



INTERNATIONAL STANDARDS on Data Protection & Privacy



→ Jose Leandro Nunez Garcia
Advisor on International Affairs
Agencia Española de Protección de Datos

BACKGROUND

A long time global process

During last year, the main Internet Governance fora have expressed the need for **Global Standards on Data Protection and Privacy**:

IGF 2009 – Chairman’s Summary

“The Latin America and Caribbean regional meeting stressed the importance of privacy and remarked on the need for legal and regulatory harmonization generally within and among countries”.

The International Conference of Data Protection and Privacy Commissioners has been also claiming for years for this kind of **Global Standards**:

2007 – Montreal

These discussions reflect a growing recognition within the data protection and privacy community that data protection and privacy legislation, while essential to ensuring the protection of personal information, is not, by itself, sufficient.

International standards also have a role to play as a mechanism for assisting parties to establish and demonstrate compliance with legal requirements of a data protection and privacy nature.



→ Background

The 30th International Conference of Data Protection and Privacy Commissioners **adopted unanimously** a draft resolution proposed by Switzerland and Spain that mandated the **organizer of the 31st Conference** to establish a Working Group to draft a Joint Proposal for setting **International Standards on privacy and personal data protection.**

The Working Group was **composed by...**

- 24 data protection and privacy authorities
- 6 observer institutions

With **contributions from** representatives of:

- Governments
- Industry
- University
- Civil Society

→ Background



Barcelona Meeting



Draft Joint Proposal (v1,2,3)



Explanatory Memorandum



Bilbao Meeting



Final Draft Joint Proposal

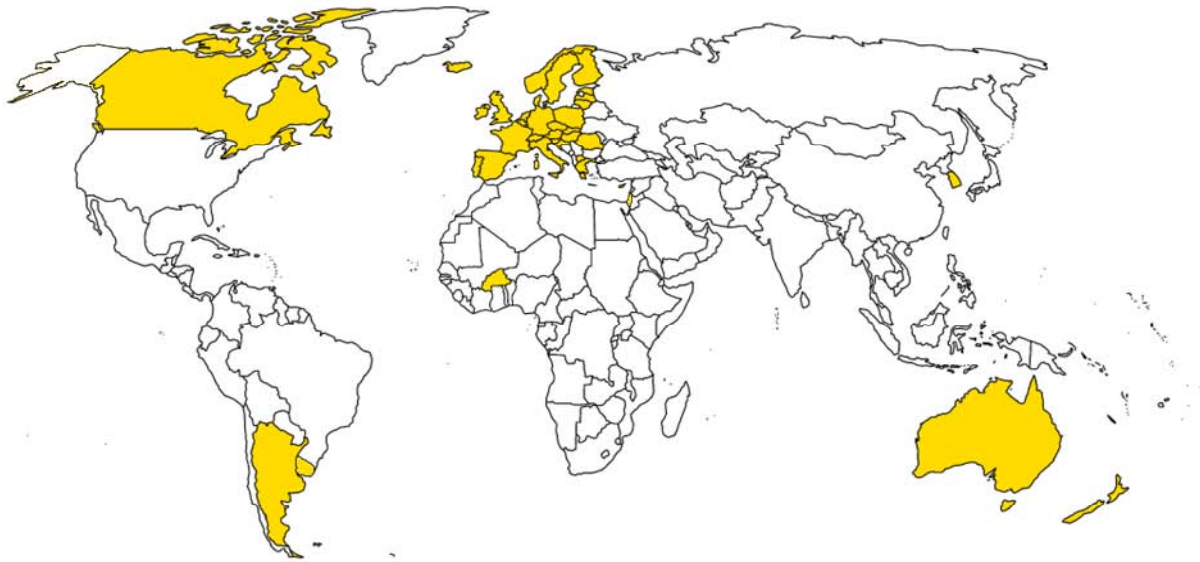


31st International Conference



→ Background

The document has been welcomed by
the 31st International Conference,
composed by
80 authorities from 42 countries





→ Background

Through a Resolution, the Conference entrusts Spain and Israel to co-ordinate a **Contact Group** responsible for...

- disseminating and promoting the Joint Proposal (...) as a basis for further work towards the development of a **binding international convention**...
- exploring (...) other ways (...) for developing **international understanding and cooperation** on data protection...

BODY OF THE STANDARDS

Drawing on the existing principles
and defining new ones



→ Main features

- **Not an innovative text** (based on existing principles and criteria) **but innovative solutions**
- **Not a European text**: looking for maximum consensus;
- Guarantees an **adequate level of protection**: principles, basic rights, redress and monitoring mechanisms;
- Importance of **international transfers**;
- Importance of **self regulation**;

The document is structured in **6 parts**

General provisions (purpose, definitions, scope)

Basic principles

Legitimacy for processing

Rights of the data subject

Security

Compliance and monitoring



→ Some relevant elements

Review of the controller and processor notions

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.



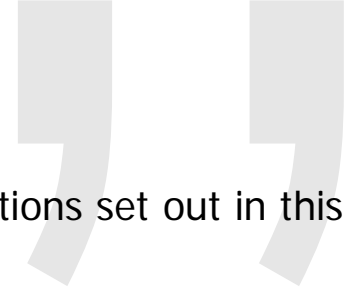
→ Some relevant elements

Inclusion of the
notion of **accountability**

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.





→ Some relevant elements

Adaptation of the definition of
sensitive data,
looking at the purposes of the
processing

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.

Catalogue of **Data Subject's Rights**

- Right of access
- Rights to rectify and to delete
- Right to object



→ Some relevant elements

International data transfers if the recipient (country or company) offers the level of protection provided by the International Standards

→ Some relevant elements

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, in particular where required by the supervisory authorities pursuant to the powers laid down in paragraph 23.2.



→ Some relevant elements

Need of appropriate
security measures

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.



→ Some relevant elements

Importance of **proactive measures**,
as a way for reducing liability
in case of infraction

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.

→ Some relevant elements

- 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.



→ Some relevant elements

Broader idea of **Supervisory Authority**,
which, for instance, may be an
arbitration institution or a
consumer authority

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.



A WELCOMED DOCUMENT

Statements supporting the initiative



Statement on the Joint Proposal for a draft International Standards... (02.09.2009)

The T-PD welcomes this attempt to provide an up-to-date statement of the applicable principles. Such an endeavour is particularly important and timely in an increasingly globalised world characterised by rapid technological development which transforms the communication between individuals and public and private organisations.

ORACLE®



accenture

Microsoft®

Google



P&G



IBM®



Statement on the necessity of international frameworks in support of the protection of Privacy... (27.10.2009)

In keeping with our strong commitment to sound management of personal information, we, the undersigned, **welcome the initiative** of the International Conference of Data Protection and Privacy Commissioners to explore frameworks for better global coordination of privacy regimes.



Madrid Privacy Declaration (03.11.2009)

“ Call for the establishment of a **new international framework for privacy protection**, with the full participation of civil society, that is based on the rule of law, respect for fundamental human rights, and support for democratic institutions”



¿FUTURE?



THANK YOU!



AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



www.agpd.es