically considered in the context of Web 2.0.)?

24. Generally speaking, those who replied are in favour of introducing an exception to the scope of the Convention for data processed for personal or household purposes.

25. Many of them stress that this must be done in a concern to align the Convention's protection model with that of Directive 95/46.

26. However, several contributors think it will be extremely difficult to decide exactly what such an exception would cover.

27. The AEDH, which is in favour of this exception, proposes making it conditional on data not being communicated to third parties and that the exception goes hand in hand with an obligation on services supporting such personal activities (electronic mail, address book, diary, archive service etc.) to inform their clients about their obligations and offer them confidentiality functions.

28. The CNIL suggests following the European Union model and stating that it lies within the power of interpretation of the national supervisory authorities to define what comes under the exception and what does not.

29. The CIPPIC (Canada) observes that this question was mentioned as being a future challenge in the data protection field. At all events, there must be careful balancing with the right to freedom of expression when it comes to settling this question of individuals' private activities. It was precisely when giving consideration to freedom of expression as against data protection that the Centre for Socio-Legal Studies developed its standpoint on this exception hypothesis. Realising that many of the situations in which personal data are processed in the most intrusive and unwarranted way are the result of private individuals motivated by non-commercial reasons, the Centre does not wish these activities to be excluded from the scope of all protection rules. In its opinion, a better solution would be, first to ensure that such individual activities can benefit fully from a new and broader clause on freedom of expression, and then to impose on individuals just some of the obligations of file controllers, determined in a clear, proportionate manner.

30. The European Privacy Association, whose views on this point are shared by the APEP (the Spanish Professional Association for Privacy) and by the State Data Protection Inspectorate of Lithuania, points out that the activities of individuals nowadays may easily harm others and therefore their activities cannot be wholly excluded from data protection rules. On the other hand, however, purely personal activities cannot be made subject to disproportionate obligations and burdens, especially in relation to security (Article 7) and transborder flows (Article 12). The APEP stresses that regulations must be able to sanction the misuse of personal data by individuals. This association would consider it disproportionate to place obligations on individuals such as having to declare data processing, to provide information in accordance with Articles 10 and 11 of Directive 95/46, to take security measures or to ensure that such measures are being taken by the platform they are using.

31. Senegal's Data Protection Commission suggests that, over and beyond the proposed exception, which it supports, it be broadened by the addition of "processing of data not intended for systematic communication to third parties or for distribution".

5. The definition of automatic processing does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list?

32. All who replied favour including the concept of collection in that of automatic processing. This stance is motivated primarily by the desire to ensure consistency with European, national and international standards. There is also the belief that it is useful for collection to be made subject to all the principles governing data processing, not just to one particular provision.

33. The concern for consistency among legal systems also explains why many contributors, such as CEA Insurers of Europe or the AFME BBA (banking & financial services), call for the adoption of the concept of "processing" as presented in the European directive. The CEA considers that it would be helpful for the "disclosure by transmission" operation, which is a fundamental operation in data processing, to be expressly included in the list of operations covered. The CNIL believes that the concept of processing should be as broad as possible, so great is the tendency for operations carried out on data to grow in number and diversity.

34. The AFME BBA, like the European Banking Federation, points out that the terminology must not be confined to such concepts as "file" which have a dated technological connotation that could compromise both the neutrality of the text and the broad application of the Convention, as this notion is no longer relevant in the present-day Internet and cloud computing situation.

35. Lastly, the Portuguese Direcçao Geral da Politica de Justiça asks us to reflect on the broadening of the scope of the Convention to include non-automatic processing. That body is aware that such processing is a minority today, but considers that it has not entirely disappeared and that prudence requires its inclusion in the sphere of protection.

The definition of the controller of the file should be reviewed: should several criteria be listed, should such criteria be cumulative, can there be several controllers for one file ?

36. Some contributors think that the current version of the Convention should not be amended on this point. The present definitions are sufficient to render the persons involved in data protection responsible.

37. Others believe that the definition of "responsable du traitement/data controller" used in Directive 95/46 should be substituted for that of "controller of the file".

38. The Data Protection Commissioner of Mauritius proposes replacing the definition by the following one: "The controller of the file is any natural or legal person, whether public or private, who decides on any activity, whether automated or not, carried out on personal data". The APEP - Spanish Professional Association for Privacy proposes that the definition be amended to include "any person or persons who has/have the de facto right to decide on the purpose and means of processing personal data, either by virtue of the law or in accordance with a contractual agreement with the person concerned or a third party". That body considers it important, for reasons of legal certainty, that only persons having legal personality should be responsible for processing.

39. Several replies observe that it would be desirable to allow for cases in which there are several persons responsible for processing the same data. The AEDH quotes the example

of a decision to use a file taken by a number of responsible persons for joint purposes, such as compiling a file common to a trade or profession in relation to defaulting customers. The APEP draws a distinction between joint controllers (processing the same data for the same purpose) and several controllers (processing the same data but for different purposes).

40. The European Privacy Association draws attention to the fact that advanced technologies (such as cloud) are increasingly resulting in the automated processing of data by multiple agencies. This association believes it is important, not to state the names and functions of those agencies but to define the processing activities, the requirements and obligations linked to those activities and the related responsibilities. This view is shared by the Information Commissioner for the United Kingdom (ICUK), who says that, rather than listing the criteria for what constitutes a "controller", he would prefer there to be a better description of the activities which a file controller may carry out.

41. EFAMRO ESOMAR (research sector) thinks it necessary to introduce a clearer definition of "data controller", laying responsibility on the shoulders of the persons who decide how data are to be processed, as distinct from those who control a particular computer system or file. This would make just one data of the file responsible for assessing the need to process data and the security of the available systems before opting to process data using such systems. It would also provide citizens with a single focus of responsibility and accountability.

42. The German Insurance Association would welcome a review of the concept of file controller, because it would present an opportunity to make changes in data processing in the world of business. Centralisation of service tasks within groups and recourse to outsourcing of tasks to competent services are the principal areas concerned. Being able to present the entity transferring data and the one receiving them jointly as a single entity responsible for processing would facilitate data transfer and simplify group life.

43. That standpoint echoes a remark made by the Computer Law and Security Review consortium, the International Association of IT Lawyers and the Institute for Law and the Web (University of Southampton): they point out that in a network environment, the concept of controller of the file is no longer as relevant as before, because of the increasing use of systems of data sharing and interconnection. In such environments, it would be preferable to appoint a single entity to take overall responsibility (as in the European Union systems of binding corporate rules). An obligation should be placed on those responsible for individual processing to inform the persons concerned of any data sharing and interconnection involving them and provide particulars of the coordinating entity.

44. Lastly, Mydex Community Interest Company states – and says that its view is shared by many others, including the World Economic Forum – that in future, the technical architectures of future generations will place individuals at the centre of their own personal data ecosystems, so that they will themselves take responsibility for processing. The legislation will have to reflect this new modus operandi and permit this "data empowerment by design".

6. New definitions may be necessary, such as for the sub-contractor or the manufacturer of technical equipment.

45. Contributors welcome the intention to introduce new definitions if it is done in a concern for consistency with those developed in the European Union. That would make it possible to improve legal certainty, enhance the protection of the persons concerned and avoid creating confusion in the minds of controllers of the file.

46. Several replies wisely observe that there is no point in including definitions of additional players if a particular legal regime setting out obligations is attached to these new players.

47. Several replies state that it is essential to add a definition of sub-contractor. The Italian Garante per la protezione dei dati personali further observes that the need to introduce such a definition has already been felt in several Council of Europe instruments (Recommendation 2002(9) on data protection in the insurance sector and Recommendation 2010(13) on profiling).

48. By contrast, Privacy International considers that the concept of sub-contractor is no longer useful, since sub-contractors in fact have to comply with so many obligations in respect of security and respect for privacy that their role becomes very hard to identify. There is a problem in asking controllers to take responsibility for privacy and security measures when they are in reality entirely dependent on the contractual conditions laid down by service providers (especially cloud) who are not subject to the regulations.

49. The German Insurance Association calls for a flexible definition here, permitting the parent company, depending on circumstances, to be appointed as sub-contractor by a company in the group, though in such cases there should be limits on recognising the right to issue instructions in accordance with existing law.

50. The AEDH proposes that a distinction be made in the case of service providers processing data on behalf of the data controller of the file but enjoying clear autonomy in the provision of the service, so that they would wear the two hats – that of data controller of the file and that of sub-contractor. In this hypothesis one could introduce the concept of "person entrusted" with processing ("personne chargée"): where the sub-contractor acts strictly on behalf of and on the instructions of the data controller of the file and is not responsible as controller of the file, the person entrusted with processing could be regarded as bearing part of the responsibility, either jointly or in full.

51. In the opinion of the ICUK, the mere distinction between controller of the file and sub-contractor no longer reflects the complex relationship which exists between organisations processing personal data. The model definitions in Directive 95/46 correspond to a passive sub-contractor acting only on the instructions of the controller, whereas in reality the person regarded as sub-contractor may have considerable influence on the manner in which processing takes place and may, in many respects, act as a controller of the file. The CNIL considers that this situation, in which actual day-to-day processing of data is in effect, increasingly, in the hands of the sub-contractor, not of the data controller of the file, ultimately requires that this category of player be defined. That body believes that consistency with the definition in the directive stating that it is the organisation acting on behalf of the data controller of the file is necessary. It also argues that the rules governing the sub-contractor's responsibility should be more fully harmonised and regulated at European level.

