International Standards on the Protection of Personal Data and Privacy

The Madrid Resolution

International Conference of Data Protection and Privacy Commissioners
5th November 2009.

presentation

It is a pleasure for me to introduce to you the Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data, which was welcomed by the International Conference of Data Protection and Privacy Commissioners, held in Madrid on 5 November 2009.

The joint efforts of the privacy guarantors from fifty countries, coordinated by the Spanish Data Protection Agency, has resulted in a text that seeks to reflect the many approaches that the protection of this right allows for, by integrating legislations on five continents. This consensus document adds new values by stressing the universal nature of the principles and guarantees underlying this right, and by contributing to a better protection of rights and freedoms of individuals in a globalized world, characterised by cross-border flows of information.

As of now, we the supervisory and monitoring authorities take on the challenge of its dissemination and promotion, from our strong commitment to provide our citizens with a better protection of their privacy and personal data.

ARTEMI RALLO LOMBARTE
DIRECTOR OF THE SPANISH
DATA PROTECTION AGENCY

Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data

For further information about the drafting process of this document, please visit the Spanish Data Protection Agency website, at www.agpd.es, where an Explanatory memorandum and other useful documentation are available.

Part I: General Provisions

1 Purpose

The purpose of this Document is:

a. To define a set of principles and rights guaranteeing the effective and internationally uniform protection of privacy with regard to the processing of personal data; and

b. The facilitation of the international flows of personal data needed in a globalized world.

2 Definitions

In the context of this Document:

a. "Personal data" means any information relating to an identified natural person or a person who may be identified by means reasonably likely to be used.

b. "Processing" means any operation or set of operations, automated or not, which is performed on personal data, such as collection, storage, use, disclosure or deletion.

c. "Data subject" means the natural person whose personal data are subject to processing.

d. "Responsible person" means any natural person or organization, public or private which, alone or jointly with others, decides on the processing.

e. "Processing service provider" means any natural person or organization, other than the responsible person that carries out processing of personal data on behalf of such responsible person.

3 Scope of application

1. This Document is aimed in its application at any processing of personal data, wholly or partly by automatic means, or otherwise in a structured manner, and carried out in the public or the private sector.

2. Applicable national legislation may lay down that the provisions of this Document do not apply to the processing of personal data by a natural person in the course of activities related exclusively to his/her private and family life.

4 Additional measures

1. States may supplement the level of protection provided for in this Document with additional measures guaranteeing a better protection of privacy with regard to the processing of personal data.datos de carácter personal.

2. In any case, the provisions of this Document shall be an appropriate basis for permitting international transfers of personal data, where such transfers are carried out pursuant to section 15 of this Document

5 Restrictions

States may restrict the scope of the provisions laid down in sections 7 to 10 and 16 to 18 of this Document, when necessary in a democratic society in the interests of national security, public safety, for the protection of public health, or for the protection of the rights and freedoms of others. Such restrictions should be expressly provided by national legislation, establishing appropriate guarantees and limits meant to preserve the rights of the data subjects.

Part II:
Basic Principles

6

Principle of lawfulness and fairness

1. Personal data must be fairly processed, respecting the applicable national legislation as well as the rights and freedoms of individuals as set out in this Document and in conformity with the purposes and principles of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

2. In particular, any processing of personal data that gives rise to unlawful or arbitrary discrimination against the data subject shall be deemed unfair.

7

Purpose specification principle

1. The processing of personal data should be limited to the fulfilment of the specific, explicit and legitimate purposes of the responsible person.

2. The responsible person should not carry out any processing that is non-compatible with the purposes for which personal data were collected, unless he has the unambiguous consent of the data subject.

8

Proportionality principle

1. The processing of personal data should be limited to such processing as is adequate, relevant and not excessive in relation to the purposes set out in the previous section.

2. In particular, the responsible person should make reasonable efforts to limit the processed personal data to the minimum necessary.

9

Data quality principle

1. The responsible person should at all times ensure that personal data are accurate, as well as sufficient and kept up to date in such a way as to fulfil the purposes for which they are processed.

2. The responsible person shall limit the period of retention of the processed personal data to the minimum necessary. Thus, when personal data are no longer necessary to fulfil the purposes which legitimized their processing they must be deleted or rendered anonymous.

