Publication date: 21/01/2004
Publication number: 003
Publication year: 16
Document date: 18/12/2003
Body: 01.2. Acts
Summary: Qualified Act 15/2003, of 18 December, of personal data protection

---

Qualified Act 15/2003, of 18 December, of personal data protection.

(*Translator's note*: A qualified law is a law which, to be passed, requires a higher majority than other laws).

Whereas the General Council (Parliament) in its session of 18 December 2003 approved the following:

Act 15/2003, of 18 December, qualified law of personal data protection.

Exposé of grounds

The purpose of this Act is to regulate the processing carried out by private persons and entities and by the Public Administration over data corresponding to individuals.

This regulation seeks to fulfil three fundamental objectives: first, to supply a sufficient and reasonable degree of protection for the right that everyone has to privacy, a fundamental right recognised by the Constitution in article 14; second, that this protection does not involve establishing excessive obligations which could hinder or make seriously difficult the financial, administrative or management activities of Andorran public or private entities; third, to bring Andorran legislation closer to the regulations of neighbouring countries in these matters. The regulation contained in this Act seeks to express a balance between these three principles.

Regulation of the processing of personal data is not unknown in our country. In fact, the Regulation on the public sector data bank, approved in 1976, already established a whole series of provisions for the processing of personal data, although limiting the field of action to the use of the data of persons administrated in the public sector.

Taking this precedent into account, the regulation established in this Act contains a specific provision relating to the processing of data by the Andorran

Administration and includes other questions considered fundamental in the regulation of personal data processing.

Thus, the first chapter of the Act regulates the territorial and material ambit, with identification of the matters which, for their specific nature, must be excluded from its field of application; the second chapter defines the fundamental principles applicable to any personal data processing; the third chapter, the specific requirements applicable to the processing of personal data by private entities; chapter four, the specific requirements for personal data processing by public entities; chapter five, infringements and sanctions arising from non-compliance with the Act; chapter six, the requirements applicable to international communication of personal data; chapter seven, the public authority in charge of overseeing compliance with the Act; and, finally, there are the provisions of a transitional, additional and final nature which facilitate compliance with the Act.

Chapter one. Purpose, ambit of the Act and exclusions

Article 1
Purpose

The purpose of this Act is to protect and guarantee, with regard to the processing and use of personal data, the fundamental rights of individuals, especially those relating to privacy.

Article 2
Ambit of application

This Act is applicable to data of a personal nature which are susceptible of being processed and to any subsequent use of these data.

Article 3
Definitions

For the purposed of this Act the following definitions are understood:

1. Personal data: all information relating or linked to identified or identifiable individuals.

2. Personal data processing: any operation applied to or carried out involving personal data, whether or not computerised.

3. Personal data file: structured and organised assembly of personal data, whatever may be its form or method of creation, storage, organization and access.

4. Processing manager: the individual or legal persona, whether of a public or private nature, with decision over personal data processing and the means used for this processing, and which oversees that the intended purposes of the processing correspond to those specified in the rule or decision to create the file.

5. Supplier of personal data services: individual or legal persona, of a public or private nature, which processes the data for the account of the processing manager, or accesses the personal data in order to supply a service in favour of or under the control of the processing manager, provided that the data accessed are not used for its own purposes, and are not made available outside the instructions received or for purposes other than the service to be supplied to the manager.

6. Interested party: individual to whom the personal data the subject of processing correspond.

7. Public registries: all the personal data files of which the processing manager is a public entity to which the interested parties are obliged to supply their data for the purpose of entries or other functions.

8. Accessible public registries: public registries to which any citizen or entity, whether public or private, can have access.

9. Communication of data: any assignment of personal data made by the processing manager in favour of a third person ultimate recipient of the data, provided that the data are used by the ultimate recipient for its own purposes, including any access that the ultimate recipient may have to the data under the control of the processing manager.

10. Ultimate recipient: third party, individual or legal persona, of a public or private nature, having access to data communication.

11. Sensitive data: data referring to political opinions, religious beliefs, membership of political or trade union organizations, health, sex life or ethnic origin of the interested parties.

12. Files of a private nature: personal data files the processing manager of which is an individual or legal persona of a private nature or a public authority company subject to private law.

13. Files of a public nature: personal data files the processing manager of which is the Public Administration.

14. International data communication: all data communication, or all access to data by a supplier of personal data services, when the ultimate recipients of the communication or the suppliers of services are resident abroad, or make use of means of processing personal data located abroad for the data communication or for the supply of the service.