52. Regarding the addition of a definition of “manufacturer of technical equipment”, some contributors such as the European Banking Association see this as a good idea, while the AEDH regards it as quite essential, whether the equipment in question is hardware or software. The Cyberspace Law and Policy Centre (Australia), in common with the Cyprus Commissioner for Personal Data Protection and the CLSR-IAITL-ILAWS consortium, observe that this will prove to be necessary if rules on “Privacy by Design” are introduced – which, unlike the others, the Cypriot authority would not welcome.

53. The Italian Garante has a less clear-cut approach: it believes that it would undoubtedly be useful to set out the guarantees which should be offered by any additional entity which plays any part in processing (such as a manufacturer of technical equipment), while placing the legal obligation to check that these guarantees are respected on the data controller of the file.

54. Privacy International, on the other hand, thinks it would not be wise to define equipment manufacturers beyond a specific risk to privacy and a security context. The Direcçao Geral da Politica de Justiça in Portugal is also opposed to the inclusion of this concept, which it does not find helpful.

Protection principles

7. New principles could be added to the Convention, such as the proportionality principle, which should apply to all operations carried out on data. Such a principle is also linked to the data minimisation principle which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection whenever possible.

55. Many contributors point out that the proportionality principle is already contained in Article 5 of the Convention. They accordingly restrict the application of this principle to data which must be relevant and not excessive.

56. Other contributors think that the inclusion of the principles of proportionality and minimisation or limitation of data collection in the protection principles should be recommended, and some argue that these principles should be explicitly stated, not merely implied. The explicit formulation of these principles would make it possible to define their scope better and more precisely. In particular, it would make it possible to stipulate that the proportionality principle applies to all operations, not just to data collection (Cyprus Commissioner). In other words, the proportionality principle linked to the purpose of each processing operation (Garante) or the criterion in respect of the non-excessive character of an entire private data processing project relative to the fundamental freedoms and rights in question must be respected, in addition to the need to minimise the data processed (AEDH). Similarly, the AEDH says that the principle of data minimisation must not replace that of proportionality because the latter must go beyond data alone.

57. Some contributors are strongly in favour of including these principles, which they see as very important (CLPC, Australia; APEP - Spanish Professional Association for Privacy; Czech Office for Personal Data Protection; CLSR-IAITL-ILAWS; Italian Garante).

58. Morpho-Groupe Safran (identification technologies), which regards the proportionality principle as one “which seeks to strike a balance between the processing of data and the aim pursued”, is mistrustful of the subjective approach implied by the application of this principle. That subjectivity results in divergences between national data protection authorities in the acceptance or otherwise of an industrial product or device. Consequently, they would like this principle, if it is set forth in the Convention, to be accompanied by

objective provisions such as to encourage recourse to labelling/certification procedures based on precise criteria which the manufacturer would have to respect in order to develop his products.

59. The GDD (German data protection and data security association) considers that certain advantages should be granted to organisations using pseudonyms rather than data directly linked to persons.

60. ARD and ZDF (radio and television) consider that, whereas users of traditional media have always enjoyed complete anonymity, that is no longer true of services provided via the Internet. Consequently, they strongly support the principle of strictly limiting data collection to the aim pursued.

61. CEA Insurers of Europe asks for data minimisation to be presented as an objective, not as an obligation.

8. Should the question of consent be considered in close connection with the principle of transparency and obligation to inform, or as a necessary condition for fair and lawful processing, to be met before any other step?

62. Several contributors believe that the role of consent as the legal basis for data processing should be qualified. In any case, it ought not to be the sole basis. Some believe it should not be presented at all as a condition to be met for processing to be legal and fair. In many cases the persons who give consent do not realise what they are agreeing to. Consent is neither a guarantee of protection for the persons concerned nor a practicable solution for data controllers of the file, for whom it may constitute a disproportionate burden (for example in the worlds of marketing or insurance).

63. Quality of consent causes huge apprehension. There are references to problems of genuinely free consent, and problems arising from the form of consent increasingly employed.

64. On this point, the GDD (German data protection and data security association) considers that the relevant German law offers consumers good protection. It stipulates that if consent is given in a form other than writing, the data controller of the file must give written confirmation of the substance of that consent to the person concerned, unless consent was given in electronic form, in which case the controller must keep a record of the consent to which the person concerned must have access and which he/she can revoke at any time with future effect.

65. The CLPC (Australia) proposes the example of the Canadian law governing protection of privacy in the private sector (PPIDEPA). There is a particularly interesting proposed amendment to that legislation: “An individual’s consent is valid only if it may reasonably be expected that the individual understands the nature, purpose and consequences of the collection, utilisation or disclosure of the personal information to which he/she consents”. The CLPC says that, if the concept of consent is introduced, consent must be expressly defined as free, informed and revocable and not linked to other consents. There should also be a general principle stating that, where true consent is a realistic option, it should constitute the main basis of legitimate processing, which would be consistent with the overall aim of transparency in the processing of personal data.

66. The US Federal Trade Commission points out that denying the persons concerned the choice of practices which are straightforward for consumers makes it possible to restore meaning to choices about more problematic practices (such as transferring their data to third parties who have no connection with the purpose of the data processing).

67. Many contributors stress that consent must be linked to transparency. In the opinion of Privacy International, transparency must even prevail over consent, in the sense that prime importance must attach to clear, easily found and easily understood information provided for the persons concerned before judging whether processing is authorised (and then based on opt-out rather than opt-in). Furthermore, other contributors stress that one should be wary of long and rarely read privacy policies. For the APEP - Spanish Professional Association for Privacy believes that a general duty of information should be established in order to ensure transparency.

68. The European Newspaper Publishers Association and the FAEP (European Federation of Magazine Publishers) point out that an exception for the media would be needed for any question of consent, whether in terms of an obligation of transparency and information or as a necessary condition for fair, lawful processing. This must apply to all their activities - archiving of articles, recording of research material for preparation of articles, everyday collection of news, investigation, verification, publishing, deletion, whether or not this leads to publication of the material, and lastly subsequent publication and communication.

9. Should the legitimacy of processing be addressed by Convention 108 as Directive 95/46 does in its Article 7?

69. Some contributors fear that the introduction of such a list would reduce the flexibility of the Convention (TechAmerica). The Garante, like the Cyprus Commissioner for Personal Data Protection and CEA Insurers of Europe, emphasises that one should avoid modelling the Convention's principles too closely on those set out in Directive 95/46, since that would mean introducing excessively detailed provisions into the Convention. This concern is shared by the German Insurance Association, which argues in favour of a high degree of abstraction in the Convention, especially bearing in mind third countries' wish to accede. Similarly, the FEDMA states that this ought not to appear in the substance of an international convention. It would be more appropriate to a directive.

70. Privacy International is more radical still, considering that such an approach to legitimacy is redundant and pointless. Dishonest aims are obviously not legitimate, unless they are (sic) (hypothesis of aiming to deceive a fraudster, for example). As they see it, the list of reasons for legitimising processing set out in the directive has created a playground for lawyers, strewn with pitfalls. Finally, they fear that a list of positive bases for carrying out data processing will inevitably be incomplete. They see the combination of the requirement of fairness and lawfulness (= not "unlawful"), coupled with the other general principles of proportionality, data minimisation and non-intrusive collection as appropriate criteria. These last points are restated word for word by the Cyberspace Law and Policy Centre and the CLSR-IAITL-ILAWS consortium.

71. At the other end of the spectrum, some contributors find it opportune, useful, and indeed important, to include such a list of legitimate bases, out of a concern for consistency with European Union law or a concern for clarity for those in the field who need to have clear parameters on lawful processing (AEDH, European Privacy Association, European Banking Federation, Data Industry Platform, the Czech Office for Personal Data Protection, the Bulgarian Personal Data Protection Commission, the Portuguese Direcçao Geral da Politica

de Justiça, the Ministry of Justice of the United Kingdom). EFAMRO and ESOMAR are in favour of the introduction of a basis for legitimate data processing into the Convention, but not of an exhaustive list of legitimate bases.

10. Convention 108 does not expressly mention the need for compatibility between the use made of data and the initial purpose of collection. In today's context, personal data are commonly used for purposes that go far beyond what may have been initially foreseen, hence the issue of compatibility.

72. Few contributors understood the pertinence of this question, since Article 5 of the Convention already requires that data should not be used in a manner that is incompatible with the purposes. For many people, therefore, the question has already been settled.

73. However, some of them observe that the question of later processing arises more and more often, mainly owing to the mass availability of data on the Net, and should be dealt with.

74. The European Privacy Association believes that the main issue is not to mention the requirement of compatibility with purpose but rather to extend the scope of Article 5 (b) of the Convention to all data processing. They suggest taking the text of Article 6.1 b) of the directive as a model.

