

**THIS IS AN UNOFFICIAL TRANSLATION. THE ONLY LEGAL
BINDING TEXT IS THE ONE PUBLISHED IN THE SPANISH
OFFICIAL JOURNAL. (BOE 151, 11 JUNE 1999)**

ROYAL DECREE 994/1999, of 11 June, which approves the Regulation on Mandatory Security Measures for the Computer Files which contain Personal Data.

CHAPTER I. General provisions

Article 1.- Scope and purposes

The purpose of this regulation is to lay down the technical and organisational measures necessary to guarantee the security of automated files, processing centres, premises, equipment, systems, programs and the persons involved in the automated processing of personal data subject to the regime set up by Organic Law No. 5/1992 of 29 October 1992 regulating the automatic processing of personal data.

Article 2.- Definitions.

For the purposes of this Regulation, the following terms shall be defined as follows:

1. Information system: a set of automated files, programs, media and equipment used to store and process personal data;
2. User: the subject or process authorised to access data or resources;
3. Resource: any component part of an information system;
4. Authorised access: authorisation granted to a user to use the various resources;
5. Identification: a procedure for identifying users;
6. Authentication: a procedure for verifying a user's identity;
7. Access control: a mechanism granting access to data or resources following authenticated identification;
8. Password: confidential information, frequently made up of a chain of characters, which can be used in user authentication;
9. Incident: any anomaly which affects or which might affect data security;
10. Medium: a physical object likely to be processed in an information system and on which data may be recorded or from which they may be retrieved;
11. Security officer: a person or persons to whom the controller has formally assigned the duty of coordinating and monitoring the security measures to be applied;

12. Backup copy: a copy of the data contained in a computer file stored on a medium to make recovery possible.

Article 3.- Security levels

1. The requisite security measures shall be classed in three levels: basic, medium and high.
2. Those levels shall be set, bearing in mind the nature of the information processed, in relation to the extent to which it is necessary to guarantee the confidentiality and integrity of the information.

Article 4.- Application of security levels.

1. All files containing personal data must adopt the security measures classed as basic level.
2. Files containing data relating to the commission of administrative or criminal infractions, the Ministry of Finance, financial services and those files the operation of which is governed by Article 28 of Organic Law No. 5/1992 must take the basic-level measures and those classed as medium-level.
3. Files containing data on persons' ideologies, religion, beliefs, racial origins, health or sex life and any containing data collected for police purposes without the consent of the persons concerned must take the basic, the medium-level and the high-level measures.
4. Files containing a set of personal data sufficient to permit an assessment of an individual's personality must take the medium-level measures laid down in Articles 17, 18, 19 and 20.
5. Each of the levels described above represent the minimum required, without prejudice to the specific legal or regulation provisions in force.

Article 5.- Access to data via communications networks

The security measures required for access to personal data via communications networks must guarantee a security level equivalent to that applying to local access.

Article 6.- Working procedures outside the premises where the file is located

The processing of personal data outside the premises where the file is located must be expressly authorised by the controller, and, in any case, the corresponding level of security must be guaranteed for the processed file.

Article 7.- Temporary files

1. Temporary files must guarantee the corresponding level of security for the purposes of the criteria laid down in this Regulation.
2. All temporary files must be erased once they are no longer necessary for the purposes for which they were created.

CHAPTER II. Basic-level security measures

Article 8.- Security document

1.- Controllers shall draw up and implement security rules in the form of a compulsory document for staff who have access to automated personal data and information systems.

2.- The document must cover the following aspects, as a minimum:

- a) the scope of the document, with a detailed specification of protected resources;
- b) measures, standards, procedures, rules and norms to guarantee the level of security required by this Regulation;
- c) the functions and obligations of staff;
- d) the structure of files containing personal data and a description of the information systems on which these are processed;
- e) the procedures for reporting, managing and responding to incidents;
- f) the procedures for making backup copies and recovering data;

3.- The document must be kept up to date at all times, and must be revised whenever relevant changes are made to the information system or to how it is organised.