15. Rules governing the creation of files of a public nature: decrees approved and published by the General Administration or, in the case of the communes (local councils), the provisions applicable in accordance with the Qualified Act of delimitation of the competences of the communes, destined to regulate the creation, modification or

deletion of files of a public nature, in accordance with the requirements established in articles 30 and 31 of this Act.

Article 4
Territorial ambit

This Act applies to the creation of files and personal data processing by processing managers resident in the Principality of Andorra, or constituted in accordance with the Laws of the Principality of Andorra.

This Act also applies to data processing carried out by processing managers not resident in the Principality or not constituted in accordance with the Laws of the Principality of Andorra, when they use means of processing located in the territory of the Principality.

Article 5
Matters excluded

The processing of personal data relating to the following matters falls outside the ambit of application of this Act:

State Security
Investigation and prevention of criminal infringements

Article 6
Personal files

Personal data processing is outside the ambit of this Act when the processing manager is an individual, and the data are destined to exclusively individual purposes, such as personal diaries or personal address books or contact details of interested parties related with the individual managing the processing.

Article 7
Data of individuals linked to their business, professional or commercial activity.

The data of individuals, linked to their business, professional or commercial activity, are outside the Act in the following circumstances:

a) Data of the personnel of legal personas or trading or professional establishments, when the information linked to the individual refers only to his belonging to the company or establishment, or to his professional capacity in the company or establishment itself.

b) Data of individuals belonging to professional groups, whenever the data refer only to the person's professional activity and his or her membership of a specific professional group.

c) Data of self-employed professionals or professional or commercial establishments, when the data refer only to their professional or trading activity.

Article 8
Supplementary application of the Act

This Act will apply, in an alternative sense, to everything not regulated in the regulations applicable to public registries and in the regulations applicable to banking secrecy. In the case of contradiction between this personal data Act and the specific regulations mentioned, the latter will prevail, but in no case can be understood repealed by this qualified Act of personal data protection.

Article 9
Professional secrecy

This Act will apply with an additional nature to the rules regulating professional secrecy, for activities and professions subject to this obligation, which governing rules may in no case be understood as repealed by this Act.

Chapter two. Principles applicable to the personal data processing

Section one. General principle

Article 10
Adaptation to the law

Personal data processing is only lawful when carried out in conformity with the provisions of this Act.

Section two. Quality of the data

Article 11
General requirements for all processing

Personal data processing may only be carried out by processing managers if they meet the following requirements:

a) That the processing is carried out for the purposes envisaged in the regulation or in the decision to create personal data files.

b) That the data subject to processing correspond to the real personal data of the interested parties, and that, for these purposes, measures are taken to update them or delete them.

c) That the data are preserved during the maximum time periods applicable in accordance with the current regulation and, in any case, during the maximum time period necessary for the purpose envisaged for their processing.

In accordance with the specific legislation and in view of the historic or scientific values, the procedure by which it is decided to maintain the integrity of certain data must be established by regulation.

Article 12
Confidentiality and security

The processing managers must establish the technical measures and organization necessary to guarantee the confidentiality and security of the personal data subject to processing.

If all or part of the processing is entrusted to the suppliers of personal data services, the processing manager is responsible to ensure that the suppliers have established sufficient technical measures and organization to guarantee the confidentiality and security of the data subject to the service. To this end, the processing managers must require from the personal data service suppliers that they establish the technical and organizational measures considered minimum by the processing manager, provided that these minimum measures correspond with those that the manager himself has established for the processing of data under his own control and of an analogous nature to those subject to the service.

Section three. Right to information

Article 13
Obtaining the data from the interested party

At the time of collection of the data, the interested party has the right to be informed by the processing manager of the following circumstances:

a) Identity of the processing manager.

b) Purpose of processing of data asked for.

c) Ultimate recipients or types of ultimate recipients of the data.

d) Rights of access to, rectification and deletion of his data and how to exercise these.

e) His right not to grant consent to the data processing, and the consequences of not granting it.

Article 14
Exceptions to the right to information

The processing managers are not obliged to give the information indicated in the preceding article when this is included in the rules for the creation of files of a public nature envisaged in article 30.

Article 15
Right of opposition

Any interested party has the right to oppose his data being the subject of processing by a processing manager, when the latter has not obtained the data directly from the interested party himself.