75. It is pointed out that later processing for historical, statistical or scientific purposes should be permitted. EFAMRO and ESOMAR call for "market, social and opinion research" not to be regarded as incompatible with the initial purpose of data processing, and this is already allowed by Recommendation R(97)18. These bodies call for the inclusion in the Convention of a provision similar to Article 6 paragraph 1 b) of Directive 95/46.

76. CEA Insurers of Europe ask that it be possible to change the purpose in cases where the new purpose can be legally justified.

77. Matthias Pocs, considering this question from the standpoint of the police where it arises in an acute form, proposes (and supports his proposal with factual arguments) that Convention 108 should provide for the processing of personal data for purposes other than the specified ones to be prohibited if the person concerned is suspected of a lesser or moderately serious offence, but permitted if the person concerned is suspected of a serious criminal offence and adequate guarantees against infringements of human dignity are given.

11. Special categories of data which enjoy enhanced protection are defined very widely, which could lead to excessive application of this restrictive regime : are the data sensitive or their processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?

78. **Relevance of a category of sensitive data:** the UK Ministry of Justice requests the Consultative Committee to reflect on the possibility of sensitive data being linked to their use rather than simply extending the list of sensitive data (he refers to the example of a photograph which might be regarded as biometric data, and where there is a huge difference between its being attached to a library ticket and being taken at the door of a treatment centre for drug addicts). This viewpoint is shared by several contributors for whom data sensitivity is essentially a matter of context.

79. In the view of several contributors, the proportionality principle offers adequate safeguards for these data. One could leave the present list as it stands and rely on the proportionality principle to counter the dangers arising from other data.

80. The Italian Garante considers that the greater protection afforded to data in the present list, which broadly corresponds to the categories protected by international instruments to combat discrimination, should be left untouched. On the other hand, one might envisage a "functional" criterion whereby additional categories of data could be classed as sensitive because of the context and/or purpose and/or processing mechanisms. In these cases, such data would be subject to enhanced protection. One could also envisage circumstances and data categories being determined and regularly updated by flexible tools not involving amendments to the Convention. This viewpoint accords with that of the Data Protection Commissioner for Mauritius, who considers that a distinction could be drawn between data that are sensitive by reason of their nature and data that are sensitive by reason of the processing applied to them (such as a name or photograph revealing racial origin). The APEP also emphasises that any prejudice which might result from the processing of these sensitive data depends on the purpose of processing.

81. **The list of sensitive data:** several contributors wonder what is covered by the concept of "biological" data. Some consider that it should not cover such characteristics as gender or age, which are apparent to everybody.

82. Some replies suggest that genetic and biometric data be added to the list.

83. Morpho-Groupe Safran, a company specialising in identification and applications using biometry, points out that, unlike names, fingerprints give no clue as to ethnic origin or supposed religious allegiance. Moreover, a name is the key giving access to masses of information on the Internet via search engines, as distinct from fingerprints. So the company wonders why biometric data should be subject to more binding legal rules when they provide less information than people's names. Moreover, Safran wonders what should be done about "voice prints" obtained from electronic messaging and stored on servers to build biometric databases. Should these data enjoy different legal rules from fingerprints, and on what basis? Safran gives information about genetic fingerprints as distinct from genetic data and points out that in some situations the use of biometric data such as iris recognition or digital fingerprints, if rendered anonymous, makes it possible to decide whether an individual may or may not be granted a right (to enter, for example) without his/her identity being disclosed.

84. The APEP - Spanish Professional Association for Privacy shares this reluctance to have biometric data regarded as sensitive, since in principle these data do not relate to information about health. This association also finds it difficult to class (national) identification numbers as sensitive.

85. In the view of the AEDH, apart from biological information needed in a medical context, the question arises whether, in the name of protection of the human person, information such as national identity numbers and biological or biometric data which serve as reliable identifiers for a person should actually exist at all, especially when they relate to every member of a community, not just to certain persons for particular reasons of public necessity. This organisation regards the existence of such information systems as highly dangerous in all exceptional circumstances (regimes becoming undemocratic). Furthermore, these systems which physically link persons to the state breach the social contract and stem from the idea that every citizen is a potential delinquent, which is unacceptable. So data of this kind must not be made subject to a system of enhanced

protection in order to prevent discrimination. What is needed is a system of prohibition which can be lifted in accordance with the criteria set out in Article 9 of the Convention.

86. The CNIL proposes referring to ethnic origin rather than racial origin.

87. Several contributors request that, if consideration is given to extending the list of sensitive data, this be preceded by an impact study.

88. Regarding the **rules governing these data**, the CNIL requests that they be more detailed, because the contents of the Convention as it now stands lack precision. It also says that an exception should be made for statistical processing and scientific research.

89. EFAMRO and ESOMAR would welcome clarification on what the term "sensitive data" covers. They also point out that insisting on recourse to an authority before sensitive data are allowed to be processed places too heavy a burden and too great a barrier on the research sector.

90. The European Newspaper Publishers Association and the FAEP call for an exemption for the press sector from the strict rules on sensitive data.

12. Specific protection could also be applied to certain categories of data subjects. In particular, children may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, what are the issues that should be addressed in such provisions?

91. Data concerning minors should not fall into the sensitive data category, since the person concerned by the data cannot constitute a sensitivity criterion (Bulgarian Personal Data Protection Commission).

92. That being said, it is important to provide for special conditions for the protection of minors because of their vulnerability. Several contributors consider this necessary. The APEP - Spanish Professional Association for Privacy observes that there is unanimous agreement that children deserve specific protection, but the discussion is about the relevant age to be taken into account, whether and from what point parental control infringes the child's right to privacy, who is to grant parental authority, etc. Specific obligations should be imposed in cases where children are the target of the processing. The specific protection regime should be based on obligations as to means, not results.

93. The Federal Trade Commission outlines the specific American on-line system of child protection (the Children's Online Privacy Protection Act), which lays down a series of rules designed to protect children below the age of 13. These rules are currently being reviewed to ensure that they continue to offer an adequate response to changing technologies, and especially to practices involving a boom in the use of mobile terminals and interactive games by children.

94. By contrast, many contributors do not believe that a particular protection regime has its place in the Convention. Specific rules are set down in other instruments. A recommendation would probably be more appropriate here. Alternatively, the explanatory report could make it clear that the introduction of the principles of proportionality and minimisation is an adequate response to the concerns about children - and other vulnerable groups (CLPC, Australia).

95. This is all the more so because there are difficulties in harmonising the meaning of “minor”, “minor with capacity of discernment” and “minor with capacity to express consent”. Just as there are difficulties in verifying and ensuring compliance with age limits on the Internet.

96. Lastly, several contributors point out that there are other categories of vulnerable persons apart from minors.

13. Article 7 of the Convention addresses security in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of data security breaches?

97. Several contributors think it desirable to provide for such a right to be informed about security breaches, applicable across the board to all sectors. The CLPC, together with the CLSR-IAITL-ILAWS consortium and Privacy International, believe that this right should not appear as part of the principle of security but as a separate principle.

98. Most replies state that is is imperative for the limits of such a right to be clearly indicated. The European Privacy Association says that the text should stipulate when the information is to be given, to whom and in what manner. TechAmerica Europe proposes markers to define this obligation. The Data Protection Commission of Senegal considers that there should be an obligation to inform the public supervisory authorities but not the persons concerned, who are in any case powerless in the face of infringements. The German Insurance Association offers the benefit of German experience: in 2009, an amendment to German data protection legislation introduced a duty to inform in cases of unauthorised access to data. That obligation applies where particularly sensitive data are concerned and where there is a real risk of serious infringement of the legitimate rights or interests of the persons concerned. To their knowledge, this rule has proved positive in practice. They stress the need to limit this kind of obligation strictly to cases of real risk to the persons concerned. Morpho-Groupe Safran does not deal with hypothetical case of unauthorised access but considers that this right to be informed of security breaches should be expressly justified by the need to protect identity and limit the risks of usurpation of identity.

99. However, several contributors fear that it would not be possible to introduce such a right without transforming the Convention into an unduly detailed instrument going beyond general principles.

100. Some contributors, such as the Czech Office for Personal Data Protection, are opposed to the idea of introducing this right, believing that the question is sufficiently dealt with in the European directive. The Data Industry Platform fears that additional burdens may be placed on agencies in the field without giving the persons concerned a higher level of protection. This group of signatories appreciates the importance of security and the need to create confidence among the persons concerned and data controllers. Thus they are sympathetic to the concept to the extent that it is an incentive to security. However, they consider that the question would be more suitably addressed by instruments of self-regulation. FEDMA and the European Banking Federation express exactly the same fears and convictions. EMOTA (European E-commerce and Mail Order Trade Association) also shares these misgivings.

101. Several contributors state that in any event one should not fall for an “overly prescriptive” wording, which would impose an excessive burden and at the same time rob the measure of its effect, making notification of those concerned routine.

102. Garante sees the question of security as crucial, especially in the context of cloud computing. Article 7 of the Convention should be revised. It would be appropriate to consider extending the concept of security to include the security of data transmission networks, over and above the physical security of the premises where data are kept.

103. Similarly, Privacy International recommends that the passive interpretation of "data security" be replaced by a positive obligation to design systems in such a way as to minimise the risk to privacy - for example ex ante minimisation. So one must not only seek to protect the data processed, but to minimise the risk to privacy throughout the system.