10

Openness principle

1. Every responsible person shall have transparent policies with regard to the processing of personal data.

2. The responsible person shall provide to the data subjects, as a minimum, information about the responsible person's identity, the intended purpose of processing, the recipients to whom their personal data will be disclosed and how data subjects may exercise the rights provided in this Document, as well as any further information necessary to guarantee fair processing of such personal data.

3. When personal data have been collected directly from the data subject, the information must be provided at the time of collection, unless it has already been provided.

4. When personal data have not been collected directly from the data subject, the responsible person must also inform him/her about the source of personal data. This information must be given within a reasonable period of time, but may be replaced by alternative measures if compliance is impossible or would involve a disproportionate effort by the responsible person.

5. Any information to be furnished to the data subject must be provided in an intelligible form, using a clear and plain language, in particular for any processing addressed specifically to minors.

6. Where personal data are collected on line by means of electronic communications networks, the obligations set out in the first and second paragraphs of this section may be satisfied by posting privacy policies that are easy to access and identify and include all the information mentioned above.

11

Accountability principle

The responsible person shall:

a. Take all the necessary measures to observe the principles and obligations set out in this Document and in the applicable national legislation, and

b. have the necessary internal mechanisms in place for demonstrating such observance both to data subjects and to the supervisory authorities in the exercise of their powers, as established in section 23.

Part III: Legitimacy of processing

12 General principle of legitimacy

1. As a general rule, personal data may only be processed in one of the following situations:

a. After obtaining the free, unambiguous and informed consent of the data subject;

b. Where a legitimate interest of the responsible person justifies the processing, and the legitimate interests, rights and freedoms of data subjects do not prevail;

c. Where the processing is necessary for the maintenance or the performance of a legal relationship between the responsible person and the data subject; or

d. Where the processing is necessary for complying with an obligation imposed on the responsible person by the applicable national legislation, or is carried out by a public authority where necessary for the legitimate exercise of its powers.

e. Where there are exceptional situations that threaten the life, health or security of the data subject or of another person.

2. The responsible person shall provide simple, fast and efficient procedures that allow data subjects to withdraw their consent at any time and that shall not entail undue delay or cost, nor any gain whatsoever for the responsible person.

13

Sensitive data

1. The following personal data shall be deemed to be sensitive:

a. Data which affect the data subject's most intimate sphere; or

b. Data likely to give rise, in case of misuse, to:
   i. Unlawful or arbitrary discrimination; or
   ii A serious risk to the data subject..

2. In particular, those personal data which can reveal aspects such as racial or ethnic origin, political opinions, or religious or philosophical beliefs as well as those data relating to health or sex life, will be considered sensitive data. The applicable national legislation may lay down other categories of sensitive data where the conditions referred to in the previous paragraph are met.

3. Due guarantees shall be established to preserve the rights of the data subjects by applicable national legislation, which shall lay down additional conditions for processing sensitive personal data.

14

Provision of processing services

The responsible person may carry out processing of personal data through one or more processing service providers, without considering it a disclosure of data to a third party, provided that:

a. The responsible person ensures that the processing service provider guarantees, at least, the level of protection contained in this Document and in the applicable national legislation; and

b. The legal relationship is established through a contract or legal instrument that allows proving its existence, scope and content, and that sets out the processing service provider's obligation to comply with these guarantees and to ensure the personal data are processed in compliance with the instructions of the responsible person.

15 International transfers

1. As a general rule, international transfers of personal data may be carried out when the State to which such data are transmitted affords, as a minimum, the level of protection provided for in this Document.

2. It will be possible to carry out international transfers of personal data to States that do not afford the level of protection provided for in this document where those who expect to transmit such data guarantee that the recipient will afford such level of protection; such guarantee may for example result from appropriate contractual clauses. In particular, where the transfer is carried out within corporations or multinational groups, such guarantees may be contained in internal privacy rules, compliance with which is mandatory.

3. Moreover, national legislation applicable to those who expect to transmit data may permit an international transfer of personal data to States that do not afford the level of protection provided for in this Document, where necessary and in the interest of the data subject in the framework of a contractual relationship, to protect the vital interests of the data subject or of another person, or when legally required on important public interest grounds

4. Applicable national legislation may confer powers on the supervisory authorities referred to in section 23 to authorize some or all of the international transfers falling within their jurisdiction, before they are carried out. In any case, those who expect to carry out an international transfer of personal data should be capable of demonstrating that the transfer complies with the guarantees provided for in this Document and in particular where required by the supervisory authorities pursuant to the powers laid down in paragraph 23.2.

