

# PERSONAL DATA PROTECTION CODE

Legislative Decree no. 196 of 30 June 2003, entered into force 1 January 2004

[...]

## TITLE V – DATA AND SYSTEM SECURITY

### CHAPTER I – SECURITY MEASURES

#### Section 31

*(Security Requirements)*

1. Personal data undergoing processing shall be kept and controlled, also in consideration of technological innovations, of their nature and the specific features of the processing, in such a way as to minimise, by means of suitable preventative security measures, the risk of their destruction or loss, whether by accident or not, of unauthorized access to the data or of processing operations that are either unlawful or inconsistent with the purposes for which the data have been collected.

#### Section 32

*(Specific Categories of Data Controller)*

1. The provider of a publicly available electronic communications service shall take suitable technical and organisational measures under Section 31 that are adequate in the light of the existing risk, in order to safeguard security of its services and integrity of traffic data, location data and electronic communications against any form of unauthorised utilisation or access.

2. Whenever security of service or personal data makes it necessary to also take measures applying to the network, the provider of a publicly available electronic communications service shall take those measures jointly with the provider of the public communications network. Failing an agreement between said providers, the dispute shall be settled, at the instance of either provider, by the Authority for Communications Safeguards in pursuance of the arrangements set out in the legislation in force.

3. In case of a particular risk of a breach of network security, the provider of a publicly available electronic communications service shall inform subscribers and, if possible, users concerning said risk and, when the risk lies outside the scope of the measures to be taken by said provider pursuant to paragraphs 1 and 2, of all the possible remedies including an indication of the likely costs involved. This information shall be also provided to the Garante and the Authority for Communications Safeguards.

### CHAPTER II – MINIMUM SECURITY MEASURES

#### Section 33

*(Minimum Security Measures)*

1. Within the framework of the more general security requirements referred to in Section 31, or else provided for by specific regulations, data controllers shall be required in any case to adopt the minimum security measures pursuant either to this Chapter or to Section 58(3) in order to ensure a minimum level of personal data protection.

#### Section 34

*(Processing by Electronic Means)*

1. Processing personal data by electronic means shall only be allowed if the minimum security

measures referred to below are adopted in accordance with the arrangements laid down in the technical specifications as per Annex B:

- a) computerised authentication,
- b) implementation of authentication credentials management procedures,
- c) use of an authorisation system,
- d) regular update of the specifications concerning scope of the processing operations that may be performed by the individual entities in charge of managing and/or maintaining electronic means,
- e) protection of electronic means and data against unlawful data processing operations, unauthorised access and specific software,
- f) implementation of procedures for safekeeping backup copies and restoring data and system availability,
- g) keeping an up-to-date security policy document,
- h) implementation of encryption techniques or identification codes for specific processing operations performed by health care bodies in respect of data disclosing health and sex life.

### **Section 35**

*(Processing without Electronic Means)*

1. Processing personal data without electronic means shall only be allowed if the minimum security

measures referred to below are adopted in accordance with the arrangements laid down in the technical specifications as per Annex B:

- a) regular update of the specifications concerning scope of the processing operations that may be performed by the individual entities in charge of the processing and/or by the individual organisational departments,
- b) implementing procedures such as to ensure safekeeping of records and documents committed to the entities in charge of the processing for the latter to discharge the relevant tasks,
- c) implementing procedures to keep certain records in restricted-access filing systems and regulating access mechanisms with a view to enabling identification of the entities in charge of the processing.

### **Section 36**

*(Upgrading)*

1. The technical specifications as per Annex B concerning the minimum measures referred to in this Chapter shall be regularly updated by a decree of the Minister of Justice issued in agreement with the Minister for Innovation and Technologies by having regard to both technical developments and the experience gathered in this sector.

[...]