14. There are special risks arising from the use of traffic and location data (technical data accompanying a communication) since such data can reveal movements, orientations, preferences and associations with others. Do we need special rules for the use of such data ?

104. There are contrasting replies to this question.

105. Some contributors think it would be desirable to provide for a stronger protection regime for processing aimed at locating individuals spatially.

106. The AEDH observes that traffic data affect freedom of communication, and location data freedom to come and go. Because of this interference with freedoms, a more stringent regime should be applied to them. The same is true of requests made on a search engine, which affect freedom of information. Similarly, Privacy International sees traffic and location data as data concerning social relations and impinging on freedom of association and the right to associate freely, in a private, unobserved way. Consequently, Privacy International takes the view that such data should constitute a special category and be considered as inherently "toxic" to privacy.

107. The CNIL points out that placing these data in the sensitive category could well place a check on certain technical innovations. It would be better to add clearly distinctive protection elements to the Convention, designed in particular to require appropriate guarantees for "personal data used in processing for the purpose of revealing an individual's spatial position". That would make it possible to exclude data which may reveal an individual's position but whose purpose is not to do so, while not placing these data in the special categories provided for in Article 6 of the Convention. A third possible option suggested by the CNIL would be to propose a specific right not to be geo-located.

108. Other contributors see no need to provide for specific rules. The British Information Commissioner likewise believes that sensitivity relates more to data processing and t he effects it may have on individuals rather than to the nature of the data processed.

109. The CLPC, echoed by the CIPPIC, argues that there should be no need for a particular regime if care is taken to ensure that traffic and location data are brought within the definition of personal data, stating explicitly that "personal data" covers any information which permits or facilitates communication with a person on an individualised basis, whether or not that information conforms to the present definition of personal data.

15. Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full compliance with data protection rules be introduced?

110. Most of those who replied to this question favour the idea of introducing an obligation to comply with the accountability principle as a guarantee of improving the protection afforded. Accountability mechanisms should be clearly defined; they should not be excessive and should be implemented by all signatories in the same way.

111. Privacy International, in common with the CLSR-IAITL-ILAWS consortium, advises caution with regard to the suggestion made by some contributors that accountability should be seen as an alternative to the requirement of respect for the protection rules. Accountability must not become an alternative to restrictions on the export of data. This organisation is concerned about the consequences, or rather the absence of consequences, which accountability failures may have if this principle is interpreted loosely.

112. The APEP - Spanish Professional Association for Privacy considers that a "reward" (for example a lesser penalty) should go to file controllers who are "accountable" in cases where data protection infringements are due solely to an exceptional error.

113. TechAmerica Europe supports the introduction of an accountability principle if it is defined in an ex post approach based on the application of the rules rather than an ex ante approach based on conformity with the rules. In an ex-post system, organisations are responsible for what they do with data wherever the latter go, instead of simply trying to comply with the law. This has implications for the way in which the organisation sees data protection, the way in which it implements it and the way in which it oversees it.

114. Some contributors are opposed to the introduction of an obligation to demonstrate compliance because it would constitute a burden, especially for small and medium-sized enterprises.

16. Should the principle of "privacy by design", which aims at addressing data protection concerns at the stage of conception of a product, service or information system, be introduced?

115. In view of the fact that the principle of privacy by design has been proclaimed by several bodies, was the subject of a resolution adopted by the 32nd international conference of data protection authorities and is being taken into account by the European Commission in the framework of its revision of Directive 95/46, it seems logical that this principle should also be enshrined in Convention 108 (Safran).

116. Other contributors share the belief that this principle should be expressly encouraged, even if it will be difficult to give it operational effect by way of a specific rule (Privacy International, British Ministry of Justice, CNIL, Senegal's Data Protection Commission). Or else they say it is welcome, but the way in which it is to be defined and implemented must be clarified before it can really be advocated (TechAmerica Europe). Introduction of the privacy by design principle would foster a proactive approach to protection rather than reliance solely on corrective measures

(Garante). As the AEDH sees it, the obligation to apply protection principles from the stage of design of equipment and applications could be simply stated in the text without necessarily employing a “marketing vocabulary” such as that of privacy by design. The ICUK observes that this principle is already implied by the existing protection principles. However, an explicit requirement would have the advantage of sending a clear signal to data systems designers, those who supply them and those who operate them.

117. The Italian Garante points out, however, that the effectiveness of the principle cannot be guaranteed except by specifying how its impact on particular processing operations can or should be measured and by whom, in the light of specific technological provisions.

118. The Bulgarian Personal Data Protection Commission considers that, for this principle to be applied effectively, data controllers should be required to carry out assessments of the risk to privacy in data processing. Privacy International also favours an obligation to carry out a privacy impact assessment for major projects.

119. The last-mentioned organisation says that the simplest way of expressing the principle of privacy by design is to state that, if scientific discoveries show that a service can be offered in practice by a method which is more respectful of privacy, the adoption of advanced protection technologies may be made mandatory. It also observes that one must not be influenced by the false rhetoric of lobbyists who attempt to confine privacy by design to a mere state of mind, an awareness of the principles of data protection when commercial products are designed, “immunising” the concept against any technical obligations.

120. According to TechAmerica, privacy by design is a process which organisations should follow at the start of a project and re-assess at regular intervals in order to check that data protection and security measures are still appropriate. It is important that, whatever requirement is laid down in the legal instrument, it remains a matter of procedures, not technology. The AFME BBA (banking) considers that the wording of the principle must be high-level and not prescriptive with regard to the measures to be adopted.

121. For its part, the FTC recommends in its report designed to improve protection of privacy in the United States that firms should adopt a privacy by design approach. This means constructing privacy protection mechanisms as part of day-to-day business practices. This protection includes the provision of reasonable security for personal data, limits on data collection to necessary data only and conservation of data for a limited period of time. On the basis of its own experience, the FTC encourages the Consultative Committee under Convention 108 to adapt the concept of adaptability when dealing with the question of privacy by design.

Rights – Obligations

17. The right of access should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the logic of the processing?

122. Adding the right of access to the origin of the data and to the logic underlying processing is absolutely necessary in the opinion of the AEDH, very important in the opinion of the Bulgarian Commission, and achieves consistency with the European Union rules in that of the ICUK and the British Ministry of Justice: the CIPPIC and the Garante consider it necessary in the growing context of the complex IT models on which criteria and assumptions are made, with potentially negative effects on individual privacy; and other replies state simply that it must be envisaged. The European Privacy Association fears, however, that given the involvement of large numbers of players in automated processing today, the obligation of transparency of processing - which the association supports - may not be achievable without excessive cost.

123. The AFME BBA (banking) supports the move provided it does not go beyond the right introduced by Directive 95/46, in so far as it would not mean obliging the persons concerned to keep information about data sources and entails only the duty to transmit the information about sources where they are known. On the question of keeping information about data sources, the reply of the German Insurance Association states that German data protection law contains an obligation to keep data about sources and recipients of data for a period of two years.

124. Portugal's Direcçao Geral da Politica de Justiça considers that access to processing logic requires that the data subject demonstrate an interest and must be limited to the extent strictly necessary to satisfy that interest. Thus access to processing logic must not translate into unwarranted disclosure of business secrets.

125. CEA Insurers of Europe points out that some requests for access are frivolous and seek only to check the processing of data rather than verify the accuracy of the data processed. Consequently, this group believes that the right of access should be limited and that introduction into Convention 108 of a right of access to the logic should not be envisaged. This stance is shared by the Data Industry Platform, which is anxious to preserve commercial secrets, companies' competitiveness and their intellectual property. Internal predictive analysis techniques are of crucial value to the business world and should not be disclosed to third parties. The FEDMA shares this view.

126. Privacy International considers that the protection secured to intellectual property (patents) permits transparency without fear. In exceptional cases where secrecy must be preserved, the supervisory authorities should be allowed confidential access to the algorithms in order to check their legitimacy.

127. The FTC provides information about cases in the United States in which consumers are entitled to obtain information from firms which have taken action with negative consequences for them. One case illustrates the possibility of achieving a compromise between transparency and business secrecy: credit reporting agencies are not required to reveal exactly how credit ratings are calculated, but the disclosure required of them must include the range of possible credit ratings in the assessment model and the key factors negatively affecting the consumer's rating.

128. The CNIL insists that the exercise of access, opposition, correction and blocking rights must be free of charge.

129. The Garante invites the Committee to reflect, where technologies based on cloud computing are concerned, on the introduction of a right to know the physical location and the country where data are kept or where distribution servers are situated.

18. The right of opposition is justified in cases where the data processing is not based on the data subject's consent. The link between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect for, and exercise of, this right.

The right of opposition

130. The right of opposition is justified in the opinion of most contributors, but not in all circumstances. One might consider introducing this right into the Convention for reasons of consistency with the directive. Some replies (others disagree) state that this right should be granted even where processing is based on consent, if it is admitted that consent can be revoked in all circumstances.

131. A similar right exists in Canadian law (PIPEDA), permitting the persons concerned to object by way of opt-out to collection, utilisation and communication of personal data for non-necessary purposes.

