



DIRECTIVES FOR HARMONISATION OF DATA PROTECTION IN THE IBERO-AMERICAN COMMUNITY

Summary: 1. Introduction; 2. The essential nucleus of the right to data protection. Harmonisation criteria; 3. Directives (principles, rights and obligations) a national law on personal data protection must contain.

I. Introduction

The paper on development of regulations and harmonisation prepared by the Permanent Working Group on Regulatory Development of the Ibero-American Data Protection Network, at the meeting held at Santa Cruz de la Sierra, Bolivia, from 3rd to 5th May 2006, considers one of the maximum priorities to be the Network task of preparing directive proposals to contribute to the regulatory initiatives on Data Protection arising in the Ibero-American Community.

Establishment of a harmonised framework for global data protection has been the main foundation stone for the adoption of the different international instruments that now exist on data protection.

The aim is thus to guarantee that worldwide development of trade is compatible with protection of personal rights, especially with regard to protection of information.

Thus, establishment of a homogeneous regulatory framework for the right to data protection, either by adopting binding supranational instruments, or by adopting domestic laws that enshrine the essential content of that right, will guarantee development of commerce in the area, facilitating information exchange between the different operators located in the Ibero-American States and these with third countries, in particular the Member States of the European Union, under conditions that are not restricted due to different levels of protection of the fundamental right to personal data protection.

Thus, the Preamble to the Recommendation by the OECD Council, concerning the Directives that govern protection of privacy and cross-border circulation of personal data, approved on 23rd September 1980, specifically recognises that "cross-border movement of personal data contributes to economic and social development", but at the



same time provides the reminder that “national laws on protection of privacy and cross-border movement of personal data may hinder such cross-border movement”.

For that reason, the Recommendation is based on the essential objective of “encouraging free movement of information between the member countries and avoiding creation of unjustified obstacles to development of economic and social relations between the member countries”. The aim is thus for cross-border exchange of information not to be limited by domestic data protection laws, whilst, at the same time, guaranteeing adequate protection of that fundamental right.

With greater clarity, if at all possible, Directive 95/46/EC, of the European Parliament and the Council, of 24th October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, expresses this idea in sections 6 to 9 of its Recitals, as follows:

“(6) Whereas, furthermore, the increase in scientific and technical cooperation and the coordinated introduction of new telecommunications networks in the Community necessitate and facilitate cross-border flows of personal data;

(7) Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions;

(8) Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas Community action to approximate those laws is therefore needed;



(9) Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy; whereas Member States will be left a margin for manoeuvre, which may, in the context of implementation of the Directive, also be exercised by the business and social partners; whereas Member States will therefore be able to specify in their national law the general conditions governing the lawfulness of data processing; whereas in doing so the Member States shall strive to improve the protection currently provided by their legislation; whereas, within the limits of this margin for manoeuvre and in accordance with Community law, disparities could arise in the implementation of the Directive, and this could have an effect on the movement of data within a Member State as well as within the Community;”

Most of the Constitutions of the States that constitute the Ibero-American Community contain provisions that guarantee to individuals the fundamental right to protection of their personal data and the “*habeas data*”. These provisions are also complemented by the resolutions handed down by the Courts of Justice and, in particular, those of the Constitutional Tribunals or Courts.

The constitutional and case law channels thus recognise a fundamental right of citizens to protection of their personal data, which is quite independent and autonomous from the right to privacy, and which consists of the right a citizen has to freely dispose of information concerning him.

Bearing this in mind, it is necessary for the public authorities to adopt the necessary measures to guarantee to their citizens the safeguard of that fundamental right, as an essential guarantee of the rule of law.

However, as stated, recognition of the fundamental right ought to be complemented with the establishment of a uniform set of regulations, to allow an equivalent level of protection of this right to be guaranteed through the regulatory recognition of the principles, rights and duties that configure it. Thus, one may ensure that, with that fundamental right being fully guaranteed, the Ibero-American States may benefit from the economic, social and cultural enrichment that may arise from free cross-border flows of information containing personal data.



This paper aims to define those essential profiles that configure the fundamental right to personal data protection, in order to offer the public authorities of the Ibero-American States some guidelines that may be of use in development of regulatory initiatives that might be adopted, thus facilitating establishment of a homogeneous framework for protection that permits the exchange of flows of information between them all and towards third States that have adopted similar standards of protection.