For these purposes, when an ultimate recipient of personal data is the subject of a communication of data, and within a maximum time of fifteen days counting from when the data were received, he must advise the interested parties whose data has been received of the following circumstances:

a) Identity of the new processing manager.

b) Identity of the individual or legal persona from whom the manager has received the data.

c) Purpose of processing the data obtained.

d) Ultimate recipients or types of ultimate recipients of the data.

e) Rights of access to, rectification and deletion of their data and how to exercise these.

Within a maximum period of one month from the time when the interested parties have been informed of the above circumstances, the latter may exercise their right of opposition, requesting the new processing manager to delete their data. If the right of opposition has not been exercised by the end of this period, it is understood that consent is given for the processing by the new manager.

Article 16
Exceptions to the right of opposition

Article 15 is not applicable when the communication of data takes place in any of the following circumstances:

a) When the communication of data is between entities of a public nature, and this communication is established in the rules for creation of files of a public nature envisaged in article 30.

b) When the communication of data is necessary for compliance with the purposes and functions of public registries.

c) When the communication of data takes place in compliance with a current rule, or in order to comply with a current rule.

d) When the communication of data is necessary for compliance with contractual obligations established between the interested party and the processing manager, or is necessary for compliance with, development and control of other legal relationships which may exist between the interested party and the processing manager.

e) When the communication is necessary to preserve the vital interest of the interested party.

f) When the communication is required by a judicial order.

Section four. Legitimisation for processing

Article 17
Consent

The processing of personal data may only be carried out by processing managers with the unequivocal consent of the interested parties.

Article 18
Exceptions to the consent

The consent of the interested parties for the data processing is not necessary if any of the following circumstances apply:

a) When the data processing corresponds to entities of a public nature, provided that the processing is done within the limits established in section a) of article 11.

b) When the data processing is necessary for compliance with the purposes and functions of public registries, pursuant to their regulations.

c) When the data processing is carried out in accordance with a current rule.

d) When the data subject to processing has been obtained from accessible public registries.

e) When the data processing is necessary for compliance with contractual obligations established between the interested party and the processing manager, or is necessary for compliance with, development and control of other legal relationships which may exist between the interested party and the processing manager.

f) When the processing is necessary to preserve the vital interest of the interested party.

g) When the processing is carried out exclusively for historical or scientific purposes, or for artistic or literary expression.

Article 19
Sensitive data

Sensitive data can only be the subject of processing or communication with the express consent of the interested party. The creation of files for the exclusive purpose of collecting or processing sensitive data relating to political opinions, religious beliefs, membership of political or trade union organizations, health, sex life or ethnic origin of individuals is prohibited.

Article 20
Exceptions to the express consent for sensitive data

The express consent of the interested party for the processing or communication of sensitive data is not necessary if any of the following circumstances apply:

a) When the processing or communication of sensitive data is done by or between entities of a public nature, being strictly necessary for compliance with their legitimate functions and purposes, and can be included in the rules of creation of files of a public nature envisaged in article 30.

b) When the processing or communication of sensitive data is necessary for compliance with the purposes and functions of public registries, pursuant to their regulations.

c) When it is necessary in order to preserve the vital interest of the person concerned.

d) When the data have been obtained from accessible public registries.

e) In relation to the processing of sensitive data relating to health, when the processing or communication is made by medical, health or social work professionals, and is necessary for diagnosis and medical treatment or for health or social care.

f) In relation to the processing of sensitive data relating to health, when the processing or communication is necessary for the epidemiological studies or for the prevention and treatment of epidemics.

Article 21
Files relating to criminal or administrative offences or sanctions

Files relating to criminal or administrative offences or sanctions may only be created by judicial or administrative public entities which, pursuant to a current rule, have the capacity of imposing administrative sanctions or resolving legal proceedings of a criminal nature.

Section five. Rights of the interested parties

Article 22
Right of access

Any interested party has the right to be informed by the processing manager of his data which are the subject of processing. The manager can only refuse this right of access on the grounds envisaged in this Act.

The manager, if it does not correspond to him to refuse access to the data, must inform the interested party within a maximum time of five working days counting from the time when the manager received the application from the interested party.

The manager must deliver the information by the means he considers most suitable, either through direct visualisation of the data, or by despatch in printed form, or in any other way that he deems fit.

In every case, any refusal of access to the data must be for a defined reason and will be capable of being appealed before the competent jurisdiction.

Article 23
Right of rectification

Any interested party has the right to ask the processing manager to correct the data subject to processing, if they are erroneous.