4.- The content of the document must at all times comply with the provisions on the security of personal data.

Article 9.- The functions and obligations of staff

1. The functions and obligations of every individual with access to personal data and to information systems shall be clearly defined and documented, in accordance with the provisions of Article 8.2.c).
2. Controllers shall adopt the measures necessary to make staff familiar with the security rules concerning the performance of their functions and the consequences of any breach of these rules.

Article 10.- Record of incidents

The procedure for reporting and managing incidents shall necessarily include a record of any kind of incident, the time at which it occurred, the person reporting it, to whom it was reported and the effects thereof.

Article 11.- Identification and authentication.

1. The controller shall ensure that an up-to-date record is kept of those users who have authorised access to the information system, and shall set up identification and authentication procedures for such access.

2. When authentication mechanisms are based on passwords, a procedure which guarantees their confidentiality and integrity shall be set up for assigning, distributing and storing these.
3. Passwords shall be changed at the regular intervals laid down in the security document, and shall be stored in a way which makes them unintelligible while they remain valid.

Article 12.- Access control

1. Users shall have authorised access only to those data and resources necessary for them to perform their duties.
2. Controllers shall set up mechanisms to avoid any user gaining access to data or resources with rights other than those authorised.
3. The record of users referred to in Article 11.1 of this Regulation shall contain the authorised access available to each.
4. Only those staff who are authorised to this end in the security document may grant, alter or cancel authorised access to data and resources, in accordance with the criteria laid down by the controller.

Article 13.- Management of media

1. Media containing personal data must permit the kind of information they contain to be identified, inventoried and stored at a location with access restricted to staff who are authorised to this end in the security document.
2. The removal of media containing personal data from the premises on which the file is located may solely be authorised by the controller.

Article 14. - Backup copies and recovery

1. The controller shall be responsible for checking the definition and correct application of the procedures for making backup copies and recovering data.
2. The procedures laid down for making backup copies and for recovering data must guarantee that they can be reconstructed in the state they were in at the time they were lost or destroyed.
3. Backup copies must be made at least once a week, unless no data have been updated during that period.

CHAPTER III. Medium-level security measures

Article 15.- Security document

In addition to complying with Article 8 of this Regulation, the security document must identify the officer or officers responsible for security, the periodic checks to be carried out to monitor compliance with the provisions of the document itself and the measures which need to be taken when any media are to be disposed of or reused.

Article 16.- Security officer

The controller shall appoint one or more individuals as security officers, who shall be responsible for coordinating and monitoring the measures defined in the security document. Under no circumstances may such appointments entail any delegation of the responsibility borne by the controller pursuant to this Regulation.

Article 17.- Audit

1. Every two years at least, the information systems and data processing installations shall undergo an internal or external audit to check that the procedures and instructions in force regarding data security comply with this Regulation.
2. The audit report must provide an opinion on the extent to which the measures and controls comply with this Regulation, identify their shortcomings and propose such corrective or supplementary measures as necessary. It should also include the data, facts and observations on which the opinions reached and the recommendations proposed are based.
3. The audit reports shall be analysed by the security officer who is responsible for this area, who shall refer the conclusions to the controller so that he can take the appropriate corrective steps, and the reports shall remain at the disposal of the Data Protection Agency.

Article 18.- Identification and authentication

1. Controllers shall set up mechanisms which permit unequivocal, personalised identification of any user who attempts to access the information system and a check to establish whether each user is authorised.
2. Limits shall be placed on the scope for repeating attempts to gain unauthorised access to the information system.

Article 19.- Physical access control

Only those staff duly authorised in the security document may have access to the premises where information systems with personal data are located.

