Decree
approving the Regulations
of the Andorran Data Protection Agency

Preamble

With the approval of Qualified Law 15/2003 of 18th December on the protection of personal data (LQPD), the Principality of Andorra has fulfilled the objective of regulating the processing carried out by both persons and private entitles as well as the Andorran Public Administration with regard to data corresponding to physical persons, while guaranteeing the fundamental rights of persons, especially those concerning privacy, related to the processing and use of personal data.

The Andorran Data Protection Agency was created by the same Law for the purpose of making sure that respect for the fundamental rights of physical persons is maintained in all matters involving operations that are carried out using automatic or manual processes for personal data, with special protection given to the right to privacy.

The Decree approving the Regulations of the Public Register for the Inscription of Personal Data Files of 1st July 2004, with the correction of errata of 7th July 2004, annex 1 of which was amended by the Decree of 1 October 2008, and the Decree of the Regulations of the Andorran Data Protection Agency of 1st July 2004, which was amended by Decree of 21st July 2004, developed chapters three, four and seven of Qualified Law 15/2003 of 18th December on the protection of personal data (LQPD).

The experience of more than five years that the Andorran Data Protection Agency has had in the application of the Regulations has provided it with knowledge on some aspects that can be improved, and these are specified in the application of Qualified Law 15/2003 of 18th December on the protection of personal data (LQPD).

In developing Qualified Law 15/2003 of 18th December on the protection of personal data (LQPD), there also arises the need to take into consideration the General Council's ratification at its session of 18th October 2007 of the Convention for the protection of individuals with regard to the automatic processing of personal data done at Strasbourg on 28th January 1981, and the additional Protocol of the Convention for the protection of persons with regard to the automatic processing of personal data related to supervisory authorities and transborder data flows, done at Strasbourg on 8th November 2001, both of which have been in force since 1st September 2008.

Accordingly, the scope of the reform is considered to be of sufficient importance to justify the repeal of the Decree approving the Regulations of the Andorran Data Protection Agency of 1st July 2004, the new draft of which is included in the Regulations being approved, and whose purpose is to reinforce the protection of personal data, bearing in mind that transborder flows of personal data are necessary for the development of international trade; considering the compromises acquired by the Andorran State for the main purpose of developing the provisions envisaged in the Convention and the additional Protocol; Taking into consideration European Parliament and Council Directive 95/46/EC of 24th October 1995 concerning the protection of physical persons with regard to the processing of personal data and the free circulation of these data; and finally, overseeing improvements in the transparency and security of the processing, and also for the consolidation of an adequate and sufficient level of protection of personal data with regard to the level of requirement established by the European Community.

This Decree has been passed at the proposal of the Head of Government, at the session of the Andorran Government held on 9th June 2010:

Single article
The Regulations of the Andorran Data Protection Agency are hereby approved

Regulations of the Andorran Data Protection Agency

Chapter one. General provisions for the protection of individuals in the processing of personal data

Article 1
Purpose

The purpose of these Regulations is to develop Qualified Law 15/2003 of 18th December on the protection of personal data (LQPD), in particular chapters One, Purpose, scope of the Law and exclusions; Two, Principles applicable to the processing of personal data; Three, Private files; Four, Public files; Six, International communication of data; and Seven, Supervisory authority; bearing in mind the compromises acquired by the Andorran state in applying the Convention for the protection of individual with regard to the automatic processing of personal data, done in Strasbourg on 28th January 1981; and the additional Protocol of the Convention for the protection of individuals with regard to the automatic processing of personal data concerning supervisory authorities and transborder data flows, done at Strasbourg on 8th November 2001.

Article 2
Area of application

These Regulations shall apply to personal data that are susceptible to being processed, either manually or automatically, and to any subsequent use of these personal data in the public and private sectors.

Article 3
Areas excluded

The following are excluded from the scope of the Regulations:

1. Personal data related to the security of the state and to the investigation and prevention of criminal offences, which are regulated by a Law of a criminal nature and which lie within the framework of criminal proceedings.

2. The data of physical persons related to their business, professional or commercial activity, in the following circumstances:

   a) The personal data of legal entities or commercial or professional establishments, when the information related to physical persons refers solely to their belonging to the company or the establishment, or to their professional status within the company or establishment;

   b) The data of physical persons who belong to professional collectives, provided that the data refer solely to the professional activities of the persons or to their belonging to a certain professional collective;

   c) The data of autonomous professionals or professional or commercial establishments, when the data refers solely to their professional or commercial activity.

3. The processing of data carried out by a physical person in the course of a purely personal or household activity, such as correspondence and the management of a list of addresses.

Article 4
Territorial scope

1. These Regulations shall apply to the creation of files and any processing of personal data carried out by data controllers who are resident in the Principality of Andorra, or who are established in accordance with the Laws of the Principality of Andorra.

   When the preceding circumstance concerning the data controller does not exist, but where a service provider of personal data resident in the Principality of Andorra does exist, the precepts contained in these Regulations must also be applied.