2. The essential nucleus of the right to data protection. Harmonisation criteria.

As already stated, most of the laws of the Ibero-American States recognise, either by direct reference to their Constitution, or as a consequence of the decisions adopted by their judicial bodies, the right of citizens to personal data protection, essentially by recognition of the resort to “*habeas data*”, by means of which a citizen may become aware of the data related to him, and of the purpose for which they are being processed by a specific controller, in which case correction, cancellation or updating may be requested.

Exercise of this right has given rise to a rich case law that has evolved toward recognition of a series of principles the Public Administrations and private entities processing personal data must abide by.

In Colombia, the Constitutional Court, through more than 140 rulings, has defined the scope and characteristics of *habeas data*, as well as the conditions that must apply to personal data processing, enshrined in Article 15 of the Constitution of 1991.

From the first ruling (T 414/92), the Court has established that the person is the holder and owner of the personal data. Thus, controllers are obliged to correctly administer and protect files and databases that contain personal or socially relevant information and not to violate the fundamental rights of citizens. The Constitutional Court pointed out, in general terms, that “*the function of managing a database must be based on the principles of liberty, need, veracity, integrity, inclusion, purpose, utility, restricted circulation, expiry and individuality*”. Specifically, it has stated that the controllers must: (1) Previously obtain authorisation from the persons whose data they intend to include in the database; (2) Notify the person on inclusion of his data in the database and inform him that information in the data base is to be reported in order that he may exercise his rights of correction and updating from the offset; (3) Permanent, self-regulated updating of the information to ensure it is true, complete and that factors that might change the good name of the data subject are not omitted; (4) *Ex officio* elimination of negative information that has expired as time has elapsed; (5) Compensation of damages caused due to lack of diligence, or due to possible failures in



management, processing or administration of personal data; (6) Guaranteeing the right to access, update and correct. These rights involve a citizen having *“the possibility (...) of immediately obtaining complete knowledge of how, why and where any datum related to him appears”*; (...) *if the information is erroneous or inexact, the data subject may demand, also with the right to an immediate reply, that the entity responsible for the system make the relevant corrections, clarifications or eliminations in it, in order to preserve his fundamental rights that have been violated*”. Finally, the Court has specified that, as a general rule, *“one may not gather information on “sensitive” data such as, for example, personal sexual orientation, political persuasion or religious beliefs, when this, either directly or indirectly, may lead to a policy of discrimination or marginalization”*.

In Spain, Ruling 292/2000, of 30th November, after severing the link between the right to data protection from the right to privacy, the Constitutional Court stated that *“the content of the fundamental right to data protection consists of a power of disposal and control over personal data that enables a person to decide which of that data may be provided by a third party, either the State, or a private concern, or which that third party may gather, and also allows the data subject to know who holds that personal data and for what purpose, being able to oppose that possession or use”*, adding that *“these powers of disposal and control over personal data, that constitute part of the content of the fundamental right to data protection, are specified legally in the power to consent the gathering, obtention and access to the personal data, its subsequent storage and processing, as well as its possible use or uses by a third party”*. Thus, it concludes that *“characteristic elements of the constitutional definition of the fundamental right to personal data protection are the rights of the data subject to consent gathering and use of his personal data and to knowledge concerning this. The indispensable factors to effectively apply that content are recognition of the right to be informed of who holds his personal data and for what purpose, and the right be able to oppose that possession and use, requiring the party concerned to put an end to the possession and use of the data. That is, to require the holder of the file to inform him what data it has on his person, accessing the relevant records and entries, and to what use they have been put, which also covers possible assignees; and when appropriate, requiring him to correct or cancel them”*.

In Mexico, the right to personal data protection applies, in the scope of public files at federal level, pursuant to the Federal Act on Transparency and Access to Governmental Public Information (LAI), and each State legislature includes ad-hoc chapters within the framework of its laws on access to information.



