Elta Elettronica Srl
Vat IT00453520231 , Registrered in Verona REA num. VR-139873 , Capital € 25.480,00
Registered Office , Headquarter : via Fossa Contarina, 4 – 37057 - S.Giov.Lupatoto- Verona - Italia
Phone: +39 045 9251577 - Fax: +39 045 548828 - Web: www.eltasrl.com - Email: info@eltasrl.com

ANNEX B. TECHNICAL REGULATIONS ON MINIMUM SECURITY MEASURES ABOUT PERSONAL DATA PROCESSING
(Arts. from 33 to 36 of the Code)

Processing with electronic tools

Technical methods to be adopted by the data holder, the data manager if appointed and the data processing operator, in the case of processing with electronic tools:

IT authentication system

1. Personal data processing with electronic tools is allowed if carried out by operators assigned authentication credentials which allow them to pass through an authentication procedure for specific processing or a series of processing procedures.

2. The authentication credentials comprise a code for the operator's identification, associated with a confidential password known only to the same, or an authentication device exclusively held and used by the operator, possibly associated with a user name or a password, or a biometric feature of the operator possibly associated with a user name or a password.

3. One or more credentials are assigned to, or associated with, each operator.

4. The operators are instructed to take the necessary precautions to ensure secrecy of the confidential part of their credentials and to take suitable care of the devices in their hands for the exclusive use of each operator.

5. The password, when contemplated by the authentication system, is composed of at least eight characters or, in the case of an electronic device which does not allow this, by as many characters as allowed; it does not contain references easily traceable to the operator and this latter changes it the first time he/she uses it and, successively, at least once every six months. In the case of the processing of sensitive and judicial data, the password is changed at least once every three months.

6. The identification code, once used, cannot be assigned to any other operator even at a distance in time.

7. Authentication credentials that have not been used for at least six months are deactivated, except those authorised in advance solely for technical management.

8. The credentials are deactivated also if the operator loses the authority for access to the personal data.

9. The operators are instructed not to leave the electronic tool unattended during a processing session.

10. When access to the data and to the electronic tools is allowed only by means of the use of the confidential component of the authentication credentials, suitable and preventive written instructions are issued clearly indicating the method by which the data holder can ensure the availability of the data or electronic tools in the case of the operator's prolonged absence or impediment for which it is essential and non-deferrable to take action exclusively for operational and system security needs. In such a case, the custody of the copies of the credentials are organised in a manner which guarantees their secrecy and with prior identification of the subjects responsible for their custody, which latter must immediately inform the operator of the action performer.

11. The provisions on the authentication system indicated in the above points and on the authorisation system are not applicable to the processing of personal data destined to be disclosed.

Authorisation system

12. When the authorisation profiles relative to different environments are identified for the operators, an authorisation system is used.

13. The authorisation profiles, for each operator or for each class of similar operators, are identified and configured before the start of the processing, to limit access solely to the data necessary for performing the processing operations.

14. Periodically, and in any case at least once a year, the existence of the conditions for maintaining the authorisation profiles are verified.

Other security measures

15. Within the sphere of the periodic updating, at least once a year, of the identification of the processing environment accessible to the individual operators and to those responsible for the management or maintenance of the electronic tools, the list of the operators may also be drawn up for classes of similar operators and the relative authorisation profiles.

16. The personal data are protected against the risk of intrusion and programming action as contemplated by art. 615-quinquies of the Italian criminal code, by the activation of suitable electronic tools to be updated at least once every six months.

17. The processing programmes are updated at least once a year to prevent the vulnerability of the electronic tools and to correct any defects of the same. Sensitive and judicial data are updated at least once every six months.

18. Organisational and technical instructions are issued according to which the data must be backed up at least once a week.

Security programme document

19. Within 31 March every year, the holder of sensitive or judicial data draws up, also through the data manager, if appointed, a document on the security programme containing suitable information regarding:

19.1. the personal data processing list;

19.2. the distribution of the duties and responsibilities among the structures appointed to process the data;

19.3. the analysis of the risks to which the data are subject;

19.4. the measures to be adopted to guarantee the intact nature and the availability of the data, as well as the protection of the areas and premises involved in data custody and access;

19.5. The description of the criteria and methods for recovering the availability of the data subsequent to destruction or damage, referred to in point 23 below;

19.6. The programme of training activities for data processing operators to make them aware of the risks to which the data are subject, the measures available to prevent damaging events, the most important profiles as regards personal data protection rules, according to the relative activities, the consequent responsibilities, and the means for updating the minimum measures adopted by the data holder. Training is programmed from the moment of entering into service, and in the case of changes in duties or the introduction of significant new tools which have an impact on personal data processing;

19.7. The description of the criteria to be adopted to guarantee the adoption of the minimum security measures for the outsourced processing of the personal data, in compliance with the Code;

19.8. For personal data which can reveal the state of health or sexual activity, referred to under point 24, the identification of the criteria to be adopted for encrypting or for separating these data from the other personal data of the subject concerned.

Additional measures for the processing of sensitive or judicial data

20. Sensitive and judicial data are protected against unauthorised access, pursuant to art. 615-ter of the criminal code, by the use of suitable electronic tools.

21. Organisational and technical instructions are issued for the custody and use of the removable devices on which the data are memorised, to avoid unauthorised access and forbidden processing.

22. If the removable devices containing sensitive or judicial data are no longer used, they are destroyed or rendered unusable, or they may be reused by another operator, not authorised to process such data, if the information previously contained on the same is not intelligible and it is technically impossible to reconstruct the same.

23. Suitable measures are adopted to guarantee the restoration of the access to the data in the case of damage to the same or to the electronic instruments, within specified times compatible with the rights of the persons concerned and, in any case, within seven days.

24. Health authorities and health workers process data which can reveal the state of health and sexual activity contained on lists, on registers or in data banks, according to the methods prescribed by article 22, paragraph 6, of the Code, also to allow for such data to be processed separately from the other personal data which allow for directly identifying the persons concerned. The data relative to genetic identity are processed exclusively inside protected premises accessible only to the processing operators and subjects specifically authorised to enter the same; the transport of the data outside the premises reserved for their processing must take place in containers provided with locks or similar devices; for electronic transfer, the data are encoded.

Measures for protection and guarantee

25. The holder which adopts minimum security measures and which takes avail of subjects external to its own structure for the implementation of said measures, receives from the installer a written description of the action carried out which testifies to compliance with the provisions of these technical regulations.

26. In the report which accompanies the financial statement, if due, the holder declares that the security programme document has been drafted and updated.

Processing without the use of electronic instruments

Technical methods to be adopted by the data holder, the data manager if appointed and the data processing operator, in the case of processing without electronic tools:

27. The operators are given written instructions, for the entire cycle necessary for the performance of the processing operations, for the control and custody of the deeds and documents containing personal data. At least once a year, within the sphere of the periodic updating of the identification of the processing environment accessible to the individual operators, the operators may also be listed according to classes of similar operators and of the relative authorisation profiles.

28. If the deeds and documents containing sensitive or judicial personal data are entrusted to the processing operators for the execution of their relative duties, the said deeds and documents are checked by the operators and remain in their care until they are returned, so that unauthorised persons cannot gain access to the same, and they are returned on completion of the assigned operations.

29. Access to the files containing sensitive or judicial data is controlled. Persons allowed access, on any grounds whatsoever, after closing time, are identified and registered. When the archives are provided with electronic tools or with surveillance personnel for controlling access, those who gain access must have prior authorisation.