The manager can only refuse this right of rectification on the grounds envisaged in this Act.

For the exercise of the right of rectification, the manager may ask the interested party to supply the necessary documents to accredit the correctness and reality of the new data, and may reject the application if the interested party does not supply these documents or the reality of the new data is not accredited.

In every case, the processing manager must communicate to the interested party the refusal of the application, or the effective correcting of the data, within a period of one month, counting from when he received the application from the interested party if the application is accompanied by all the documents necessary to check the reality and correctness of the new data, or to count from when the manager receives all these documents.

In every case, any refusal of access to the data must be for a defined reason and will be capable of being appealed before the competent jurisdiction.

Article 24
Right of deletion

Every interested party has the right to require the processing manager to delete the data subject to processing.

The manager can refuse this right of deletion in the following cases:

a) When the preservation of the data is necessary for the processing manager, in accordance with a valid rule.

b) When the preservation is necessary for compliance with the lawful purposes of the file manager, in the maximum periods established in Article 11(c).

c) When the preservation is necessary in virtue of the legal relationship or contractual obligations existing between the interested party and the file manager, or in the case of possible legal or out of court claims or administrative obligations arising from these legal relationships or contractual obligations.

The file manager will have a maximum time of one month, counting from when he received the application from the interested party, to communicate the effective deletion of the data or the refusal of the application, if any of the circumstances indicated in the preceding paragraph apply.

In every case, on refusal of the application, for which there must be a defined reason, the interested party may appeal against the decision before the competent jurisdiction.

Article 25
Exercise of the rights of access rectification, deletion and opposition

The exercise of the rights set out in articles 15, 22, 23 and 24, cannot be subjected by the file manager to any formality, nor to payment by the interested party of the expenses which may correspond to it.

Article 26
Right to compensation

The sanctions envisaged in chapter five of this Act are understood without prejudice to the third party liability which may be incurred by the processing manager in the case of non-compliance with the Act.

Chapter three. Files of a private nature

Article 27
Obligation of registration

Individuals or legal personas of a private nature who are the data processing managers must register the files of personal data under their control in the public registry managed by the controlling authority indicated in chapter seven. The manager must register the file before creating it.

Article 28
Content of the registration

At the time of registration, the file manager must supply the following information to the controlling authority:

a) Name and address of the processing manager.

b) Structure of the file.

c) Purpose of the data processing.

d) Type of data subject to processing.

e) Sources from which the data will be obtained.

f) Period of preservation of the data.

g) Ultimate recipients or categories of ultimate recipients to whom it is envisaged to communicate the data.

h) International communications of data envisaged.

i) Generic description of the technical and organisational measures applied in processing the file, in accordance with article 12 of this Act.

Article 29
Updating the registration

Similarly, if after the first registration there are amendments of the information supplied to the controlling authority in accordance with article 28, the manager must inform the aforesaid controlling authority of these changes at the time when they occur, for the corresponding registry records.

Chapter four. Files of a public nature

Article 30
Rules of creation of files

The creation, modification or deletion of files of a public nature must be carried out by means of a rule of creation, which must be approved by the public entity managing its processing, and must be published in the Official State Gazette of the Principality of Andorra before the creation, modification or deletion of the file.

The approval of a rule of creation of a file of a public nature is not necessary for files of personal data under the control of entities of a public nature relating to public registries which have their own regulation, nor to those to which reference is made in matters excluded from the ambit of this Act, in accordance with article 5.

Article 31
Content of the rules of creation

The rules of creation and modification of files of a public nature must contain, at least, the following information:

a) Purpose of processing the file.

b) Sources from which the personal data will be obtained.

c) Type of data which the file will contain.

d) International communications of data which it is envisaged to effect.

e) Other entities of a public nature with which it is envisaged to exchange personal data for the purposes of file management.

f) Identification of the organs managing the file and the organs before which the rights of access, rectification, deletion and opposition may be exercised.

g) Generic description of the technical and organisational measures applied to the file processing, in accordance with article 12.

Article 32
Exceptions to the exercise of the rights of access, rectification, deletion and opposition

The managers of files of a public nature can refuse the exercise of the rights of access, rectification, deletion and opposition by the interested parties when they consider that this could endanger:

a) Public security.

b) Administrative actions destined to ensuring compliance with taxation obligations.

c) Prevention or prosecution of administrative offences.

d) Prevention or prosecution of criminal offences.

e) The public interest or that of the interested party himself.