Likewise, these Regulations shall be applicable to data controllers who are not resident in the Principality of Andorra when they depend on Andorran legislation under the rules of public international law; and they are also applicable to the processing of data carried out by data controllers who are not resident in the Principality or not established in accordance with the laws of the Principality of Andorra when they use processing means, whether automatic or not, that are situated on Andorran territory.

2. Data controllers who are not resident in the Principality of Andorra and who depend on Andorran legislation under the rules of public international law, and data controllers who are not resident in the Principality of Andorra or who are not established according to the laws of the Principality, and who use processing means, whether automatic or not, located on Andorran territory must designate a representative established in the Principality of Andorra to the Andorran Data Protection Agency, without prejudice to any actions that may be taken against the data controllers themselves.

3. For the purposes of this article, residence or establishment, independent of its legal form, shall be understood as any stable installation that allows the effective and real exercise of an activity.

Article 5
Definitions

In order to regulate the protection of personal data in the Principality of Andorra, the following definitions shall be used:

1. Personal data: all numeric, alphabetic, graphic, photographic, acoustic information or information of any other type that is related to a identified or identifiable physical person ("data subject"); identifiable shall be understood to mean any person who has an identity that can be determined, directly or indirectly, in particular through an identification number or one or several specific elements, characteristics of his physical, physiological, psychical, economic, cultural or social identity.

2. Consent: any free, specific, clear, certain and informed declaration of will, through which the person concerned consents to the processing of personal data that affect him.

3. Processing of personal data ("processing"): any operation or series of operations carried out using automatic or non-automatic procedures, and applied to personal data, such as the collection, recording, organization, conservation, elaboration or modification, extraction, consultation, use, communication by transmission, dissemination or any other form that allows access, comparison or the interconnection, blocking, elimination or destruction.

4. Personal data filing system (“file”): any structured and organized set of personal data, whether centralized or not, irrespective of its form or method of creation, storage, organization or access.

5. Automatic processing: operations that are carried out, either wholly or partially, with the help of automatic procedures, such as data storage; the application of logical and/or arithmetical operations to these data; and the modification, elimination, extraction or dissemination of the data.

6. Private files: personal data files, the controller of which is a physical person or a private legal entity or a public company subject to private law.

7. Public files: personal data files, where the controller is the Public administration.

8. Anonymous data: data which can not be associated with an identified or identifiable person, considering the series of means that the data controller or any other person can reasonably use to identify this person.

9. Data controller: the physical person or legal entity, service or any other body that is competent to decide on the processing of personal data and the means that are to be used for such processing, and which makes sure that the ends that are sought through the processing correspond to those stated in the rule or in the decision that was used to create the file.

10. Provider of services of personal data: the physical person or legal entity of a public or private nature, or public authority or service or any other body which, alone or together with others, processes personal data on behalf of the data controller, or which accesses the personal data in order to provide a service in favour of, and under the control of the data controller, provided that it does not use the data to which it has access for its own ends, or it does not use them for purposes that go beyond the instructions received, or for ends that are different to the service that has to be provided in favour of the data controller.

11. Data subject: the physical person to whom the personal data being processed belong or concern.

12. Third party: a physical person or legal entity, public authority, service or any other body other than the concerned party, the data controller or his representative and the service provider.

13. Public registers: all personal data files whose controller is a public entity, to whom the persons concerned are obliged to provide their data for inscription or other purposes.

14. Accessible public registers: public registers that can be accessed by any citizen or by any public or private entity.

15. Public interest: a definite and certain concept understood as a general, important and primordial advantage, which justifies the reason for intervention by the State and which is based on legitimacy, always within the framework of objectivity and the constitutional principles of legality, hierarchy, the openness of legal rules, non-retroactivity of the restrictive provisions of individual rights or those which involve an unfavourable effect or establish an unfavourable sanction, legal certainty, liability of public powers and prohibition of any arbitrariness.

16. Vital interest: an interest that is essential for the life of the data subject.

17. Recipient: a third party, which can be either a physical person or a legal entity, service or any other body that receives a data communication

18. Granting or communication of data: any granting or communication of personal data that the controller carries out in favour of a third party recipient provided that the data are used by the recipient for the fulfilment of purposes that are directly related to the legitimate functions of the assignor and the grantee.

19. Sensitive data: data referring to political opinions, religious beliefs, membership of political or trade union organizations, the health, sexual life or ethnic origin of the persons concerned.

20. Personal data related to health: any information related to the past, present and future physical or mental health of a person; it may concern a healthy, ill or deceased person; among other aspects, data related to the health of persons include those concerning their percentage of disability or their genetic information as well as those related to the consumption of alcohol, toxic drugs and psychotropic substances.

21. International communication of data: any communication of data or any access to the data by a service provider of personal data, when the recipients of the communication or the service providers are resident abroad, or when they use means for processing personal data that are located abroad for the communication of the data or for the provision of the service.