There are now two initiatives of constitutional reform, the first presented before the Senate, which enlarges Article 16 of the Political Constitution of the United States of Mexico in order to recognise the right to personal data protection as a fundamental right, this being approved in the preceding legislature and submitted to Parliament for the appropriate constitutional purposes, although its discussion and approval in the present one is still pending. The second initiative was presented on 27th March 2007, to reinforce that stated before, that already provides Parliament with specific powers to enact a law on the matter, stating that it is relevant not only due to being a matter of protection of human rights and fundamental liberties, but also due to the basic effects that these have on the domestic economy. *Finally, one must state that the Plenary Meeting of the IFAI, at its session on 25th April 2007, unanimously approved forming a working group between the private sector and that institution, to prepare a bill on personal data protection.*

In Peru, diverse case law by the Constitutional Court has pronounced upon the recognition of the right to informative self-determination recognised under Article 2, section 6) of the Political Constitution of 1993 and it has also stated the object of that right, its relational nature and declared the differences between it and other human rights, such as those of privacy, image and personal identity.

Thus, for example, the ruling dated 29th January, handed down in Case No. **1797-2002-HD/TC**, states that *“The right recognised in section 6) of Article 2 of the Constitution is that recognised academic authorities call the right to informative self-determination, and its object is to protect personal or family privacy, image and identity against the hazard posed by the use and eventual manipulation of data using electronic computers. On the other hand, although its object is to protect privacy, the right to informative self-determination may not be identified with the right to personal or family privacy, recognised in turn, by section 7) under present Article 2 of the Constitution (...) due to its very nature, the right to informative self-determination, being a subjective right that has the characteristic of being, prima facie and in general terms, a right of relational nature, as the requirements that demand its respect are quite often linked to protection of other constitutional rights.”* The ruling ratifies what is stated in the ruling handed down in File No. 666-1996-HD/TC, specifying what is included in protection of the right to informative self-determination through *habeas data*, stating that it covers: *“firstly, the capacity to jurisdictionally demand the possibility of access to the records of information, whether computerised or not, whatever their nature, in which the data on a person are kept. Such access may have the object of allowing knowledge of what is recorded, for what purpose and for whom recording of the information was performed, as well as the person or persons who gathered that information. Secondly, habeas data may have the purpose of adding data to the existing records, either due to the need to*



update those already recorded, or in order to include those not recorded, but which are necessary to obtain a full reference of the image and identity of the person affected. Likewise, in the right concerned, and should it not exist, by means of habeas data, a data subject may correct the personal and family information that has been recorded; prevent it being distributed for purposes other than those that justified its recording, or even, having the power to cancel that which should not reasonably be saved”.

As far as Europe is concerned, the fundamental right to personal data protection has been specifically recognised as a fundamental right, clearly distinguishable from the right to personal and family privacy of citizens, under Article 8 of the Charter of Fundamental Rights of the European Union, Article 8 of which states as follows:

“1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data that has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.”

Sections 2 and 3 of this principle define the essential content that must be embodied in the legislation that regulates the fundamental right to personal data protection. Thus:

- The data must be processed fairly;
- The data must be processed for specific purposes;
- Processing must be performed on the basis of consent by the person concerned or due to some other legitimate grounds foreseen by law;
- All persons shall be entitled to the rights of access, correction and cancellation of processing;
- There must be an independent authority in charge of safeguarding guarantee of the right.



On the other hand, different international instruments, from Supranational Bodies, of which all or part of the Ibero-American States are members, have come to establish the basic principles that configure the right to personal data protection.

Thus, the already cited recommendation by the OECD defines these principles, listing the following as basic:

1. Application to all data processing in the public and private sector;
2. Restrictive interpretation of possible exclusions to application of the principles;
3. Collection limitation principle;
4. Data quality principle;
5. Purpose specification principle;
6. Use limitation principle;
7. Security safeguards principle;
8. Openness principle;
9. Individual participation principle (Habeas data);
10. Accountability principle;
11. Guarantees of uninterrupted, safe cross-border flows of personal data between the States that abide by the principles;
12. Establishment of penalties and sufficient resources in the event of non-compliance.

In turn, one must take into account that the Guidelines for the regulation of computerised personal data files, adopted by Resolution 45/95 of the UN General Assembly, on 14th December 1990, that consider, as minimum guarantees, that national laws must foresee the following principles:

1. Legality and loyalty principle
2. Exactness principle
3. Purpose specification principle
4. Data subject access principle
5. Non- discrimination principle
6. Limitation of the power to make exceptions
7. Security principle
8. Supervision and penalties, through an authority that must provide guarantees of impartiality, independence and technical competence
9. Cross-border data flow based on similar safeguards
10. Minimum field of general application to all the public and private computerised files.