Chapter five. Infringements and sanctions

Article 33
Infringements and sanctions for files of a private nature

Non-compliance with this Act by individuals or legal personas of a private nature is subject to administrative sanction. The first non-compliance by a file manager will be sanctioned with a fine of up to a maximum of €50,000, and subsequent non-

compliances by the same manager will be sanctioned with a fine of up to a maximum €100,000.

The amount of the sanction will be set by the controlling authority, taking into account the following criteria:

a) The specific circumstances of the infringement.

b) The seriousness of the non-compliance.

c) The number of people affected.

d) The damage caused to interested parties.

e) Repetitions.

Article 34
Infringements and sanctions for files of a public nature

The proceedings and sanctions to apply in the case of non-compliance with this Act by public entities are those established in the regulating provisions of the disciplinary regimes. For these purposes, the sanctioning capacity corresponds to the controlling authority established in chapter seven of this Act, without prejudice to the administrative appeals provided in the Administrative Regulations or the legal protection to which the interested parties are entitled.

Chapter six. International communication of data

Article 35
Requirements for the international communication of data

No international data communication may be effected unless the current regulations in the country of destination establish a level of personal data protection at least equivalent to that established in this Act.

Article 36
Countries with equivalent protection

It is understood that the following have a level of protection equivalent to this Act:

a) Member countries of the European Union.

b) Countries declared by the European Communities Commission as countries with protection equivalent.

c) Countries declared as such by the Andorran Data Protection Agency.

Article 37
Exceptions

The prohibition established in article 35 of this Act does not apply when the international communication:

a) Is made with the unequivocal consent of the interested party.

b) Is made in accordance with international conventions of which the Principality Andorra is a party.

c) Is made for the purposes of international legal assistance, or for the recognition, exercise or defence of a right in the context of legal proceedings.

d) Is made for medical prevention or diagnosis, health care, social prevention or diagnosis or for the vital interest of the interested party.

e) Is made for the purpose of bank remittances or transfers of money.

f) Is necessary for the establishment, execution, fulfilment or control of legal relationships or contractual obligations between the interested party and the file manager.

g) Is necessary to preserve the public interest.

h) Is concerned with data taken from public registries or is made in compliance with the functions and purposes of the public registries.

Chapter seven. Controlling authority

Article 38
Creation of the Andorran Data Protection Agency

The Andorran Data Protection Agency is formed as a public body with its own legal personality, independent of the Public Authorities and with full capacity to operate.

Article 39
Composition and financing of the Andorran Data Protection Agency

The Andorran Data Protection Agency will be composed of:

a) The head of the Data Protection Agency.

b) Two inspectors, who will be under the head of the Agency.

The head of the Data Protection Agency and the inspectors will be appointed by the General Council, by a special majority of two thirds parts in the first vote; and if in

the first vote the majority required above should not be reached, in a second vote the candidates will be elected who obtain the favourable vote of the absolute majority.

The appointment is for a term of four years and the appointment may be renewed at the end of each period.

The Andorran Data Protection Agency will be financed exclusively from the budget appropriations established each year for its functioning in the general budget of the General Council.

Article 40
Powers of the Andorran Data Protection Agency

The powers of the Andorran Data Protection Agency are:

a) To oversee compliance with this Act.

b) Management of the Public Registry for the Registration of Personal Data Files.

c) Annual publication of the list of countries with equivalent protection, pursuant to article 36 of this Act.

d) Exercise of the power of inspection and sanction for the infringements typified in chapter five of this Act.

e) Proposing improvements in the personal data protection regulations as it considers appropriate.

f) Preparation of an annual report on its activity and the results emerging from it. The annual report will be public.

Article 41
Power of inspection

The Andorran Data Protection Agency has the competence of inspection. File managers are obliged to supply the inspectors of the Andorran Data Protection Agency with all the information requested from them, and also to arrange access to their premises and computer systems and other types of resources used in data processing when this is requested in the exercise of this power of control.

In every case, the inspecting activity can only be carried out with the corresponding authorisation from the head of the Andorran Data Protection Agency, which authorisation must contain the obligatory information established by regulation. File managers will have the right to require the inspectors to show this authorisation and can lawfully refuse the inspection if the authorisation is not exhibited to them, or if it does not contain the obligatory information established by regulation.

The inspection can be initiated by the Andorran Data Protection Agency on its own initiative or be applied for by any interested party who considers that their rights have been affected or that a processing manager has failed to comply with his obligations as established in this Act.