22. Rules for the creation, modification or elimination of public files: decisions of the organs of the public Administration defined by the Code of the Administration, which are subject to the provisions of the Qualified Law on the protection of personal data, and to the texts that develop this Law; which are intended to regulate the creation, modification or the elimination of public files in accordance with the requirements established under Qualified Law 15/2003 of 18th December on the protection of personal data (LQPD).

Chapter two. Principles applicable to the processing of personal data

Article 6
Principles concerning the quality of the data

In order to be gathered and processed, the personal data must compulsorily and in all cases:

1. be obtained and processed in a trustworthy and legal manner;

2. be collected for specific, explicit and legitimate purposes and not be subsequently processed in a manner that is incompatible with these ends;

3. be adequate, pertinent and not excessive in relation to the purposes for which they are gathered and for which they are subsequently processed;

4. be exact and updated when necessary; it is necessary to take all reasonable measures to ensure that any data that are inaccurate or incomplete in terms of the purposes for which they have been gathered or for which they have been subsequently processed, are deleted or rectified;

5. be conserved in a manner that allows the identification of the persons concerned during a period that is not greater than that necessary for which they have been gathered or for which they have been subsequently processed.

The responsibility for the fulfilment of the preceding obligations lies with the data controller, whose name or trade name must be clearly indicated when the data are being collected.

Article 7
Principles concerning the legitimation of the processing of data

1. The processing of personal data may only be carried out with the express consent of the data subject.

   If any doubts arise in relation to proof of the existence of the consent of the data subject, the responsibility for the proof shall lie with the data controller.

   The data subject may revoke his consent by making use of his rights, which are included in Chapter Three of these Regulations.

2. The provision of section 1 shall not apply when:

   a) the processing of data corresponds to entitles of a public nature, provided that it is done for the purposes envisaged in the regulations or in the decision to create the personal data filing system;

   b) the processing of data is necessary for the fulfilment of the purposes and functions of the public registers in accordance with their regulations;

c) the processing of the data is done in accordance with current regulations;

d) the data to be processed is obtained from accessible public registers;

e) it is necessary for the fulfilment of contractual obligations established between the data subject and the data controller, or else it is necessary for the fulfilment, development and control of other legal relations that may arise between the data subject and the data controller;

f) it is necessary to safeguard the vital interest of the data subject;

g) it is done exclusively for historical or scientific purposes or for the purpose of artistic or literary expression,

Both the exceptions to the consent of the data subject and those concerning the conditions legitimizing the processing of personal data must always be understood and interpreted in a restrictive manner.

Article 8
Special processing categories

1. Sensitive data may only be used for processing or communication with the express consent of the data subject.

   The creation of files for the exclusive purpose of collecting or processing sensitive data concerning political opinions, religious or philosophical beliefs, membership of political or trade union organizations, health, sexual life or racial or ethnic origin of the persons is not allowed.

   In the event of doubt, proof of the existence of the data subject's consent shall lie with the data controller.

2. The consent of the data subject for the processing or communication of sensitive data shall not be necessary when:

   a) the processing or the communication of sensitive data is done by, or between public entities, when it is strictly necessary for the fulfilment of their legitimate functions and purposes, and may be included in the regulations for the creation of public files envisaged under Qualified Law 15/2003 of 18th December on the protection of personal data (LQPD);

   b) the processing or the communication of sensitive data is necessary for the fulfilment of the purposes and functions of public registers, according to the regulations that determine them and regulate their functioning;

   c) it involves preserving the vital interest of the person affected;

d) the data has been obtained from public registers that are accessible in accordance with their regulations;

e) the processing or the communication of sensitive data related to health is done by medical or health professionals or social workers who are obliged to respect professional secrecy and to ensure the confidentiality of all the nominative and personal information received while exercising their professional praxis, and which is necessary for medical diagnosis and treatment, or for health or social assistance;

f) the processing or the communication of sensitive data related to health is necessary to carry out epidemiological studies or is needed to prevent or treat epidemics, with sensitive personal data being made anonymous prior to the communication;

g) when the processing or the communication of sensitive data carried out by or between public entities is strictly necessary for the fulfilment of their legitimate functions and ends, and can be included in the rules for the creation of public files envisaged by the Law.

Article 9
Access to data by service providers

Any access that is necessary for the provision of a service for the data controller's account shall not be treated as a data communication.

The provision of personal data services must be regulated in a contract, which should be drawn up in written form and which should allow the agreement and content to be accredited, and it should be expressly established that the service provider must only process the data in accordance with the instructions of the data controller, and that he may not apply or use them for a purpose that is different to that which appears in the contract agreed to, or communicate them to other persons, not even for the purpose of conserving them.

The contract also stipulates that the personal data as well as any support or document in which any of the personal data being processed is recorded must be destroyed or returned to the data controller once the contractual service has been completed.