Along with these instruments, one must not forget the analysis performed within the scope of the European Union to fulfil Directive 95/46/EC. The importance of the Directive in the supra-European scope is essential; firstly as it is the international text that provides greater precision and detail in regulation of the principles, rights and duties that configure the fundamental right to data protection.

Moreover, one must remember that the basis for the EC Directive, as indicated, consists of establishing a harmonised protection framework for the right to personal data protection that guarantees the free flow of information within the European Union, thus favouring trade and enrichment arising from flows of information.

Lastly, one must not forget that Articles 25 and 26 of the EC Directive establish a specific regime for cross-border flows of personal data, requiring, as a starting point, that the State to which the data are to be sent provides an adequate level of personal data protection. Thus, the EC Directive provides fulfilment of the essential principle of balance between free disclosure of information and protection of citizens' rights.

Thus, taking on the principles that may be considered "adequate" to those foreseen in the Directive may be an appropriate starting point to facilitate cross-border flows of information on both sides of the Atlantic, maintaining adequate guarantees of the fundamental right to personal data protection. The aim is thus not to obtain transborder application of European laws, but rather to achieve adequate conciliation between both.

Within the Ibero- American area, one must recall the effort made within the scope of the UNESCO and the Latin American Information Society Strategy (ELAC) implemented within the CEPAL, in order to design the regulatory harmonisation mechanisms within the scope of privacy and personal data protection.

Likewise, one must point out that, in recent years, some States have adopted initiatives in this sense. Thus, one must not forget the regulatory developments carried out by Argentina, which led to Adoption of the Commission Decision of 30th June 2003. Indeed, Argentina is considered to guarantee an adequate level of protection with regard to the personal data transferred from the European Community.

Within that framework, it may be interesting for analysis the activity performed by the Working Group under Article 29 of 95/46/EC; in particular its Finding 4/2002, of 3rd October, on the standard of personal data protection in Argentina.



The diverse findings approved within that Working Group in relation to the standard of data protection in third party States have been taken as a reference in the working paper by the Group on personal data transfers to third countries: application of Articles 25 and 26 of the EC Data Protection Directive, approved on 24th July 1998, Chapter 1, which analyses what should be understood by “adequate protection”.

To that end, the paper defines two types of analysis that should be performed on the State legislation to assign data, in order to be able to define whether it is adequate: that concerning their material content, and that related to the mechanisms and procedures for application of the material legislation.

As to the material content, the laws of the destination State must contain the basic data protection principles that have traditionally been recognised by internationally recognised agreements and directives adopted in this field, that have been stated beforehand, these being as follows:

1. Limitation of purpose
2. Data quality and proportion
3. Transparency
4. Security and confidentiality
5. Rights of access, correction, suppression and blocking data
6. Restrictions on subsequent transfer
7. Special data categories
8. Direct marketing
9. Automated individual decision

These principles must at least be enshrined in the legislation of the State receiving the data, so it may be considered to offer an adequate level of protection.

Logically, in order to be able to consider there is an effective legal reflection of these principles in the laws of the State concerned, it will be necessary for those regulations to have a general scope of application to processing performed by the public and private sectors, so no further limits to their application are established than those related to merely personal or family activities by those performing them, or those that are adequate limitations on the fundamental right within the framework of activity of a democratic society.

On the other hand, as to the analysis related to procedures to apply the material rules, the paper considers that their existence is essential for the data protection system to be



able, in practice, to provide an adequate standard of protection, as it involves the existence of mechanisms to control the principles contained in the domestic laws.

As indicated in the paper, this element is generally materialised by establishment of an independent data protection authority and provision of adequate procedures that allow the data subject to obtain protection of his rights or to have the damages caused to them to be corrected.

Thus, as a general rule, one may consider that the State grants an adequate level of protection in cases in which it has laws to regulate protection of data containing the material principles that have been listed, and when there is an authority in charge of safeguarding their fulfilment, to which citizens may address their complaints, which has powers of inspection and investigation of processing.

A last essential requisite for that authority will be its capacity to impose measures that guarantee the effectiveness of the right, such as penalties in the event of breach or, at least, the capacity to ensure that the Courts of Law enforce those measures in cases in which exercise of its powers of investigation reveal breach of the data protection laws.

The analysis described has allowed the Group to establish a favourable finding on implementation of the standards of Personal Data Protection in the States with regard to which a decision by the Commission in that sense has subsequently adopted. It shall suffice to analyse the aforementioned Finding 4/2002, with regard to the standard of data protection in Argentina, to see that its structure and analysis is based on what is established in that working paper.