Part IV: Rights of the Data Subject

16

Right of access

1. The data subject has the right to obtain from the responsible person, upon request, information on the specific personal data subject to processing, as well as the source of such data, the purposes of processing and the recipients or categories of recipients to whom such data are or will be disclosed.

2. Any information to be furnished to the data subject must be provided in an intelligible form, using a clear and simple language.

3. Applicable national legislation may limit the repetitive exercise of this right that would require the responsible person to respond to multiple requests within short periods of time, unless the data subject states a legitimate reason when exercising this right.

17

Rights to rectify and to delete

1. The data subject has the right to request from the responsible person the deletion or rectification of personal data that might be incomplete, inaccurate, unnecessary or excessive.

2. Where justified, the responsible person should carry out the rectification or deletion requested. The responsible person should also notify this fact to third parties to whom personal data had been disclosed, where they are known.

3. Deletion of personal data is not justified where personal data must be retained for the performance of an obligation imposed on the responsible person by the applicable national legislation, or possibly by the contractual relations between the responsible person and the data subject.

18

Right to object

1. The data subject may object to the processing of personal data where there is a legitimate reason related to his/her specific personal situation.

2. The exercise of this right to object is not justified where the processing is necessary for the performance of a duty imposed on the responsible person by the applicable national legislation.

3. Any data subject may also object to those decisions which produce legal effects based solely on automated processing of personal data, except when the decision had been specifically requested by the data subject or when it is necessary for the establishment, the maintenance or the performance of a legal relation between the responsible person and the data subject. In the latter case, the data subject must be able to put his/her point of view in order to defend his/her right or interest.

19

Exercise of these rights

1. The rights provided for in sections 16 to 18 of this Document may be exercised:

a. Directly by the data subject, who shall satisfactorily establish his/her identity to the responsible person.

b. Through a representative, who shall satisfactorily establish his/her status to the responsible person.

2. The responsible person must implement procedures to enable data subjects to exercise the rights provided for in sections 16 to 18 of this Document in a simple, fast and efficient way, which do not entail undue delay or cost nor any gain whatsoever for the responsible person.

3. When a responsible person concludes that, pursuant to the applicable national legislation, the exercise of rights under this Part is not justified, the data subject should be informed of the reasons that led to this conclusion.

Part V: Security

20 Security measures

1. Both the responsible person and any processing service provider must protect the personal data subject to processing with the appropriate technical and organizational measures to ensure, at each time, their integrity, confidentiality and availability. These measures depend on the existing risk, the possible consequences to data subjects, the sensitive nature of the personal data, the state of the art, the context in which the processing is carried out, and where appropriate the obligations contained in the applicable national legislation.

2. Data subjects should be informed by those involved in any stage of the processing of any security breach that could significantly affect their pecuniary or non-pecuniary rights, as well as the measures taken for its resolution. This information should be provided in good time, in order to enable data subjects to seek the protection of their rights.

21 Duty of confidentiality

The responsible person and those involved at any stage of the processing shall maintain the confidentiality of personal data. This obligation shall remain even after the ending of the relationship with the data subject or, when appropriate, with the responsible person.

Part VI: Compliance and Monitoring

22 Proactive measures

States should encourage, through their domestic law, the implementation by those involved in any stage of the processing of measures to promote better compliance with applicable laws on the protection of privacy with regard to the processing of personal data. Such measures could include, among others:

a. The implementation of procedures to prevent and detect breaches, which may be based on standardized models of information security governance and/or management.

b. The appointment of one or more data protection or privacy officers, with adequate qualifications, resources and powers for exercising their supervisory functions adequately.

c. The periodic implementation of training, education and awareness programs among the members of the organization aimed at better understanding of the applicable laws on the protection of privacy with regard to the processing of personal data, as well as the procedures established by the organization for that purpose.

d. The periodic conduct of transparent audits by qualified and preferably independent parties to verify compliance with the applicable laws on the protection of privacy with regard to the processing of personal data, as well as with the procedures established by the organization for that purpose.

e. The adaptation of information systems and/or technologies for the processing of personal data to the applicable laws on the protection of privacy with regard to the processing of personal data, particularly at the time of deciding on their technical specifications and on the development and implementation thereof.

f. The implementation of privacy impact assessments prior to implementing new information systems and/or technologies for the processing of personal data, as well as prior to carrying out any new method of processing personal data or substantial modifications in existing processing.

g. The adoption of codes of practice the observance of which are binding and that include elements that allow the measurement of efficiency as far as compliance and level of protection of personal data are concerned, and that set out effective measures in case of non compliance.

h. The implementation of a response plan that establishes guidelines for action in case of verifying a breach of applicable laws on the protection of privacy with regard to the processing of personal data, including at least the obligation to determine the cause and extent of the breach, to describe its harmful effects and to take the appropriate measures to avoid future breaches.