The service provider shall apply any technical and organizational measures that may be necessary to protect the personal data against accidental or illicit destruction, accidental loss and against any unauthorized alteration, dissemination and access, in particular when the processing includes the transmission of data within a network, as well as against any other illicit processing of personal data.

If the service provider should use the data for a purpose that is different to that which has been agreed, or communicate them or use them in breach of the stipulations of the contract, he shall be treated as a data controller and shall be personally responsible for any infractions that he has committed.

Chapter three. Rights of the data subject

Article 10
Right of information

1. At the moment the data are collected, the data subject shall always be informed by the data controller or his representative in a clear, express, accurate and unequivocal manner:

   a) of the identity of the data controller and, if appropriate, of his representative;

   b) of the purpose of the processing to which the requested data will be subject;

   c) of the recipients, or the types of recipients, of the data;

   d) of the obligation or option to reply to the questions that are put to him and of the right not to consent to the processing of the data and the consequences of not granting such consent;

   e) of the existence of rights of access, rectification, opposition and elimination of his data, and how he can exercise them.

2. The consent of the data subject must be clearly notified in such a way that he is unambiguously aware of, and understands, the purpose and the uses for which the data being collected will be used, and especially, the purpose for the gathering of his personal data and the uses made thereof.

   If questionnaires or any other printed forms are used to gather the personal data, they must state clearly, legibly and in detail the information described in the previous epigraphs; as well as the consent of the data subject.

3. It is the obligation of the data controller to conserve the support containing and showing that the obligation to inform has been fulfilled. He may also use computer or telematic means to satisfy this objective. In particular, he may scan the documentation in paper form, provided that this shows that no alteration of the original supports has occurred during the automation.

4. In the event of any doubts arising with regard to proof of the existence of the data subject's consent, responsibility shall remain with the data controller.

Article 11
Right of access

All data subjects shall have the right to be intelligibly informed by the data controller of the existence or non-existence of data processing affecting them; and they have the right to receive information, at least with regard to the

purpose of the processing(s), the data categories to which they refer and the recipients or type of recipients to whom these data are communicated. Likewise, they shall have the right to receive a communication, also in an intelligible manner, concerning the data being processed, and to be made aware of all the information available as to the origin of the data; and they shall also have the right to know the logic that has been used in the automated processing of the data referring to the data subject, at least in the cases of the automatic decisions envisaged under article 14 of these Regulations.

1. The data controller shall inform the data subject within a maximum period of five working days counting from the moment that he receives the written request signed by the data subject.

2. The data controller shall provide information using the means that he considers to be most appropriate, by direct visualization of the data, or by sending it in printed format, or by any other way that he considers convenient, but in such a way however, that the information is legible and intelligible.

3. The data controller may only deny the right of access in the cases envisaged under Qualified Law 15/2003 of 18th December on the protection of personal data (LQPD).

4. The data controller must expressly notify the data subject of any refusal to access the data, within a maximum period of five working days counting from the moment that the written request signed by the data subject is received, and this communication must be in writing and must be justified.

5. Refusal of access to data or the faulty communication thereof may be appealed before the competent jurisdiction.

Article 12
Right of rectification

All data subjects shall have the right to ask the data controller to correct any of their data that is being processed, if such data are erroneous.

1. The data controller may only deny this right of rectification in the cases envisaged under the Qualified Law on the protection of personal data.

2. For the exercise of the right of rectification, the data controller may ask the data subject to provide the documents that are necessary to accredit the correction and the reality of the new data, and he may refuse the request if these documents are not provided by the data subject or his representative, or if they do not accredit the reality of the new data.

3. In any case, the data controller must inform the data subject of the refusal of the request or the effective correction of the data within a maximum period of one month, counting from the moment that he received the request from the data subject, if the request has already been accompanied by all the documents necessary to check the reality and the correction of the new data, or counting from the moment that the data controller received all of these documents.

4. The refusal of the request must be made in writing and it must be justified; and it may be appealed before the competent jurisdiction.

5. If the data that are subject to rectification have been communicated previously, the data controller shall have the obligation to notify the rectification to the recipient to whom the notification has been given, and if the processing is maintained, the latter must also carry out the rectification.

Article 13
Right of opposition

All data subjects shall have the right to object to their data being processed by a data controller, when this data controller has not obtained the data directly from the data subject.

When the recipient of personal data is the object of a data communication from a data controller, he must inform the data subject of the following circumstances within a maximum period of fifteen working days counting from the moment that he received the data:

a) the identity of the new data controller, or if appropriate, that of his representative;

b) the identity of the physical person or legal entity from which the new data controller has received the data;

c) the reason why the data obtained is being processed;

d) the recipients or type of recipients of the data;

e) rights of access, rectification and elimination of his data and how he can exercise them.

This person may exercise his right of opposition within a maximum period of one month counting from the moment that the data subject has been informed of the previous circumstances, by asking the new data controller to eliminate his data. If he has not exercised his right of opposition by the end of this period, it shall be understood that he consents to the processing by the new data controller.