3. Directives (principles, rights and obligations) a national law on personal data protection must contain:

1. Scope of application

1.1. These directives shall be applicable to all manual or automated processing of personal data, the latter being understood as any information related to identified or identifiable individuals. Thus, the directives shall be applicable to processing carried out by all the public and private sector entities.

1.2. However, it shall be possible to exclude manual or non-automated processing from the directives when the data to be processed are not going to be included in a structured file using criteria that allow identification of persons whose data are subject to processing.



1.3. Likewise, the directives shall not be applicable to automated or manual processing of personal data that an individual performs for purposes exclusively related to his private or family life.

1.4. Exclusion from application of sections 2, 3, 4, 5, 6.1, 6.2, 6.3 and 8 of these directives shall be possible by means of a domestic law in the case of specific processing of personal data, to the extent that application of the directives may give rise to a risk for protection of national security, public order, public health or morality, and provided such a measure is strictly necessary and not excessive, within the scope of a democratic society.

2. Principles related to the purpose and quality of data

2.1. Fair, licit processing: data may only be gathered and processed in good faith, with strict respect for the Law and the rights of persons, and according to the terms foreseen in these directives.

2.2. Limitation of purpose: the data may only be gathered and processed to fulfil specific, explicit, legitimate purposes related to the activity of the party processing them.

Data may not be processed for purposes other than those for which they were collected, unless there is sufficient authorisation to do so, as established in section 3 of these directives.

2.3. Principle of proportionality: Only data that are adequate, pertinent and not excessive for the purposes stated in the preceding point may be processed.

2.4. Principle of exactness: Data must remain exact, complete and updated, according to the true situation of the person to which they refer.

2.5. Principle of conservation. Data must be cancelled or made anonymous when they have ceased to fulfil the purposes for which they were obtained and processed.

3. Authorisation for processing

3.1. Data may only be gathered or processed if consent has been obtained from the data subject.



3.2. However, the law may establish cases in which the consent of the data subject is not required to process personal data, according to the circumstances that arise in each case and, in all circumstances, as long as that exception does not damage the fundamental rights of the party concerned. In particular, the law may allow data processing without the consent of the data subject when it is performed within the framework of a legal relation, or by an Authority exercising the powers attributed to it.

3.3. Data that reveals the ideology, Trade Union membership, religion or beliefs of the data subject may only be processed with his consent, unless he has made them manifestly public.

3.4. Data concerning health, racial origin and the sexual life of the data subject may only be gathered and processed in the cases mentioned in the preceding paragraph, or when a law so provides.

3.5 In all cases, these directives shall not hinder adequate medical treatment of the person concerned, nor attention to a vital urgency he might have.

4. Transparency and information for the data subject

4.1 The data subject whose data are collected must be informed at the time of collecting of the identity of the data controller, the purposes for which the data are to be processed and how the rights referred to in sections 5 and 6 of these directives may be applied, as well as any other information required to guarantee licit processing of the data. This obligation shall only be waived if the data subject has previously been informed of these circumstances.

4.2. When the data have not been obtained from the data subject, he must be informed of the particulars provided in the preceding paragraph within a reasonable period and, in all cases, prior to the data being disclosed to a third party.

5. Rights of access, correction and cancellation held by the data subject

The data subject whose data are processed may perform the following, by clear, expedite, free or affordable procedures:

5.1 Obtain confirmation from the data controller concerning the existence or inexistence of processing of the data concerned, as well as information on at least the purpose of such processing, the categories of data concerned and the receivers, or categories of receivers to whom such data are disclosed.



5.2. Obtaining information on the data subject to processing from the data controller, in an intelligible format, as well as all the information available on the origin of the data.

5.3. To require, when appropriate, correction or cancellation of the data that might be incomplete, inexact, inadequate or excessive, as provided in these directives.

5.4. To demand third party notification to those to whom data were provided on all correction or cancellation according to the preceding paragraph.

6. Other rights of the data subject

In addition to the rights referred to in the preceding paragraph, the data subject shall have the following:

6.1. Not to be subject to decisions with legal effects on him, or that significantly affect him, which are based solely on automated processing of data intended to evaluate specific aspects of his personality, such as performance at work, credit, reliability or conduct. However, it shall be possible to adopt those decisions when carried out within the framework of a legal relationship freely accepted by the data subject, in which he is allowed the possibility to make allegations concerning the result of the valuation.