132. The Bulgarian Commission stresses that the link between the right of opposition and the right of oblivion consists in the right of opposition being exercised taking account of the purpose of processing, whereas the right of oblivion is exercised irrespective of the justification of processing in relation to purpose.

The right of oblivion

133. The following picture emerges from most of the replies. The right of oblivion may be particularly indicated and practicable in certain circumstances (mainly in the framework of social networks). Otherwise it is problematic in several respects:

134. - It conflicts with the rights, interests and freedoms of others, in particular freedom of expression, freedom of the press (it impinges on the conservation of full archives), the duty of memory, business continuity, management of employee files, the duty to keep evidence, etc. It is a hindrance to historical research. It may also hamper the provision of certain services such as medical treatment in cases where the medical history of the person concerned is not known;

135. - It is difficult to implement once the data have been rendered public on the Internet.

136. In the opinion of the APEP, the right of oblivion is not a sub-category of the right of opposition in so far as, unlike the latter, it has retroactive effect. So the question is whether individuals must be responsible sine die for their past actions and whether it is desirable for them to have the right to rewrite their past, and consequently that of others.

137. Some contributors favour its inclusion in the Convention. Others - more numerous - consider that further reflection is needed before a decision is taken, giving thought in particular to the practical obstacles to its implementation and clarifying the cost and practical implications of including such a right. Clarification should be forthcoming about the data which would be the subject of such a right of erasure: if it concerns data obtained from the person concerned, does it also cover analytical data or meta-data created by the data controller of the file? It is stressed that the right of oblivion cannot be absolute in any case. The Data Industry Platform points out that this right should not appear in a list of general principles tested over a period of time. On this point, it is supported by the Garante, which does not look favourably on the inclusion of so controversial a right in the Convention.

138. The Data Industry Platform argues that, if the inclusion of this right were to be envisaged, it should imperatively be limited to services based on data which the individuals concerned have themselves supplied and which are made accessible to third parties as part of the service. Some other replies echo this standpoint, limiting the scope of such a right to social networks.

139. Yet others, lastly, regard this right as utterly unrealistic both technically and legally (EMOTA - European E-commerce and Mail Order Trade Association) or as having disastrous consequences for publishers and freedom of expression (European Newspaper Publishers Association et European Federation of Magazine Publishers) and say it should be dismissed absolutely (a stance taken especially by the various contributors from the press sector).

19. Should there be a right guaranteeing the confidentiality and integrity of information systems?

140. It should be noted that many contributors omitted to reply to this question.

141. Some replies were positive, but in most cases not backed up by arguments. Among them, the Garante stands out by stating that, in its view, the rights concerned in this question, like those covered by the following questions, are those which most justify the Convention's list of rights and general principles.

142. However, other contributors fail to see on what grounds the confidentiality and integrity of systems should be the subject of a right, instead of strengthening the security constraints set out in Article 7. The extra value of such a right remains to be demonstrated and should be set against the risk of dilution and loss of legibility of the rights enshrined in the Convention.

143. The Czech Office for Personal Data Protection observes that the guarantee of confidentiality relates to the obligations on controllers, not to the rights.

20. Should a right 'not to be tracked' (RFID tags) be introduced?

144. Some contributors agree with the idea of introducing such a right, subject to reasonable exceptions.

145. The Garante, commenting on the three rights referred to in questions 19, 20 and 21, considers this right essential.

146. Other contributors say that further consideration is called for.

147. The AEDH and the Data Industry Platform think that application of the general protection principles (in particular the prohibition on keeping data for longer than the aim requires) provides a satisfactory answer. Similarly, the CIPPIC believes that the principles of "confidentiality, privacy and accuracy" ensure this right. The CLPC also believes that there is no need to lay down a separate right if personal data are defined in such a way as to encompass information about an individual's communications, location or behaviour.

148. The European Privacy Association suggests that, rather than a right not to be tracked, there should be an option not to be tracked. The persons concerned should be informed about tracking practices and be given the option and the technical means of refusing to be traced/located. The APEP also refers to an option to be made available to the persons concerned, rejecting the idea of a prohibition. Tracking technologies are not bad in themselves, but certain uses must be limited in cases where privacy must prevail. The association argues that the tracing of Alzheimer patients, lost luggage, vehicles, children or animals should not be prevented. Moreover, the concept of tracking is not limited to RFID but also covers cookies in particular.

149. Several contributors observe that a right must not be based on a targeted technology, which would run counter to the aim of preserving the technologically neutral character of the Convention.

150. Nor must legislation stand in the way of all progress and all technical development in this matter.

21. Should users of information and communication technologies have a right to remain anonymous?

151. The Garante, commenting on the three rights referred to in questions 19, 20 and 21, considers this right essential.

152. The AEDH observes that social life is based on a dialectic of identification and anonymity that is no longer found in present-day conditions where, for example, consultation of public information leaves identifying traces, just like any form of payment, since there is no electronic currency equivalent to banknotes. This constitutes a "basic defect". In such a context, everything rests on the length of time for which data collected are kept. In this association's opinion, there should be social and technical guarantees of the right to anonymity.

153. Similarly, the CIPPIC is of the opinion that anonymity is a right which deserves to be separately formulated and protected. The ability to act anonymously is central to the

protection of privacy in public and semi-public space. It points out that the wording of this principle as proposed by the CLPC on the basis of the provisions of Australian privacy legislation is interesting. The CLPC suggests the following wording: "Individuals must have the option of not identifying themselves when dealing with an entity, or of using a pseudonym, except where there is a legal obligation of identification or where it is not practicable for the entity to deal with individuals who are not identified or who use a pseudonym".

154. Several contributors are in favour of a right to anonymity provided the law is not infringed.

155. Other contributors, on the other hand, do not think there should be a right to anonymity because it could lead to an increase in fraud and crime, it being difficult if not impossible to find the perpetrators. The European Privacy Association is opposed to a generic right to be absolutely anonymous when using ICTs, which would conflict with practical needs (individuals need information about their use of ICTs, at least for the purpose of billing such use) and for the requirements of law enforcement bodies. However, this information must be protected against misuse. As the EPA sees it, this protection is already secured by the Convention. The APEP quotes the example of an employer legitimately overseeing the actions of his employees for which he will be held responsible.

156. The Data Industry Platform, contrary to the contributors mentioned above, inquires whether the off-line community really knows about default mechanisms or a right to remain anonymous in normal circumstances. For example, the staff of a public library know that library's users and their reading preferences. The group sees no reason to draw a distinction between the on-line community and the off-line one.

22. Should Convention 108 address the question how to strike the right balance between protection of personal data and freedom of expression (new notion of press and journalism in the context of Web 2.0.)?

157. In general yes, but replies differ somewhat about the manner of doing so.

158. The European Privacy Association believes that the - decisive - link which exists between the right of data protection and freedom of expression should be defined. A link with Article 10 of the European Convention on Human Rights could be addressed in the preamble to Convention 108.

159. In the opinion of the European Broadcasting Union (EBU-UER), Article 9. 2. b) together with paragraph 58 of the explanatory report is not sufficient and should be explicitly strengthened in order to grant a clear exemption from the application of certain data protection rules to journalistic activities, especially in the audio-visual field. That organisation accordingly proposes amending Article 9 by the addition of a paragraph reading: "9. 2. c) - protect the processing of personal data carried out solely for journalistic purposes". The EBU regards such an amendment as vital in order to preserve the freedom of the media, investigative journalism and the confidentiality of journalists' sources.

160. The Centre for Socio-Legal Studies proposes drafting a new provision requiring the parties to strike a balance between the fundamental interest of freedom of expression and the values which data protection seeks to uphold. The provision

should also mention the need to adopt broad, but not absolute, exemptions from the protection rules for these activities. As for the possibility of expressly stipulating minimum exemptions in accordance with Article 10 of the European Convention on Human Rights, this requires fuller consideration. The explanatory report should state explicitly that this provision to safeguard freedom of expression is not limited to the press. In principle, it should hold good for any form of public expression.

161. The APEP considers that any regulations in this field must be flexible: they must provide criteria to serve as guidelines, but not themselves conduct a predetermined general assessment. By contrast, the CNIL considers that similar provisions to those in the French law on data processing and freedoms could be incorporated into the Convention. That body thinks it would be helpful to state at the European level the exemptions and derogations from which processing might benefit. In the CLPC's opinion, it would not be appropriate for the Convention itself to weigh up all aspects of these conflicting interests, but it ought nonetheless to contain a provision recognising the public interest of freedom of expression.

162. The AEDH observes that even in Europe there is no consensus on the limits to be set on freedom of expression in the name of protection of privacy. That association therefore advocates an initiative aimed at bringing standpoints and procedures closer together. That initiative should be taken in the Council of Europe, possibly in conjunction with UNESCO.

163. The ICUK wonders where the line should be drawn in the age of blogging. Up to what point will supervisory authorities be required to regulate individuals' behaviour on line?

164. The Italian Garante is opposed to the inclusion in the Convention of provisions which might prove less flexible than what emerges from the case-law of the European Court of Human Rights in reconciling the two rights, or which might fail to strike the same balance. As for the questions linked specifically to Web 2.0, it seems premature to lay down specific rules.