The right of opposition may not be exercised when the communication of data:

a) is done between public entitles, and this communication is established in the rules for the creation of public files and is in keeping with the principles regarding the quality of the data;

b) it is necessary for the fulfilment of the purposes and functions of public registers that are expressly regulated;

c) it is done in fulfilment of a current regulation, or for the fulfilment of a current regulation;

d) it is necessary for the fulfilment of contractual obligations established between the data subject and the data controller, or it is necessary for the fulfilment, development and control of other legal relationships that may exist between the data subject and the data controller;

e) it is necessary to preserve the vital interest of the data subject;

f) it is required for a court order.

The refusal of the right of opposition must be made in writing, and it must be justified; and it may be appealed before the competent jurisdiction.

Article 14
Right of elimination

All data subjects shall have the right to ask the data controller to eliminate any data of theirs that is being processed.

1. The data controller may refuse this right of elimination in the following cases:

   a) when the conservation of the data is necessary for the data controller in accordance with current regulations;

   b) when the conservation is necessary for the fulfilment of the legitimate ends of the data controller, within the maximum terms that are applicable in accordance with current regulations, and in any case, during the maximum term that is necessary for the purpose envisaged for the processing;

   c) when the conservation is necessary by virtue of the legal relationships or the contractual obligations that exist between the data subject and the data controller, or in the case of possible judicial or extra-judicial claims or administrative obligations that derive from these legal relationships or contractual obligations.

2. The controller of the file shall have a maximum period of one month, counting from the moment that he receives the request from the data subject, to communicate the effective elimination of the data or the refusal of his request, if any of the circumstances indicated in the previous paragraph are present.

3. This decision results in the blocking of the personal data, which must only be kept for the use of the public administrations and courts for the purpose of dealing with any possible liabilities related to the processing, during the period of limitation for the data. They will be erased once the term has expired.

4. In any case, if the request, which must be made in writing and justified, is refused, the data subject may lodge an appeal against the aforementioned decision before the competent jurisdiction.

5. If the data shall have the obligation to notify the elimination to the recipient to whom they have been communicated, and if the processing is maintained, the latter must also carry out the elimination.

Article 15
Automated individual decisions

1. All persons shall have the right not to be subject to a decision which produces legal effects for them or which affects them significantly and which are based solely on automatic processing of data intended to evaluate certain aspects of their personality.

2. A person may be subject to one of the decisions established in section 1 when this decision:

   a) has been adopted within the framework of the conclusion or performance of a contract, provided that the petition for the conclusion or performance of the contract presented by the interested party has been satisfied or that their are adequate measures to safeguard its legitimate interest, as well as the possibility to defend its point of view; or

   b) is authorized by a Law that establishes measures to guarantee the legitimate interest of the person concerned.

Article 16
Exercise of the rights of access, rectification, opposition and elimination

The controller of the file may not subject the exercise of the rights of access, rectification, opposition and elimination to any formality or any payment by the data subject.

These rights shall be exercised by means of a written petition from the data subject.

The rights of access, rectification, opposition and elimination are personal rights and shall be exercised by the interested party himself or by his representative.

The rights of access, rectification, opposition and elimination are independent rights in such a way that the exercise of one is not a prior requisite for the exercise of another.

Chapter four. Confidentiality and security

Article 17
Confidentiality

The data controller must establish the technical and organizational measures that are necessary to guarantee the confidentiality of the personal data being processed and to avoid unauthorized dissemination or access to them.

Article 18
Security

1. The data controller must establish the technical and organizational measures that are necessary to protect the personal data against accidental or illicit destruction, accidental loss, alteration, unauthorized dissemination or access, especially when the processing involves the transmission of data over a network as well as against any other illegal form of processing. These measures must guarantee an adequate level of security according to the processing risks and the nature of the data to be protected.

2. If all or part of the processing is entrusted to service providers of personal data, it shall be the responsibility of the data controller to ensure that the providers have established sufficient technical and organizational measures to guarantee the confidentiality and the security of the data that is related to the service. To this end, the data controllers must require service providers of personal to establish the technical and organizational measures that the data controller considers to be minimum, provided that these minimum measures correspond to those that the data controller himself has established for his own data processing and are of a similar nature to those covered by the service.

Chapter five. Personal data files

Article 19
Personal data files

Before creating the file, the data controllers must register it in the Public Register for the Inscription of Personal data files in accordance with regulations.

Article 20
Public files

The creation, modification or elimination of the public file must be done in accordance with the rule published by the Public Administration and in accordance with the requirements established under Qualified Law 15/2003 of 18th December on the protection of personal data (LQPD).

Chapter six. International communication of data

Article 21
Requirements for the international communication of data and exceptions

1. International communications of data cannot be made when the country of destination has not established, in its current regulations, a level of protection for personal data that is at least equivalent to that established under Qualified Law 15/2003 of 18th December on the protection of personal data (LQPD).