23 Monitoring

1. In every State there shall be one or more supervisory authorities, in accordance with its domestic law, that will be responsible for supervising the observance of the principles set out in this Document.

2. These supervisory authorities shall be impartial and independent, and will have technical competence, sufficient powers and adequate resources to deal with the claims filed by the data subjects, and to conduct investigations and interventions where necessary to ensure compliance with the applicable national legislation on the protection of privacy with regard to the processing of personal data.

3. In any case, without prejudice to any administrative remedy before the supervisory authorities referred to in the preceding paragraphs, including judicial oversight of their decisions, data subjects may have a direct recourse to the courts to enforce their rights under the provisions laid down in the applicable national legislation.

24

Cooperation and coordination

1. The Authorities mentioned in the previous section shall try to cooperate with each other to achieve a more uniform protection of privacy with regard to the processing of personal data, at both national and international level. For the purpose of facilitating this cooperation, each State should be able to identify the competent supervisory authorities on its territory as needed.

2. These authorities will in particular realise make every effort to

a. Share reports, investigation techniques, communication and regulatory strategies and any other useful information for exercising their functions more effectively, in particular following a request for cooperation by another supervisory authority in conducting an investigation or intervention;

b. Conduct co-ordinated investigations or interventions, at both national and international level, in matters where the interests of two or more authorities are shared;

c. Take part in associations, working groups and joint fora, as well as in seminars, workshops or courses that contribute to adopting joint positions or to improving the technical ability of the staff serving such supervisory authorities;

d. Maintain the appropriate level of confidentiality in respect of the information exchanged in the course of cooperation.

2 States should encourage the negotiation of cooperation agreements among supervisory authorities, regional, national and international, that contribute to a more effective observance of this section.

25 Liability

1. The responsible person will be liable for the pecuniary and/or non-pecuniary damages caused to the data subjects as a result of processing of personal data that had infringed the applicable laws on the protection of privacy with regard to the processing of personal data, except if the responsible person can demonstrate that the damage can not be attributed to him. This liability is without prejudice to any action by the responsible person against the processing service provider involved at any stage of the processing.

2. States will promote suitable measures to facilitate the access of data subjects to the relevant judicial or administrative processes that allow them to obtain compensation for the damage referred to in the preceding paragraph.

3. The aforementioned liability should exist without prejudice to the penal, civil or administrative penalties provided for, where appropriate, in case of violation of the provisions of domestic laws on the protection of privacy with regard to the processing of personal data.

4. The implementation of proactive measures such as those described in section 22 of this Document should be considered when determining the liability and penalties provided for in this section.

Proposed resolution on International Standards of privacy

PROPOSED RESOLUTION ON INTERNATIONAL STANDARDS OF PRIVACY

PROPOSERS:

Agencia Española de Protección de Datos
Préposé fédéral à la protection des données et à la transparence (Switzerland)
European Data Protection Supervisor
Commission Nationale de l'Informatique et des Libertés (France)
Irish Data Protection Commissioner
Office of the Privacy Commissioner of Canada
Office for Personal Data Protection (Czech Republic)
Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (Germany)
Garante per la Protezione dei Dati Personali (Italy)
College Bescherming Persoonsgegevens (Netherlands)
New Zealand Privacy Commissioner
Information Commissioner's Office (United Kingdom)

CO-PROPOSERS:

Agència Andorrana de Protecció de Dades (Andorra)
Agència Catalana de Protecció de Dades (Spain)
Agencia de Protección de Datos de la Comunidad de Madrid (Spain)
Agencia Vasca de Protección de Datos (Spain)
Office of the Data Protection Supervisor (Isle of Man)
Estonian Data Protection Inspectorate
State Data Protection Inspectorate of the Republic of Lithuania
Data Protection and Freedom of Information Commissioner of Berlin (Germany)
Data Protection Commissioner of Schleswig-Holstein (Germany)
National Direction for Personal Data Protection (Argentina)
Commissioner for Data Protection (Malta)
Commission on Computers and Liberties (Burkina-Faso)
Personal Data Protection Commissioner (Cyprus)
Data Protection Ombudsman (Finland)
Information Commissioner (Slovenia)
Hellenic Data Protection Authority

Nothing that:

The 30th International Conference of Data Protection and Privacy Commissioners in Strasbourg unanimously adopted the Resolution on the urgent need for protecting privacy in a borderless world, and for reaching a Joint Proposal for setting International Standards on Privacy and Personal Data Protection.