Sanctions and remedies

23. Should class actions be introduced into the Convention? Should more scope be given to alternative dispute resolution mechanisms?

165. **Class actions**. Various contributors regard the introduction of class actions as desirable, either in certain specific contexts[1] or generally, and say that this should be mentioned in the Convention.[2] Others point out that, on the contrary, the general character of the Convention does not lend itself to this.[3] Similarly, the question of sanctions and remedies ought more broadly to fall within the scope of domestic law rather than that of the Convention.[4] Some replies also observe that the class action debate should take place in a broader context than that of data protection.[5]

166. Apart from these methodological objections, there are some misgivings about the general introduction of class actions. Some replies state that they are not needed,[6] or even that they are inappropriate.[7] It is argued that class actions are of no interest where the person concerned already has the benefit of protection mechanisms to rely on in the exercise of his/her rights[8] (eg. data protection authorities). Class actions would be useful only when other remedies are unreliable[9] or ineffective, in short where recourse to this remedy would be of direct practical interest.[10] Others note that data protection disputes are specific to individuals and would therefore not lend themselves to class actions.[11] Yet other contributors point to the risk that class actions would permit the harmful use of data protection rules.[12] Dealing with class actions at this stage would also create uncertainty.[13]

167. However that may be, the Convention could nonetheless emphasise the benefits and value of class actions if it did ultimately deal with the question of remedies.[14] And if recourse to class actions were envisaged, it would be above all important to assess the impact they might have in the European context.[15]

---

[1] Opinion of the CIPPIC.
[2] Opinion of the Czech Republic's Office for Personal Data Protection; opinion of the Mauritius Data Protection Commissioner; opinion of the Ukrainian Ministry of Justice; opinion of the United Kingdom Information Commissioner's Office; opinion of the Direccao Geral da Politica de Justica.
[3] Opinion of the EPA; opinion of the Italian Garante per la protezione dei dati personali. Various contributors stress that this is a matter for domestic law; see, for example, the opinion of the Lithuanian State Data Protection Inspectorate.
[4] Opinion of the CEA.
[5] Opinion of the EBF.
[6] Opinion of the Data Industry Platform.
[7] Opinion of the ENPA-FAEP.
[8] Opinion of the German Insurance Association. See also the opinion of TechAmerica Europe, which also emphasises that the extent of public demand for class actions should be assessed.
[9] Opinion of the Italian Garante per la protezione dei dati personali.
[10] Opinion of the UK Ministry of Justice.
[11] Opinion of the FEDMA.
[12] Opinion of the APEP.
[13] Opinion of the EMOTA.
[14] Opinion of the Cyberspace Law and Policy Centre; opinion of CLSR-IAITL-ILAWS; opinion of Privacy International.
[15] Opinion of the CNIL; opinion of the UK Ministry of Justice.

168. **ADR.** Some contributors express support for recourse to ADR,[16] which some regard as rapid and inexpensive.[17] Similarly, some replies stress the potential importance of self-regulation in a modern data protection system.[18] Some emphasise, however, that the question of dispute resolution by alternative methods is one that should be dealt with by states, not the Convention.[19] Furthermore, it is a question that ought to be discussed in the European Union context.[20] Perhaps the Convention could confine itself to laying down an obligation to create alternative dispute resolution mechanisms while leaving the substance to domestic legislation.[21]

169. Various contributors observe that if the decision is taken to resort to ADR, this should in any case not limit the other remedies available to the persons concerned.[22] Recourse to ADR could not then be a mandatory stage prior to any judicial remedy - or other remedy still involving public authority, just as it could not be the only means of settling disputes available to the persons concerned.[23] Where ADR was resorted to, it could for example be recommended that existing arbitration bodies be involved in the application of data protection.[24]

170. Several contributors mention the importance of the role which the **data protection authorities** - including data protection officers - can play in settling disputes. For example, some consider that they could be given competence to settle disputes.[25] In this connection they need the freedom to establish procedures, and the Convention could lay down a standard-setting framework for the purpose.[26] For example, it would be appropriate to give data protection authorities the power to act ex officio.[27] They could also have the possibility of intervening freely before the ordinary and administrative courts dealing with current cases.[28]

171. **Other.** On a quite different subject, some contributors stress the usefulness of creating **incentives** to respect for data protection (eg. a gradual easing of the administrative requirements based on the firm's background in simply complying with data protection principles, or even exceeding the normal requirements).[29]

[16] Opinion of the FEDMA; opinion of the UK Information Commissioner's Office; opinion of the UK Ministry of Justice.
[17] Opinion of the FEDMA.
[18] Opinion of the UK Information Commissioner's Office.
[19] Joint opinion of the AFME and BBA.
[20] Opinion of the CEA.
[21] Opinion of the Direccao-Geral da Politica de Justica.
[22] Opinion of the CIPPIC.
[23] Opinion of the CNIL.
[24] Opinion of the German Insurance Association.
[25] Opinion of the GDD; opinion of the UK Information Commissioner's Office.
[26] Opinion of the UK Information Commissioner's Office.
[27] Opinion of the German Insurance Association.
[28] Opinion of the CNIL.
[29] GSI in Europe.

The law applicable to data protection

24. Should a rule determining the law applicable to data processing (in cases where different jurisdictions are involved) be considered?

172. **General**. The problem of the law applicable appears important to many contributors, who repeatedly recommend that the rules be clarified, particularly in the context of cloud computing (an example frequently cited). The problem of applicable law is sometimes regarded as an obstacle for organisations not based in the European Union, and wishing to establish processing operations there; European law would apply without its application being justified by a sufficiently strong link between the individual situation and Union law.[30] However, some contributors reply that they are convinced that the current rules on defining the applicable law are effective.[31]

173. The risk that arises here is a classic of private international law: either there is a risk of absence of protection (no law applicable) or more than one set of rules might be applicable.[32] The replies reveal two convergent trends, both calling for greater harmonisation: more harmonisation of basic concepts and rules is desired, and greater clarity in determining the law applicable. On the latter point, a variety of suggestions is contained in the replies.

174. **Harmonisation of basic rules**. It is clear that the harmonisation of national regulations and interpretation in accordance with the Convention would have a positive effect[33] in so far as the question of the law applicable - as long as it is the law of a Council of Europe member state - would be less important if legal systems were harmonised. Accordingly, some contributors highlight the possibility of integrated harmonisation in the most global framework.[34] Promotion of international cooperation, establishment of guidelines on data protection issues and "rules between states" would help resolve the difficulties currently being encountered.[35] So concept definitions should be clarified, as should their application in the member states.[36]

175. Several contributors point to the potentially universal - or global - nature of the Council of Europe Convention and the desirability of promoting it at international level as a **global standard**.[37] Indeed, the Madrid resolution, which is universally accepted, could be drawn on in the drafting of certain of Convention 108's principles.[38] These considerations are relevant both to questions of applicability of national law and to cross-border data flows: the two sets of issues are clearly linked.

176. **Rule to determine the law applicable to data protection**. The complex nature of the question of applicable law is mentioned in some of the opinions submitted,

[30] Joint opinion of the AFMI and BBA.
[31] Opinion of the Data Industry Platform; opinion of the FEDMA.
[32] Opinion of the CNIL.
[33] See, for example, the opinion of TechAmerica Europe.
[34] GSI in Europe.
[35] Opinion of the CEA.
[36] Opinion of the EFAMRO-ESOMAR.
[37] Opinion of the AEDH; opinion of the AFAPDP and the OIF; opinion of the CNIL; opinion of Spyros Tsovilis; opinion of the Direccao-Geral da Politica de Justica.
[38] Opinion of the CNIL

particularly in such contexts as that of cloud computing.[39] Some contributors stress that it would be a complicated matter to settle this question in the framework of the Convention, especially in view of the role played by the European Union in this connection:[40] coordination is necessary. Clearly, further thought must be given to the question, but perhaps the complexity of the problem would require a case-by-case approach rather than establishing a general rule.

177. Nevertheless, some contributors think that the question should be dealt with in the Convention[41] - in conjunction with Directive 95/4642 - or in any event that this would be desirable[43] [44] as affording better legal security. Others believe that the inclusion of such a provision might perhaps constitute an obstacle to possible ratification of Convention 108 by non-member states of the Council of Europe,[45] whereas it should be made an attractive instrument for those states.[46] The protection of data and privacy are highly complex and technical issues about which political debate is still ongoing.[47] Some replies state that the Convention should lay down a general principle, leaving the rest to national regulations and international cooperation.[48] However, one reply says that it is simply not desirable for the Convention to decide the question of the law applicable to data protection.[49]

178. However that may be, different opinions offer possible approaches to determining the law applicable to data protection.