2. The international communication of data to a country that does not guarantee an equivalent level of protection according to Qualified Law 15/2003 of 18th December on the protection of personal data (LQPD), can only be carried out if:

   a) it is done with the unambiguous consent of the person concerned;

   b) it is done in accordance with international conventions which the Principality of Andorra forms part of;

   c) it is done for the purpose of international legal assistance or for the recognition, exercise or defence of a right within the framework of a judicial process;

   d) it is done for the purposes of medical prevention or diagnosis, health assistance, social prevention or diagnosis or in the vital interest of the data subject.

   e) it is done because of bank remittances or transfers within the framework of a legal relationship that involves the person concerned;

   f) it is done with data from public registers or it is done in fulfilment of the functions and purposes of public registers, which by virtue of legal provisions, are conceived to provide information to the public and which are open to consultation by the public in general, or by any person who shows a legitimate interest in them, provided that the conditions established by the regulations for the consultation are fulfilled in each particular case; in this case, the transfer must not affect the totality of the data or the data categories that the aforementioned register contains; when the purpose of a register is to be consulted by persons who have an legitimate interest in it, this transfer should only be done at the request of these persons or else when they are the recipients thereof; this exception must never be used to legitimize mass transfers of data for commercial purposes contained in public registers, or for the meticulous research of data that is accessible to the public in order to obtain the profile of certain persons;

   g) it necessary either for the performance of a contract between the data subject and the data controller (or for the implementation of pre-contractual measures taken at the request of the data subject), or for the conclusion or the performance of a contract concluded, or to be concluded, in the interest of the data subject, between the data controller and a third party;

h) it is necessary to preserve the public interest.

All the exceptions outlined in this article should be interpreted in a strict and restrictive manner, so that their application does not cause any infringement of the rights of the person and the right to privacy in particular.

Chapter seven. The Andorran Data Protection Agency

Article 22
The Andorran Data Protection Agency

1. The Andorran Data Protection Agency, created by Qualified Law 15/2003 of 18th December on the protection of personal data (LQPD), is an institution of public law, whose activity is in keeping with the system of public law.

2. The Andorran Data Protection Agency shall be an independent authority and shall act with objectivity and be fully independent of the Andorran public administrations while exercising its functions.

3. The Andorran Data Protection Agency shall have its own legal personality and full operational capacities.

Article 23
Area of action

1. The Andorran Data Protection Agency shall exercise its supervisory authority over the processing of personal data, and over any subsequent use of these data that is carried out in the Principality of Andorra by the entities that make up the public administration, and any persons and private entitles that, pursuant to article 4 of Qualified Law 15/2003 of 18th December on the protection of personal data (LQPD), are controllers and have their residence in the Principality of Andorra or which have been established in accordance with the Laws of the Principality of Andorra.

2. The Agency shall be competent to verify the correct fulfilment of Qualified Law 15/2003 of 18th December on the protection of personal data (LQPD) by service providers of personal data which have their residence in Principality of Andorra or which have been established in accordance with the Laws of the Principality of Andorra, and regardless of the residence or the nationality of the data controllers for whom they provide their services.

3. Likewise, the Andorran Data Protection Agency shall exercise its supervisory authority over the processing of data carried out by data controllers who are not resident in the Principality of Andorra or who have not been established in accordance with the Laws of the Principality of Andorra but who use means for the processing of personal data that are located in the Principality of Andorra.

4. The Agency shall also be competent to collaborate with other supervisory authorities and entities on matters related to the personal data of other countries.

Chapter eight. Competencies and functions

Article 24
Competencies of the Agency

Within its area of action the Andorran Data Protection Agency shall be competent to oversee the fulfilment of Qualified Law 15/2003 of 18th December on the protection of personal data (LQPD), propose improvements to the regulations for the protection of personal data, draft contingent optional and advisory reports prior to processing, powers of information, consultation, recording, control, inspection, investigation, decision, resolution and sanctions as well as cooperation with other supervisory authorities.

Article 25
Functions of the Agency

The functions of the Andorran Data Protection Agency shall be:

1. to issue the instructions and recommendations that are necessary to adapt the processing of personal data to the principles of current legislation on matters of personal data protection;

2. to issue reports of a consultative nature, if these should be requested, for Bills, projects for regulatory provisions that are drawn up by the Government by virtue of the delegation of legislative powers, the drafts for Regulations or provisions of a general nature that affect the protection of personal data;

3. to issue its opinions about other Laws or regulations that affect the privacy of physical persons and the processing and the security of personal data;

4. to propose improvements related to the current regulations on matters concerning the protection of personal data;

5. to reply to the consultations that it receives from the Public Administrations, public and private institutions and citizens on the application of legislation on the protection of personal data;

6. to deal with petitions it receives from citizens;

7. to provide information on the rights of persons on matters of personal data protection; in particular by carrying out dissemination campaigns that it considers to be considered appropriate, and establishing the budgetary forecasts that correspond to this purpose in accordance with article 27 of these Regulations;

8. to draft, approve and publish the list of countries that provide equivalent protection on personal data matters, in accordance with what is established in article 36 of the Law on the protection of personal data.