The resolution established a mandate to establish a Working Group, co-ordinated by the Spanish Data Protection Agency as the host of the 31st Conference and composed of interested Data Protection Authorities, to draft and submit to the 31st Conference a Joint proposal for setting international standards on privacy and personal data protection.

In keeping with this mandate, the Spanish Data Protection Agency established a Working Group and promoted and coordinated the work for elaborating a Joint Proposal for a Draft of International Standards.

The Working Group has drafted a Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data, based on principles that are present in different instruments, guidelines or recommendations of international scope and that have received a broad consensus in their respective geographical, economic or legal areas.

The Joint Proposal has been drafted assuming that all these principles and common approaches bring elements of value in the defence and improvement of privacy and personal information, with the aim of expanding them by adding solutions and specific provisions which could apply irrespective of any differences that may exist between the different existing models of data protection and privacy.

Accordingly, the Conference resolves:

1. To welcome the Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data attached as Annex 1 to this resolution. The Joint Proposal demonstrates the feasibility of such standards, as a new step towards the development of a binding international instrument in due course.

2. To state that the Joint Proposal provides a set of principles, rights, obligations and procedures that any legal system of data protection and privacy should strive to meet. In this perspective, the processing of personal data in the public and private sector would be performed, in a more internationally uniform approach:

   a. fairly, lawfully and in a proportionate manner in relation to specific, explicit and legitimate purposes;

   b. on the basis of transparent policies, informing adequately the data subjects and without any arbitrary discrimination against them;

   c. ensuring the accuracy, the confidentiality and the security of the data as well as the legitimacy of the processing, and the rights of data subjects to access, rectification, erasure of data and to object against their processing;

   d. implementing the principles of accountability and liability, even if the processing operations are carried out by service providers on behalf of the controller;

   e. offering more appropriate guarantees where the data are sensitive;

   f. ensuring that personal data transferred internationally benefits from the level of protection provided by the above-mentioned set of standards,

   g. subject to the monitoring of independent and impartial supervisory authorities provided with adequate powers and resources also in connection with their duty to cooperate among themselves;

   h. in a new and modern framework of proactive measures, such as those oriented in particular to prevent and detect breaches and based on the appointment of privacy officers as well as on efficient audits and privacy impact assessments.

3. To invite the Data Protection and Privacy Authorities accredited to the International Conference, to disseminate the Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data, as widely as possible.

4. To entrust the organizing authorities of the 31st and 32nd International Conference to co-ordinate a Promotion Group, composed of the interested Data Protection Authorities, which will be responsible for:

a. disseminating and promoting the Joint Proposal among relevant private entities, experts and national and international authorities as a basis for further work towards the development of a binding international convention, and in particular to the bodies and organizations mentioned in the Montreux Declaration; and

b. exploring and reporting back on other ways in which the Joint Proposal might be used as a basis for developing international understanding and cooperation on data protection and privacy, particularly in the context of enabling international transfers of personal data to take place in a way that safeguards the rights and freedoms of individuals.

5. To request the Promotion Group:

a. to coordinate its work with the Conference's Steering Group on Representation before International Organisations, and

b. to report on any relevant progress at the 32nd International Conference to ensure continued attention for the subject of this resolution.

Explanatory Note

The 30th International Conference of Data Protection and Privacy Commissioners adopted the Resolution on the urgent need for protecting privacy in a borderless world, and for reaching a **Joint Proposal for setting International Standards on Privacy and Personal Data Protection**, jointly submitted by the data protection authorities from Switzerland and Spain and supported by twenty other authorities.

In that resolution, the Conference recalled several declarations and resolutions adopted during the last ten years that aimed to strengthen the universal nature of the right to the protection of personal data and privacy, and which called for the development of a universal convention for the protection of individuals with regard to the processing of personal data.