Article 20.- Management of media

1. A system for recording incoming media must be set up which permits direct or indirect identification of the kind of media, the date and time, the sender, the number of media, the kind of information contained, how they are sent and the person responsible for receiving them, who must be duly authorised.
2. A system shall also be set up for recording outgoing media which permits direct or indirect identification of the kind of media, the date and time, the recipient, the number of media, the kind of information contained, how these are sent out and the person responsible for doing so, who must be duly authorised.
3. When media are to be disposed of or reused, the necessary measures shall be taken to prevent any subsequent retrieval of the information stored on them before they are withdrawn from the inventory.

4. When media are to leave the premises on which the files are located as a result of maintenance operations, the necessary measures shall be taken to prevent any undue retrieval of the information stored on them.

Article 21.- Record of incidents

1. The register governed by Article 10 must also record the procedures put in place to recover data, indicating the person who undertook the process, the data restored and, as appropriate, which data had to be input manually in recovery process.
2. Written authorisation from the controller shall be necessary for any data recovery procedures.

Article 22.- Tests with real data

Testing prior to the implementation or modification of information systems processing files with personal data shall not use real data unless the level of security corresponding to the type of file processed can be guaranteed.

CHAPTER IV. High-level security measures

Article 23.- Distribution of media

Media containing personal data may only be distributed if the data have been enciphered or another mechanism used to guarantee that that information is not intelligible or is not manipulated in transit.

Article 24.- Access record

1. The minimum details to be recorded for every access shall be the user's identity, the date and the time of access, the file accessed, the kind of access and whether this was authorised or denied.
2. If access was authorised, it shall be necessary to retain the information which permits the record accessed to be identified.
3. The mechanisms permitting the data set out in detail in the preceding paragraphs to be recorded shall be under the direct control of the competent security officer, and under no circumstances must it be permissible to deactivate these.
4. The minimum period for retaining the data recorded shall be two years.
5. The corresponding security officer shall be responsible for periodically reviewing the control information recorded, and shall draw up a report on the reviews carried out and any problems detected at least once every month.

Article 25.- Backup copies and recovery

A backup copy and data recovery procedures must be kept at a different location from the site of the computer equipment processing the data and the security measures required in this Regulation must be taken in any event.

Article 26.- Telecommunications

Personal data may be distributed via telecommunications networks only if they have been enciphered or another mechanism is used to guarantee that the information is not intelligible or is not manipulated by third parties.

CHAPTER V. Infractions and penalties

Article 27.- Infractions and penalties

1. Breach of the security measures described in this Regulation shall be punishable in accordance with Articles 43 and 44 of Organic Law No. 5/1992 when the files are in private ownership.
The procedure to be observed for imposing the penalty referred to in the preceding paragraph shall be that laid down in Royal Decree No. 1332/1994 of 20 June implementing particular aspects of Organic Law No. 5/1992 of 29 October 1992 governing the automatic processing of personal data.
2. When the files are the responsibility of general government, the procedure and the penalties shall be those provided in Article 45 of Organic Law No. 5/1992.

Article 28.- Controllers

Controllers subject to the penalties of Organic Law No. 5/1992 must take the technical and organisational measures necessary to guarantee the security of personal data on the terms laid down in this Regulation.

CHAPTER VI. Powers of the Director of the Data Protection Agency

Article 29.- Powers of the Director of the Data Protection Agency

Pursuant to Article 36 of Organic Law No. 5/1992, the Director of the Data Protection Agency may:

1. issue, when appropriate and without prejudice to the powers of other bodies, the instructions necessary to have authorised processing comply with the principles of Organic Law No. 5/1992.
2. order the cessation of any processing of personal data and the deletion of files when the security measures provided for in this Regulation are not implemented.

SOLE TRANSITIONAL PROVISION. Time limits for implementing measures

For information systems which are operating when this Regulation comes into force, the basic-level security measures provided in this Regulation must be implemented within six months of its coming into force, the medium-level measures within one year and the high-level measures within two years.

When the information systems in operation do not technologically permit any of the security measures provided in this Regulation to be implemented, these systems must be adapted and the security measures must be implemented within three years of the date on which this Regulation comes into force.