9. to deal with the consultations related to the validity of the international communications of personal data to countries whose legislation does not offer a sufficient and adequate level of protection;

10. to decide fairly on the legitimacy or inadmissibility of the requests for the inscription, modification or elimination of files that have to be made to the Public Register for the Inscription of Personal Data Files and make registrations and the updates of personal data files in the Register;

11. to require data controllers and the service providers of personal data to take the measures that are necessary to adapt the processing of personal data under investigation to current legislation, and if necessary legally request the cessation of the processing and the cancellation of the files;

12. to bring, institute and decide the disciplinary proceedings concerning those responsible for the processing of privately owned files;

13. to press for the inception of disciplinary proceedings in the cases of infractions committed by the organs responsible for the files of the Andorran public Administration, and verify the effectiveness of the proceedings;

14. to prepare an annual report, which should be published in such a way that it is accessible to everybody in a public and generalized manner; it should be made accessible using the telematic means referred to in chapter twelve of these Regulations; the report should include information on the application of Qualified Law 15/2003 of 18th December on the protection of personal data (LQPD) and other legal and regulatory provisions for the protection of data.

Chapter nine. Personnel, economic and patrimonial system

Article 26
System for personnel

1. The system applicable to the Director and to the inspectors of the Agency for the development of their positions shall be that outlined in these Regulations with regard to the provisions of the Code of the Administration.

2. The system applicable to the personnel assigned to the Agency, other than the Director and the inspectors, shall be that established in the current regulations on labour matters.

3. The vacancies reserved for personnel assigned to the Agency must be filled by means of a public announcement and in accordance with the principles of equality, merit and capacity.

Article 27
Economic system

1. With regard to resources, the Andorran Data Protection Agency shall receive the annual appropriations that are established in the budgets of the General Council.

2. The accounts of the Andorran Data Protection Agency must be in line with the public accounting system.

3. The Accounts Tribunal shall exercise its function of supervising the Andorran Data Protection Agency.

Article 28
Budget

The Andorran Data Protection Agency must prepare its budget project each year and this should be sent to the General Council.

Article 29
Patrimonial and contracting system

1. The Andorran Data Protection Agency shall have its own capital resources consisting of the assets and rights that it acquires.

2. The Agency's legal system for contracting shall be that established in current legislation for Public Administration contracts.

   The Director of the Agency shall be the contracting organ.

Chapter Ten. Organs of the Agency

Article 30
Organic structure

1. The structure of the Andorran Data Protection Agency shall include the following organs:

a) The Director of the Agency.
b) Two inspectors.
c) Personal assigned to the Agency.

Article 31
The Director of the Agency

1. The Director of the Agency shall manage and legally represent the Andorran Data Protection Agency. He shall carry out his functions with full independence, neutrality and objectivity and he shall not be subject to any imperative mandate or instructions.

2. The Director of the Agency shall be appointed by the General Council, with the majority of votes established under Qualified Law 15/2003 of 18th December on the protection of personal data (LQPD); In the development of his activity, he shall be considered as a public authority and he shall be obliged to maintain the secrecy of the information that he acquires in the exercise of his functions, even after he has ceased to exercise them.

3. The Director of the Agency shall be appointed for a mandate of four years, which may be renewed when it ends.

4. The Director of the Agency shall be specifically responsible for:

   a) adjudicating and formalizing the contracts that are required for the management of the Agency and overseeing the fulfilment and performance of these;

   b) approving expenses and order payments within the limits of the Agency's budget spending credits;

   c) exercising the economic and financial control of the Agency;

   d) preparing the budgetary project of the Agency;

   e) approving the annual report of the Agency.

Article 32
The inspectors

1. The two inspectors of the Andorran Data Protection Agency shall assist and collaborate with the Director of the Agency in the exercise of the functions that are typical of the Agency.

2. The two inspectors shall be appointed by the General Council with the same majority of votes as that required to appoint the Director of the Agency.

3. In the performance of their tasks, the inspectors shall be considered as a public authority and they shall be obliged to maintain secrecy over the information that they acquire in the exercise of their functions, even after they have ceased to exercise them.

4. The inspectors shall be appointed for a mandate of four years, which may be renewed when it ends.

5. The inspectors of the Agency shall be specifically responsible for:

   a) carrying out the inspections entrusted to them by the Director of the Agency in accordance with what is established in these Regulations

   b) carrying out the other functions that are entrusted to them by the Director of the Agency.

Article 33
Remuneration

The Director and the inspectors of the Andorran Data Protection Agency shall receive the remunerations that have been assigned to their posts in the budget of the Agency that has been passed by the General Council.

Article 34
Abstention and recusation

The system of abstention and recusation of the Director of the Agency and the two inspectors must be in line with that which has been established in the Code of the Administration.