Furthermore, the resolution stated that the Conference considered the rights to data protection and privacy as fundamental rights of individuals, irrespective of their nationality or residence, while noting that the persisting data protection and privacy disparities in the world, in particular due to the fact that many states have not yet passed adequate laws, harm the exchange of personal information and the implementation of effective global data protection.

Therefore, the resolution expressed the conviction of the Conference that recognition of these rights requires the adoption of a universal legally binding instrument establishing, drawing on and complementing the common data protection and privacy principles laid down in several existing instruments, and strengthening the international cooperation between data protection authorities.

In this regard, the resolution expressed the Conference's support for the Council of Europe's efforts to improve the fundamental rights to data protection and privacy and invites States, whether or not members of the organization, to ratify the Convention for the protection of individuals with regard to automatic processing of personal data and its additional protocol, while confirmed its support for actions carried out by APEC, OECD and other regional and international fora to develop effective means to promote better international standards of privacy and data protection.

The resolution mandated the Spanish Data Protection Agency, as host of the 31st International Conference, to establish and coordinate a Working Group composed of interested data protection authorities, to draft and submit to its closed session a Joint proposal for setting international standards on privacy and personal data protection.

The resolution included a list of criteria to govern the drafting process of this Joint Proposal, and in particular indicated that it should be developed by encouraging broad participation of public and private organizations and entities, with the purpose of obtaining the broadest institutional and social consensus.

In keeping with this mandate, the Spanish Data Protection Agency established the Working Group referred to in the resolution and promoted and coordinated the work for elaborating a Joint Proposal for a Draft of International Standards.

The Spanish Data Protection Agency sent invitations to participate in the preparatory Working Group to all the data protection and privacy authorities accredited to the International Conference. The authorities listed in Annex 2***** expressed their desire to take part in this Working Group and consequently joined it.

The Working Group met in January and June 2009. The first meeting agreed on the drafting methodology of the Joint Proposal and its material scope, while the second discussed an advanced version of the draft proposal for its subsequent submission to the 31st Conference.

According to the criteria and methodology set forth by the Strasbourg Resolution and agreed by the Working Group, the Spanish Data Protection Agency has carried out an intensive activity and elaborated various documents, which incorporated contributions from data protection and privacy authorities and other public entities related to data protection, as well as from experts from the industry, the legal profession, academia and international organizations and NGOs.

In particular, the Working Group has drafted a Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data, based on principles that are present in different instruments, guidelines or recommendations of international scope and that have received a broad consensus in their respective geographical, economic or legal areas.

The Joint Proposal has been drafted assuming that all these principles and common approaches bring elements of value in the defence and improvement of privacy and personal information, with the aim of expanding them by adding solutions and specific provisions which could apply irrespective of any differences that may exist between the different existing models of data protection and privacy.

* AUTHORITIES BELONGING TO THE WORKING GROUP: CDATA PROTECTION COMMISSION (Austria),PRIVACY PROTECTION COMMISSION (Belgium),, COMMISSION ON COMPUTERS AND LIBERTIES (Burkina-Fasso),,OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, INFORMATION ACCESS COMMISSION OF QUEBEC (Canada), OFFICE FOR PERSONAL DATA PROTECTION (Czech Republic), EUROPEAN DATA PROTECTION SUPERVISOR, NATIONAL COMMISSION ON COMPUTERS AND LIBERTIES (France),FEDERAL DATA PROTECTION COMMISSIONER (Germany), DATA PRO TECTION AND FREEDOM OF INFORMATION COMMISSIONER OF BERLIN (Germany), DATA PROTECTION COMMISSIONER OF SCHLESWIG-HOLSTEIN (Germany), PRIVACY COMMISSIONER FOR PERSONAL DATA (Hong Kong), IRISH DATA PROTECTION COMMISSIONER, ITALIAN DATA PROTECTION AUTHORITY, DATA PROTECTION COMMISSION (Netherlands), NEW ZEALAND PRIVACY COMMISSIONER, NATIONAL DATA PROTECTION COMMISSION (Portugal), INFORMATION COMMISSIONER OF THE REPUBLIC OF SLOVENIA, SPANISH DATA PROTECTION AGENCY (Spain), CATALAN DATA PROTECTION AUTHORITY (Spain), DATA PROTECTION AGENCY OF MADRID (Spain), BASQUE DATA PROTECTION AGENCY (Spain), FEDERAL DATA PROTECTION COMMISSIONER (Switzerland), INFORMATION COMMISSIONER'S OFFICE (United Kingdom)