179. With regard to **jurisdiction criteria**, the replies contain different proposals. For example, with each state guaranteeing equivalent protection - in the context of the European Union, say -, an enterprise active in several of its states would be required to comply with only one set of regulations, that of its principal place of establishment.[50] According to certain contributors, each state's rules should be deemed equivalent.[51] Generally speaking, the replies favour the application of a "country of origin principle".[52]

180. Other differences are proposed as regards jurisdiction criteria. Some contributors suggest that the place of establishment of the data controller of the file be taken as

[39] See, for example, the opinion of the UK Ministry of Justice.
[40] Joint opinion of the AFME and BBA.
[41] Opinion of the Bulgarian Personal Data Protection Commission; opinion of the Cyprus Commissioner for Personal Data Protection; opinion of the Czech Office for Personal Data Protection; opinion of the Lithuanian State Data Protection Inspectorate; opinion of the Data Protection Commissioner of Mauritius; opinion of Mydex (point 24); opinion of the Ukraine Data Protection Authority.
[42] Opinion of the EPA; opinion of the German Insurance Association.
[43] Opinion of the CNIL; opinion of the Cyberspace Law and Policy Centre; opinion of the EBF; opinion of CLSR-IAITL-ILAWS; opinion of Privacy International. The T-PD should also look into the question (opinion of the Direccao-Geral da Politica de Justica).
[44] In the opinion of the Albanian Data Protection Commissioner, it is pointed out that the Convention should provide for a rule enabling the states to lay down specific rules on this.
[45] Opinion of the CNIL.
[46] Opinion of CLSR-IAITL-ILAWS.
[47] US Federal Trade Commission.
[48] Ukraine – Ministry of Justice.
[49] Opinion of the Italian Garante per la protezione dei dat personali.
[50] Opinion of the EPA.
[51] Opinion of the APEP.
[52] Opinion of the FEDMA; opinion of TechAmerica Europe.

the principal criterion, a secondary criterion being the place to which the data controller of the file specifically directs his activity.[53] The direction of activities criterion would be one to take into account in particular when the controller of the file is situated outside the territory of the European Union.[54] It is sometimes suggested that the law applicable should be that of the country where the bulk of the processing operations takes place or, if that cannot be determined, the law of the country where the controller of the file is situated.[55]

181. By contrast, some contributors go so far as to consider that, where several jurisdictions are involved, "the persons concerned should be entitled to choose the most protective legislation in the event of problems".[56] Alternatively, that the law applicable to data protection should be that of the "victim"[57] (the person concerned). This rule could possibly be seen as the principle, with exceptions being envisaged.[58]

182. Whatever the criteria ultimately adopted, **considerations to be taken into account** in their definition are mentioned in the replies. For example, if the aim is to reduce the risk of "forum shopping",[59] the "compliance burdens" on enterprises should also be limited.[60] Similarly, simplification of the rules is called for in the case of enterprises belonging to the same international group with cross-border activities,[61] in particular by clarifying responsibilities within such groups.

183. Some replies state that any change to the rules in question should entail improvement in the free movement of personal data.[62] Changes to the rules of private international law must not involve a competitive disadvantage for the internal (European Union) market.[63] Nor should any "extra-jurisdictional reach" be introduced.[64] In order to avoid the last-mentioned problem, it is recommended that account be taken of individuals' desire to use the services of suppliers wholly outside the European Economic Area (EEE-EEA) and foster properly informed decision-making.[65]

184. On a different point, the rules determining the law applicable should not permit persons bringing cases against media enterprises to choose a forum where the protection rules are more stringent than those in the state where such enterprises are established, which would pose a risk to freedom of expression.[66]

---

[53] Opinion of the CNIL.
[54] Opinion of the APEP.
[55] Opinion of the EPA.
[56] Opinion of the AEDH.
[57] Opinion of the Senegal Data Protection Commission.
[58] The opinion of the Direccao-Geral da Politica de Justica appears to follow this line, recommending that the law of the person concerned be applied where it refers to "national law". However, it emphasises that exceptions should certainly be provided for, especially in the context of the European Union.
[59] Opinion of the CEA.
[60] Opinion of the CEA; opinion of the EMOTA; opinion of the ENPA-FAEP; FEDMA.
[61] Opinion of the Data Industry Platform; opinion of the GDD.
[62] Joint opinion of the AFME and BBA; opinion of the Data Industry Platform; opinion of the EMOTA; opinion of the FEDMA.
[63] Opinion of the APEP.
[64] Joint opinion of the AFME and BBA.
[65] Joint opinion of the AFME and BBA.
[66] Opinion of the ENPA-FAEP.

185. A Convention provision on applicable law should not hamper the domestic protection afforded to consumers.[67]

186. Account must also be taken of the fact that any change to the rules determining the law applicable has implications not only for "B2C" relations but also for relations between enterprises and governmental authorities, including law enforcement authorities.[68]

187. Lastly, although the replies received often deal with the question of the law applicable, some of them mention criteria of competence and the need for them to be pragmatic. If appropriate, a distinction could be drawn between civil jurisdiction and criminal jurisdiction; the T-PD concerned should look into this question.[69]

Data protection authorities

25. How to guarantee their independence and ensure international cooperation between national authorities?

188. Better cooperation is called for.[70] Some contributors observe that cooperation between data protection authorities should probably be the subject of additional measures written into the Convention[71] (others do not share that view and prefer to leave the problem to domestic law[72]): international mechanisms facilitating cross-border cooperation in the application of data protection rights;[73] mechanisms to be defined, such as a common forum;[74] a minimum of regulation should at all events be stipulated.[75] The aim then would be to clarify and facilitate international cooperation - cooperation conditions, joint action procedures - but not to impose it.[76] Some contributors consider, on the contrary, that cooperation has to be imposed where problems are global.[77]

189. It is also proposed that authorities should be able to carry out joint investigations on the territory of several member states - international complaints, cross-border controls[78] - but without this jeopardising their funding.[79] In this connection it is important to clarify the powers of authorities to take action abroad.[80] Others observe that effort should be put into the better recognition between data protection authorities of the measures taken by them - including notifications.[81] One contributor went so far as to propose the creation of a supranational authority.[82]

---

[67] Opinion of the CIPPIC.
[68] Opinion of TechAmerica Europe.
[69] Opinion of the Direccao-Geral da Politica de Justica.
[70] Joint opinion of the AFME and BBA.
[71] Opinion of the AEDH.
[72] Opinion of CLSR-IAITL-ILAWS; opinion of Privacy International; opinion of the Ukraine Ministry of Justice.
[73] Opinion of the EBF.
[74] Opinion of the Italian Garante per la protezione dei dati personali.
[75] Opinion of the Lithuanian State Data Protection Inspectorate.
[76] Opinion of the CNIL.
[77] Opinion of the APEP.
[78] Opinion of the Bulgarian Personal Data Protection Commission; opinion of the CNIL.
[79] Opinion of the Bulgarian Personal Data Protection Commission.
[80] Opinion of the CNIL.
[81] Opinion of TechAmerica Europe.
[82] Opinion of the Senegal Data Protection Commission.

190. Finally, it was stated that Article 13 § 3. b) of the Convention is an obstacle to international cooperation between authorities because it prevents the transfer of personal data involved in disputed processing despite it being necessary to the settlement of disputes.[83]

191. Concerning the independence of these control authorities, the Portuguese Direccao-Geral da Politica de Justica proposes the following criteria: there must be guarantees that the data protection authority is not subject to instructions or conditions such as to hinder its independent decision-making capacity, that is to say there must be no interference of any kind on the part of a public or private entity; and the necessary resources for its functioning must be covered by the public budget.

26. Should their role and tasks be specified?

192. Yes. The AEDH observes that the additional protocol is not very explicit about the functions and powers of the supervisory authorities. All the examples given in the explanatory report deserve to be codified in the actual text of the protocol. The CLPC suggests that the provision be transferred to the Convention itself.

193. In the view of the ICUK, clarification would be welcome in a landscape where the existing national authorities present a multi-coloured patchwork. Their educational role should in any case be kept. The CNIL considers that these authorities' a posteriori role should be strengthened. The Bulgarian Commission requests that an excessive burden should not be placed on these authorities. The CLPC stresses one function in particular: the obligation of accountability, especially to the public, in respect of obligations to deal with complaints. The Italian Garante believes it would be important to clarify cooperation mechanisms between authorities, perhaps by envisaging specific interaction machinery or joint forums.

194. In addition, in the opinion of the EPA and the APEP, their decisions should be mutually recognised by other states parties; this would be valuable, especially with regard to BCRs. The CIPPIC calls for thought to be given to making the decisions of supervisory authorities binding in law through the common law concept of stare decisis.

[83] Opinion of the UK Information Commissioner's Office.

Transborder data flows

27. The aim of Convention 108 was to reconcile effective data protection with the free flow of information, regardless of frontiers. The Convention's principles have been further developed in an additional protocol (CETS 181, 2001). In principle, an adequate level of protection must be ensured.

28. Do we need to reconsider the notion of "transborder data flows" entirely in the Internet age, where data instantaneously flow across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?

29. Should there be different rules for the public and private sectors? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?