Article 35
Exercise of the power of inspection and investigation of the Andorran Data Protection Agency

1. Pursuant to what is envisaged in Qualified Law 15/2003 of 18th December on the protection of personal data (LQPD), the Andorran Data Protection Agency may carry out inspections at its own initiative, or else at the request of any data subject that considers that his rights have been affected or that a data controller has not fulfilled the obligations established by the Law.

2. To exercise its functions, the Andorran Data Protection Agency may address itself directly to the persons responsible for processing or to the service providers. Both the persons responsible for processing and the service providers shall be obliged to provide the Agency inspectors with all the information that they request from them and as well as providing access to their premises and to the computer resources or those of any other type used

in the processing of the data when they request them to do so in the exercise of this power of control.

3. The Agency may require any documentation or information that it considers relevant within the framework of any investigation.

4. The Agency shall also be responsible for carrying out inspections of both publicly owned and privately owned files. In this sense it may:

   a) request the presentation or the sending of documents and the issuing of copies;

   b) examine the systems of information support that contain personal data;

   c) examine the physical and logical equipment;

   d) examine the systems for transmission and access to the data;

   e) carry out audits of the computer systems to verify that they comply with the requirements of the Law on the protection of personal data;

   f) investigate and decide on the disciplinary proceedings;

   g) in order to gather any necessary evidence, and provided that it is necessary, the inspectors of the Agency will go to the place where the files are located, check the material, and if appropriate, they will prepare a photographic or audiovisual report.

5. The procedure for the inspection must comply with the following rules:

   a) The Director of the Agency must issue the corresponding authorization for the inspection so that the inspectors may issue the data controller with the demand for the documentation that they believe to be relevant in order to be able to carry out the inspection or, if appropriate, so that the inspectors can inspect the premises of the data controller or of the service provider where the files and the computer and support systems are and where the personal data to be processed are stored, in cases where an on-site inspection is carried out.

   b) The authorization for the inspection must contain at least the following information:

      - the number of the proceedings;
      - the name of the inspector who has been designated to make the inspection;
      - the name of the person who has made the official complaint, one exists;
      - the premises and the specification of the file, or the processing concerning which the demand for information and/or the inspection are to be made, if they are known, and the reasoning behind the appropriateness of these actions in relation to the proof or evidence that there has been an infringement of the Law, or in relation to the fact that has been reported;

- when known, the names of the data controllers and those of the data service providers who are to be inspected, and those of the premises and offices that are to be inspected.

c) The Agency may verify the fulfilment of the obligations established under Qualified Law 15/2003 of 18th December on the protection of personal data (LQPD), without the need to go to the premises of the data controllers or those of the service providers of personal data, by addressing the corresponding request for information to them by means of a demand (writ). In this case, the authorization issued by the Director of the Andorran Data Protection Agency should be attached to the demand for information that is sent, with the same content established in epigraph b) of this article.

d) In cases where an on-site inspection is carried out, the inspector appointed to make the inspection must present the authorization issued by the Director of the Agency, and the data controller shall be obliged to grant him access to the premises where the files, the computer systems and the systems used to store the personal data being processed are located. When the premises have the legal status of private residence, the activity of the inspection must also comply with the rules that guarantee inviolability.

e) In case of an on-site inspection, the inspectors shall draft a document notifying the data controller once the inspection has concluded.

f) Once the inspectors have carried out the investigation, they must present a proposal to the Director of the Andorran Data Protection Agency, who shall be responsible for deciding whether or not disciplinary measures are to be taken.

g) The data controller must be notified of the decision of the Director of the Andorran Data Protection Agency, regardless of whether or not the decision involves bringing disciplinary measures.

h) For all not expressly envisaged in these Regulations, the disciplinary procedure must comply with the provisions of the Code of the Administration.

Article 36
Prescription and expiry

1. The infractions specified in Qualified Law 15/2003 of 18th December on the protection of personal data (LQPD) prescribe 3 years after they have been committed.

2. The inspection and disciplinary procedures that the Andorran Data Protection Agency has initiated shall expire 6 months after the last action carried out without a new action having occurred or a resolution being issued.

Chapter eleven. Telematic communications

Article 37
Telematic means

1. The Andorran Data Protection Agency shall authorize the appropriate telematic means to exercise its functions and to allow citizens to exercise the rights that they have recognized in these Regulations, such as the right to make consultations, present formal complaints and other rights that they have recognized in the Regulations of the Public Register for the Inscription of Personal Data Files and the Law on the protection of personal data.

2. To this purpose, the corresponding budgetary provisions must be established in accordance with what is established in article 27 of these Regulations.

Repealing provision

The Regulations of the Andorran Data Protection Agency of 1st July 2004 and the modification thereof by the Decree of 21st July 2004 are hereby repealed.

Final provision

These Regulations shall come into force 15 days after the day that they are published in the Official Gazette of the Principality of Andorra.

Andorra la Vella, 9th June 2010

Jaume Bartumeu Cassany
Head of Government