## ***TECHNICAL SPECIFICATIONS CONCERNING MINIMUM SECURITY MEASURES (ANNEX B)***

(see Sections 33 to 36 of the Code)

### **PROCESSING BY ELECTRONIC MEANS**

The following technical arrangements to be implemented by the data controller, data processor – if nominated – and person(s) in charge of the processing whenever data are processed by electronic means:

#### ***Computerised Authentication System***

1. Persons in charge of the processing shall be allowed to process personal data by electronic means if they are provided with authentication credentials such as to successfully complete an authentication procedure relating either to a specific processing operation or to a set of processing operations.
2. Authentication credentials shall consist in an ID code for the person in charge of the processing as associated with a secret password that shall only be known to the latter person; alternatively, they shall consist in an authentication device that shall be used and held exclusively by the person in charge of the processing and may be associated with either an ID code or a password, or else in a biometric feature that relates to the person in charge of the processing and may be associated with either an ID code or a password.
3. One or more authentication credentials shall be assigned to or associated with each person in charge of the processing.
4. The instructions provided to the persons in charge of the processing shall lay down the obligation to take such precautions as may be necessary to ensure that the confidential component(s) in the credentials are kept secret and that the devices used and held exclusively by persons in charge of the processing are kept with due care.
5. Where provided for by the relevant authentication system, a password shall consist of at least eight characters; if this is not allowed by the electronic equipment, a password shall consist of the maximum permitted number of characters. It shall not contain any item that can be easily related to the person in charge of the processing and shall be modified by the latter when it is first used as well as at least every six months thereafter. If sensitive or judicial data are processed, the password shall be modified at least every three months.
6. An ID code, if used, may not be assigned to another person in charge of the processing even at a different time.
7. Authentication credentials shall be de-activated if they have not been used for at least six months, except for those that have been authorised exclusively for technical management purposes.
8. Authentication credentials shall be also de-activated if the person in charge of the processing is disqualified from accessing personal data.
9. The persons in charge of the processing shall be instructed to the effect that electronic equipment should not be left unattended and made accessible during processing sessions.
10. Where data and electronic equipment may only be accessed by using the confidential component(s) of the authentication credential, appropriate instructions shall be given in advance, in writing, to clearly specify the mechanisms by which the data controller can ensure that data or electronic equipment are available in case the person in charge of the processing is either absent or unavailable for a long time and it is indispensable to carry out certain activities without further delay exclusively for purposes related to system operability and security. In this case, copies of the credentials shall be kept in such a way as to ensure their confidentiality by specifying, in writing, the entities in charge of keeping such credentials. Said entities shall

have to inform the person in charge of the processing, without delay, as to the activities carried out.

11. The provisions concerning the authentication system referred to above as well as those concerning the authorisation system shall not apply to the processing of personal data that are intended for dissemination.

### ***Authorisation System***

12. Where authorisation profiles with different scope have been set out for the persons in charge of the processing, an authorisation system shall be used.

13. Authorisation profiles for each person or homogeneous set of persons in charge of the processing shall be set out and configured prior to start of the processing in such a way as to only enable access to the data that are necessary to perform processing operations.

14. It shall be regularly verified, at least at yearly intervals, that the prerequisites for retaining the relevant authorisation profiles still apply.

### ***Other Security Measures***

15. Within the framework of the regular update – to be performed at least at yearly intervals – of the specifications concerning the scope of the processing operations that are entrusted to the individual persons in charge of the processing as well as to the technicians responsible for management and/or maintenance of electronic equipment, the list of the persons in charge of the processing may also be drawn up by homogeneous categories of task and corresponding authorisation profile.

16. Personal data shall be protected against the risk of intrusion and the effects of programmes as per Section 615-quinquies of the Criminal Code by implementing suitable electronic means to be updated at least every six months.

17. The regular update of computer programmes as aimed at preventing vulnerability and removing flaws of electronic means shall be carried out at least annually. If sensitive or judicial data are processed, such update shall be carried out at least every six months.