Article 42
Power of sanction

The Andorran Data Protection Agency has the capacity to impose the sanctions envisaged in chapter five of this Act, in accordance with the proceedings established in the Administrative Regulations.

In every case, it corresponds to the inspectors of the Andorran Data Protection Agency to send the proposals for sanctions arising from their inspections to the head of the Andorran Data Protection Agency, who shall resolve these proposals by deciding whether or not to open the corresponding sanction proceedings.

Article 43
Public Registry for Registration of Personal Data Files

The Public Registry for Registration of Personal Data Files is set up, relating to the registrations of files established in articles 27 to 29 of this Act, with the content and characteristics established by regulation.

The Andorran Data Protection Agency manages the Public Registry for Registration of Personal Data Files in conformity with the following criteria:

a) The inspectors of the Andorran Data Protection Agency are responsible to: Review the applications for registration of files and for the updating of the registrations of files addressed to the Agency, and verify that they meet the requirements established in articles 28 and 29 of this Act and in the corresponding regulation.

Propose to the head of the Agency the acceptance or not of the applications received, and in the case of proposing their refusal, to detail the grounds.

b) The head of the Andorran Data Protection Agency is responsible to resolve the proposals of acceptance or rejection of registration and inform the corresponding file managers, with a detailed indication of the reasons for his decision.

The Public Registry for Registration of Personal Data Files is of general and free public access, and the possibility of access to the information contained in this Public Registry by telematic means must be foreseen.

Article 44
Action in conformity with the Administrative Regulations

The Andorran Data Protection Agency will at all times adapt its action to the Administrative Regulations, and its resolutions will be challengeable as established in that body of law.

Additional, transitional, repealing and final provisions

Additional provision.
Development of the regulation

The Government of Andorra is charged to deliver, within one year of its coming into force, the necessary regulations for the development of this qualified Act, especially those referring to the Andorran Data Protection Agency.

First transitional provision.
Approval and publication of the rules for the creation of files of a public nature

The public entities have a period of one year from the coming into force of this Act to approve and publish in the Official State Gazette of the Principality of Andorra the decrees envisaged in article 30 affecting files of a public nature existing before the coming into force of this Act.

Second transitional provision.
Registration of files

The individuals and legal personas of a private nature who are obliged to register the personal data files under their control have a period of six months in which to register the files of a private nature existing previous to the coming into force of this Act. The period of six months will start on the date of publication in the Official State Gazette of the Principality Andorra of the regulation of development envisaged in the third transitional provision.

Third transitional provision.
Regulation regulating the Public Registry for Registration of Personal Data Files

Within a period of six months from the coming into force of this Act, the ministry in charge of Trade must approve and publish in the Official State Gazette of the Principality of Andorra the regulation of development which regulates the Public Registry for Registration of Personal Data Files, including the standard forms for use by the files managers in proceeding to registration, and the means by which they can access the information included in this Public Registry.

Fourth transitional provision.

Control of compliance with the Act until the Andorran Data Protection Agency starts up its activity

The appointment of the head and inspectors of the Data Protection Agency and approval of its means and financing and other resources necessary for the functioning of this Agency must take place within six months from the approval of the regulation relating to the Andorran Data Protection Agency, as established in the additional provision. Until the Agency comes into operation, the powers established in articles 40 to 43 of this Act will be exercised by the following controlling authorities:

a) Files of a private nature: the ministry in charge of Trade

b) Files of a public nature:

The ministry of the Presidency, for files of a public nature the managers of which are the General Administration or para-public or public law entities.

The communes, for files of a public nature the managers of which are the communes themselves.

The Higher Council of Justice, for files of a public nature the managers of which are public entities integrated into the Administration of Justice.

Repealing provision.
Regulation of the public sector data bank and other rules

All provisions which oppose this qualified Act of personal data are repealed, especially the 1976 Regulation of the public sector data bank.

Final provision.
Entry into force of this Act

This Act will come into force fifteen days after its publication in the Official State Gazette of the Principality of Andorra.

Casa de la Vall, 18 December 2003
Francesc Areny Casal
Speaker of the General Council

We the co-princes approve it and promulgate it and order its publication in the Official State Gazette of the Principality of Andorra.

Jacques Chirac
President of the French Republic
Co-prince of Andorra

Joan Enric Vives Sicília
Bishop of Urgell
Co-prince of Andorra