6.2. To refuse the processing of his data, in cases not excluded by virtue of the law, due to concurrence of an exceptional, legitimate reason arising from his specific personal situation.

6.3. To refuse, on request and free of charge, the processing of personal data with regard to which the controller is to perform activities related to advertising and commercial prospecting.

6.4. To obtain assistance from the courts of law and the authorities referred to in section 9 of these directives in the event of considering that the processing of the data is being performed in breach of these.

6.5. To be compensated for any damage or injury suffered by his assets or rights as a consequence of data processing performed in breach of the terms set forth in these directives.



7. Security and confidentiality in processing

7.1. The necessary technical and organisational measures must be adopted to protect the data against adulteration, loss or accidental destruction, unauthorised access or fraudulent use.

7.2. Those that intervene in any phase of processing personal data are obliged to observe professional secrecy with regard to these. That obligation shall subsist even after their relation with the holder of the data file has concluded.

8. Limitations on international data transfers

8.1. As a general rule, international data transfers may only be performed to the territory of States whose legislation enshrines what is set forth in these directives.

8.2. However, the law may establish exceptional cases in which international data transfers to other States may take place, according to the circumstances that arise in each case. In any case, one must take the rights and interests of the data subject into account and, in particular, whether he has consented to the transfer concerned.

8.3. Apart from the cases mentioned in the preceding two paragraphs, international data transfers shall only be possible if authorisation is secured from the authority referred to in section 9, for which it shall be necessary for the exporter to provide sufficient guarantees to ensure that the importer shall fulfil the terms of these directives in all cases.

9. Controlling authorities

9.1. The guarantee of fulfilment of these directives must be subject to control by one or several data protection authorities. The authorities may have their own status, or be part of the Public Authorities or a pre-existing Public Body. They may also have the exclusive purpose of enforcing fulfilment of data protection laws, or perform that competence along with others attributed by their legislation.

The territorial organisation of the State may not lead to an obstacle for the guarantees arising from the existence of the data protection authorities being real and effective in relation to all the processing carried out, both by the public as well as the private sector.

9.2. The data protection authorities must act with full independence and impartiality and in the exercise of their duties may not be subject to orders by any public authority.



Mechanisms must be established to guarantee the independence and reliability of the persons placed in charge of managing such authorities.

9.3 The authorities must have at least the following powers;

- To hear claims brought before them by citizens, in particular as to the exercise of the rights referred to in section 5 of these directives;
- To perform the enquiries and investigations that are necessary for fulfilment of the directives, being able to access the data subject to process and gather all the information required for fulfilment of their control mission;
- To adopt the necessary measures to avoid persistent breach of the directives;
- To maintain a record of the processing carried out by the public and private sectors, which the data subjects may access, in order to be able to exercise the rights recognised in these directives. The request for registration shall be made using simplified forms, based on technical standards, respecting the principle of technological neutrality and using electronic techniques or means whenever possible;
- To authorise international data transfers to States whose laws do not include the terms provided in these directives when necessary;
- To promote the use of self-regulation mechanisms as a complementary personal data protection instrument that: (i) provide an added value to their content with regard to the terms provided in the laws, (ii) contain or is accompanied by elements that allow their level of efficiency to be measured with regard to fulfilment and the degree of personal data protection; and (iii) that enshrine effective measures in the event of breach thereof;
- To advise on the draft provisions that might affect the fundamental right to protection of a citizen's personal data;
- To inform citizens and public authorities of the content of the fundamental right to personal data protection;
- To co-operate with the data protection authorities in fulfilment of their powers and to generate the bilateral and multilateral co-operation mechanisms to aid each other and to provide due mutual aid when required.



10. Penalties

10.1. Breach of the provisions provided in these directives must be penalised pursuant to domestic laws. The capacity to impose the relevant penalties may be assigned to the data protection authority referred to in section 9, or to judicial bodies.

10.2 In all cases, the data protection authorities must have sufficient capacity to resort to the competent judicial channels to achieve adoption of the necessary measures to guarantee fulfilment of these directives and, in particular, imposition of the relevant penalties.

10.3. If the data protection authorities are directly competent for imposing sanctions, their resolutions must be liable to appeal before the Courts of Law.

Cartagena de Indias, Colombia, 4th May 2007