18. Organisational and technical instructions shall be issued such as to require at least weekly data back-up.

### ***Security Policy Document***

19. By 31 March of each year, the controller of processing operations concerning sensitive and/or judicial data shall draw up, also by the agency of the data processor, if nominated, a security policy document containing appropriate information with regard to:

19.1 the list of processing operations concerning personal data,

19.2 the distribution of tasks and responsibilities among the departments/divisions in charge of processing data,

19.3 an analysis of the risks applying to the data,

19.4 the measures to be taken in order to ensure data integrity and availability as well as protection of areas and premises insofar as they are relevant for the purpose of keeping and accessing such data,

19.5 a description of the criteria and mechanisms to restore data availability following destruction and/or damage as per point 23 below,

19.6 a schedule of training activities concerning the persons in charge of the processing with a view to informing them on the risks applying to the data, the measures that are available to prevent harmful events, the most important features of personal data protection legislation in connection with the relevant activities, the resulting liability and the arrangements to get updated information on the minimum security measures adopted by the data controller. Said training activities shall be planned as of the start of the employment relationship as well as in

connection with changes in the task(s) discharged and/or the implementation of new, significant means that are relevant to the processing of personal data,

19.7 a description of the criteria to be implemented in order to ensure adoption of the minimum security measures whenever processing operations concerning personal data are externalised in accordance with the Code,

19.8 as for the personal data disclosing health and sex life referred to under point 24, the specification of the criteria to be implemented in order to either encrypt such data or keep them separate from other personal data concerning the same data subject.

#### ***Additional Measures Applying to Processing of Sensitive or Judicial Data***

20. Sensitive or judicial data shall be protected against unauthorised access as per Section 615-ter of the Criminal Code by implementing suitable electronic means.

21. Organisational and technical instructions shall be issued with regard to keeping and using the removable media on which the data are stored in order to prevent unauthorised access and processing.

22. The removable media containing sensitive or judicial data shall be destroyed or made unusable if they are not used; alternatively, they may be re-used by other persons in charge of the processing, who are not authorised to process the same data, if the information previously contained in them is not intelligible and cannot be re-constructed by any technical means.

23. If either the data or electronic means have been damaged, suitable measures shall be adopted to ensure that data access is restored within a specific deadline, which must be compatible with data subjects' rights and not in excess of seven days.

24. Health care bodies and professionals shall process data disclosing health and sex life as contained in lists, registers or data banks in accordance with the mechanisms referred to in Section 22(6) of the Code also in order to ensure that said data are processed separately from the other personal data allowing data subjects to be identified directly. Data concerning genetic identity shall only be processed in protected premises that may only be accessed by such persons in charge of the processing and entities as have been specifically authorised to access them. Containers equipped with locks or equivalent devices shall have to be used in order to remove the data outside the premises reserved for their processing; the data shall have to be encrypted for the purpose of electronically transferring them.

#### ***Safeguards and Protections***

25. Where a data controller adopts minimum security measures by committing the relevant tasks to external entities, prior to implementing such measures he or she shall require the installing technician(s) to supply a written description of the activities performed by which it is certified that they are compliant with the provisions set out in these technical specifications.

26. The circumstance that the security policy document has been drawn up and/or updated shall be referred to in the management report that the data controller may be required to submit together with the relevant balance sheet.

#### ***Processing without Electronic Means***

The following technical arrangements to be implemented by the data controller, data processor – if nominated – and person(s) in charge of the processing whenever data are processed without electronic means:

27. The persons in charge of the processing shall be instructed in writing with regard to controlling and keeping, throughout the steps required to perform processing operations, records and documents containing personal data. Within the framework of the regular update – to be performed at least at yearly intervals – of the specifications concerning the scope of the processing operations that are entrusted to the individual persons in charge of the processing,

the list of the persons in charge of the processing may also be drawn up by homogeneous categories of task and corresponding authorisation profile.

28. If records and documents containing sensitive or judicial personal data are entrusted to the persons in charge of the processing for the latter to discharge the relevant tasks, said records and documents shall be kept and controlled by the persons in charge of the processing until they are returned so as to prevent unauthorised entities from accessing them; they shall be returned once the relevant tasks have been discharged.

29. Access to archives containing sensitive or judicial data shall be controlled. The persons authorised to access said archives for whatever purpose after closing time shall be identified and registered. If an archive is not equipped with electronic devices for access control or is not placed under the surveillance of security staff, the persons accessing said archive shall have to be authorised in advance.