195. Questions concerning TDFs should be considered in parallel with the problems of the law applicable to data protection. One reply contained a warning: in a networking world, there are limits to the extent to which data flows can or should be controlled.[84]

196. Various contributors emphasise that the current approach to the rules on transborder data flows is not suited to the present technological context;[85] individuals involved in the virtual world have their data sent from one jurisdiction to another with just a few clicks, sometimes to a third state outside the European Union which does not guarantee adequate protection.[86] The present approach does not work effectively, being burdensome to persons acting in benign fashion and ineffective for those acting with more malice.[87] The TDF issue should be tackled more realistically.[88] At the very least, it should be stated in the context of the Internet when such transfers take place;[89] the concept of TDF must be clarified, or even reconsidered.[90] The work of the APEC was mentioned on one occasion when a more workable system was called for.[91]

197. Several contributors consider that "the approach in principle should not be changed" and that adequate protection is required.[92] Similarly, regarding the requirement of adequate protection, it is stressed that the provisions of the additional protocol should be incorporated into the Convention,[93] if appropriate by clarifying the rules.[94]

---

[84] Opinion of CLSR-IAITL-ILAWS.
[85] Joint opinion of the AFME and BBA; Opinion of the Czech Office for Personal Data Protection.
[86] Opinion of TechAmerica Europe.
[87] Opinion of CLSR-IAITL-ILAWS.
[88] Opinion of the UK Information Commissioner's Office.
[89] Opinion of the Albanian Data Protection Commissioner; opinion of the Bulgarian Personal Data Protection Commission.
[90] Opinion of the EBF; opinion of the Italian Garante per la protzeione dei dati personali.
[91] Opinion of the US Federal Trade Commission.
[92] Opinion of the AEDH, in favour of the requirement of an adequate protection standard. See also the opinion of the UK Ministry of Justice.
[93] Opinion of the Cyberspace Law and Policy Centre; opinion of CLSR-IAITL-ILAWS; opinion of Privacy International; opinion of the Direccao-Geral da Politica de Justica.
[94] Opinion of CLSR-IAITL-ILAWS.

By contrast, some replies call for a new legal instrument, separate from the Convention, containing the necessary detailed rules.[95] Others observe that the Convention is general in character and that it is rather the responsibility of the member states to deal with this complex question,[96] whereas national differences aggravate the present practical difficulties.[97]

198. Contributors are interested in the **definition of adequacy**. Some believe that a list of minimum guarantees defining "adequate level of protection" should be drawn up,[98] possibly modelled on what is being done in the European Union.[99] Some argue that Convention 108 should recognise explicitly the decisions on adequacy taken by the European Commission on the basis of Article 26 of Directive 95/46.[100] However, others criticise what is done at the European level, emphasising that what the Commission demands is sometimes more a matter of equivalence that of adequacy;[101] the Convention should reassert that only adequacy is required.[102] Thus the process could be faster and simpler.[103] The Convention could make the assessment process more transparent and, in this context, could be at the heart of developing widely recognised standards.[104]

199. More specifically, it is suggested that adequacy could be assessed on the basis of broad data processing sectors - the financial sector, IT sub-contracting, PNR etc. - ;[105] for example, a sector could be deemed to guarantee adequate protection even if the country of establishment does not offer adequate protection guarantees.[106] So adequacy should not mean a general analysis of the law of the third party state concerned, but should rather relate to the particular circumstances of the case, and in particular the controller of the file - or the sub-contractor - located in the third party state, the law of that state being only one factor in the analysis.[107] Some replies also link the adequate protection principle directly to the accountability principle.[108]

200. In the European Union context, when a third party state does not guarantee adequate protection, there are various tools which may nevertheless make TDFs possible. Some contributors call in this connection for better recognition, in the European Union context, of **Binding Corporate Rules [BCR]** or **Model Contractual Clauses [MCC]** so that data transfers inside an international group of companies subject to the same strict rules do not need specific authorisation from the data protection authorities;[109] the rules should be simplified.[110] The authorisation regime

---

[95] Opinion of the Cyprus Data Protection Commissioner.
[96] Opinion of the FEDMA.
[97] Opinion of CLSR-IAITL-ILAWS.
[98] Opinion of the Albanian Data Protection Commissioner; opinion of the Bulgarian Personal Data Protection Commission.
[99] Opinion of the Albanian Data Protection Commissioner.
[100] Opinion of the APEP.
[101] Opinion of CLST-IAITL-ILAWS.
[102] Opinion of the UK Information Commissioner's Office.
[103] Opinion of the UK Information Commissioner's Office.
[104] Opinion of CLSR-IAITL-ILAWS.
[105] Opinion of the Albanian Data Protection Commissioner.
[106] Opinion of the UK Information Commissioner's Office.
[107] Opinion of the UK Information Commissioner's Office. The US Federal Trade Commission also notes that the situation of the data recipient is not taken into account; opinion of the UK Ministry of Justice, referring to the Madrid Declaration as a starting-point for reflection.
[108] Opinion of TechAmerica Europe; opinion of the UK information Commissioner's office.
[109] Joint opinion of the AFME and BBA.

poses problems of time taken and costs incurred;[111] formalities should be simplified in cases of recourse to MCCs or BCRs approved by the authorities.[112] Greater flexibility is moreover desired in model contract clauses which, in the European Union at present, for example, do not reflect the reality of cloud computing so that the model becomes inappropriate.[113] It would also be desirable to promote TDF codes of conduct accepted by all authorities for the protection of the relevant data.[114]

201. Some of those who replied consider that **minimum international rules** should be laid down for TDFs.[115] That is the purpose of the Madrid resolution, which should be incorporated into a binding text.[116] But in all hypothetical cases where such minimum rules are desirable, the potential risk of a "race to the bottom" [117] should be borne in mind; some replies observe that such a race would be the inevitable consequence of an attempt to establish global minimum rules, destroying protection of privacy in a cross-border context and thus making that minimum undesirable.[118] Others point out that before thinking about global minimum standards, it is necessary to establish the procedural framework for their definition, involving all regions and all the parties concerned.[119]

202. Finally, on another aspect of the question, the data protection officer (DPO) could play a part with regard to TDFs, and a European DPO might be appointed for a group of companies present in different European Union countries.[120]

---

[110] Opinion of the Data Industry Platform; opinion of the EMOTA.
[111] Opinion of the German Insurance Association.
[112] Opinion of the AFCDP (p.4).
[113] Joint opinion of the AFME and BBA.
[114] Opinion of the CEA.
[115] Opinion of the CEA; opinion of the Cyprus Data Protection Commissioner; opinion of the EPA; opinion of the German Insurance Association; opinion of the AFCDP.
[116] Opinion of the APEP.
[117] Opinion of the CIPPIC.
[118] Opinion of the Cyberspace Law and Policy Centre; opinion of CLSR-IAITL-ILAWS; opinion of Privacy International.
[119] Opinion of the US Federal Trade Commission.
[120] Opinion of the AFCDP.

Role of the Consultative Committee

30. Convention 108 established a committee to facilitate its application and, where necessary, to perfect it. Should the hitherto primarily consultative role of the committee be strengthened? If so, which functions should be developed further? Standard-setting, dispute resolution, monitoring functions?

203. Most of those who replied to this question are in favour of reinforcing the role of the Consultative Committee, though some think it should remain unchanged.

204. The committee should evolve to become a veritable data protection authority, with responsibility, in its monitoring role, for identifying innovations well in advance and making relevant recommendations and, in its disputes resolution role, for receiving complaints where the parties are faced with a cross-border problem (AEDH). The Mauritius Data Protection Commissioner points out, with regard to disputes, that the national authorities and also individuals should be able to make application to this Committee once it becomes a binding authority. A stronger monitoring role would permit verification of the manner in which the Convention is implemented at national level and provide for action to be taken where it is poorly implemented (CNIL). Its role should be strengthened only in respect of supervisory functions (CEA Insurers of Europe), or these functions but also in the issuing of standards (Cyprus Data Protection Commissioner; CLSR-IAITL-ILAWS consortium), or only in issuing standards (European Privacy Association). The Committee should have a part to play in coordination of practices, experience and suggestions made by national data protection authorities, as well as a monitoring role in respect of international cooperation (Czech Office for Personal Data Protection; Lithuanian State Data Protection Inspectorate).

Role in preparing legislation

205. However, care must be taken to ensure that this does not create additional burdens on the states parties and other national authorities. Any duplication with other existing supra-national bodies, and adoption of contradictory standards, must be avoided (ICUK). The Data Industry Platform believes there there is a real risk of duplication and opposes the idea of adding an extra layer to institutions which already exist. As they see it, standard-setting, dispute resolution and monitoring functions are matters for which self-regulation is the best solution.

206. The Cyprus Data Protection Authority and the Italian Garante both point out that any strengthening of the Committee's role will depend on the human and financial resources made available. The Garante therefore argues that steps should be taken to guarantee the availability of those resources.

207. The CNIL offers a suggestion regarding the membership of the Committee. In view of its "absolutely essential" part in the practical architecture of the Council of Europe, the CNIL considers that it would be highly desirable to review its composition. Since the data protection authorities bear prime responsibility for the application of Convention 108, and because these authorities have the benefit of practical experience and expertise, they should be the ones to appoint representatives to the Committee, not the governments. The government representatives are the only persons present on the European Committee on Legal Cooperation, which is involved in drafting texts.

208. The American FTC suggests that the revision of the Convention be used as an opportunity to think about the contribution and support which the Committee might seek from industry and other key players. The role and the work of the ENISA Permanent Stakeholder Group could be taken as an example of how to obtain backing and facilitate dialogue with industry about the Convention, by reason of the important part which that group plays in the legal framework of data protection in the European Union and elsewhere in the world.