Rules for the processing of personal data in INFN

Legislative Decree 30 June 2003 n. 196
Code regarding personal data processing

1. DEFINITIONS

1.1 The processing of personal data

For the processing of personal data we refer to any operation or set of operations carried out with or without the aid of electronic instruments concerning the collection, recording, organization, storage, consultation, processing, modification, selection, extraction, comparison, use, interconnection, blocking, communication, dissemination, erasure and destruction of data, even if not registered in a database.

1.2 Types of data

Personal data are divided into: personal, sensitive and judicial data.
Personal data (so-called **common**) are information relating to individuals, corporate entities, organizations or associations, identified or identifiable even indirectly by reference to any other information, including a personal identification number.
Sensitive data are personal data that reveal racial or ethnic origin, religious beliefs, philosophical or other beliefs, political opinions, membership of parties, unions, or religious, philosophical, political, trade union associations or organizations as well as personal data reveal health and sex life.
Judicial data are data that reveal measures registered in the Criminal Records Office or in the Register of administrative sanctions due to crime and related charges or the status of being a suspect or an accused.

1.3 Subjects

The relevant parties in the processing of personal data are the *Data Controller*, the *Data Processors* and the *Persons tasked with processing*, as well as the *Data Subjects.*
Data Controller of the processing of personal data is the National Institute of Nuclear Physics as a whole.
Data Processors are the subjects that for their experience, capability and reliability provide sufficient guarantees for the respect of the rules on data processing, including the security profile. INFN, by resolution of the Board of Directors N. 6389/89, subsequently updated with the CD deliberation n. 8335/03, identified as Data Controller the Directors of the Structures, as well as the Directors of Departments and Administration Central Services and the Head of the INFN Presidency Service.
The **Persons tasked with processing** are the subjects authorized to perform data processing operations; those who are responsible for the operation and / or maintenance of processing plants are in charge of the **System Administrator** function.
Data Subjects are the subjects (natural person and corporation) to whom the personal data concern.

2. GENERAL PRINCIPLES FOR THE PROCESSING OF PERSONAL DATA

The processing of personal data must be made in respect of the rights and the fundamental freedoms, as well as the dignity of the persons to whom the data refer, with particular reference to privacy, personal identity and protection of personal data.
The National Institute of Nuclear Physics allows the processing of personal data only for the performance of institutional activities.
Each processing operation must be carried out minimizing the use of personal data, so as to exclude the processing when the purpose can be achieved by using anonymous data or protocols that allow the processing only in case of necessity; this principle must be observed - in case of processing carried out by electronic means - also in the configuration of information systems and computer programs.
In any case, personal data must be:

- processed lawfully and correctly;
- collected and recorded for specific, explicit and legitimate purposes and used in other processing operations in terms that are compatible with those purposes;
- accurate and, where necessary, updated;
- adequate, complete and not exceeding for the purposes for which they are processed;
- kept in a form which permits identification only for the time necessary for the purposes for which the data were collected or processed.

The Data Processors appoint in writing the Persons tasked with processing and the System Administrators and indicate the scope of processing possible for each.
The same Data Processors shall revoke the authorizations when the conditions for the use of processing are no longer required, such as the transfer to another office, the assignment of other activities or the termination of employment or collaboration with INFN.

3. INFORMATION NOTICE

In accordance with Legislative Decree n. 196/2003, the INFN has prepared special information for the processing of personal data of employees and associated persons, distributed to the interested parties at the time of the association or employment. They have also prepared information for the personnel selection activities and for the performance of contractual procedures.
In all other circumstances the Data Processors shall provide to the parties, orally or in writing, prior information about:

- the purposes and methods of processing;
- the compulsory or optional nature of providing data, with the indication of the consequences of a refusal to respond;
- the indication of the Data Controller and the Data Processor, and the persons to whom the data may be communicated or who can learn about them as Persons tasked with processing;
- the guarantee of being able to exercise the rights under Art. 7 of Legislative Decree. N. 196/03.

4. COMMUNICATION AND DISSEMINATION OF DATA

The communication of personal data to another public entity can be made when it is provided for by provision of law or regulation; in the absence of this rule it can be made when it is still necessary for the performance of official duties, with advance notice of the processing provided to the Guarantor, and a period of 45 days allowed for the Guarantor to revoke the right of communication of the data."
The communication to private or public economic entities and the dissemination are allowed only if they are provided for by laws or regulations.
In any case the data that reveal the state of health, may not be disseminated.

5. MINIMUM SECURITY MEASURES FOR THE PROCESSING OF PERSONAL DATA

The minimum security measures comprise the whole of technical and organizational measures that INFN is required to take in order to minimize the risks of destruction or loss, even accidental, of personal data, unauthorized access or processing not allowed or not in accordance with the purposes of collection.
Data Processors are therefore required to take all the appropriate measures to minimize the risks mentioned above and the Persons tasked with processing must avoid any conduct that may undermine the confidentiality.

5.1 Data processing carried out with electronic instruments

IT resources in the availability of Data Processors and Persons tasked with processing should be accessible with mechanisms that enable, uniquely, the user identification (Data Processor or Person tasked with processing): identification which must take place through the adoption of an authentication mechanism that is implemented in the use, at least, of a personal identification code (user-id) and a keyword (password).

5.1.1 Method of password selection and management

A proper identification of passwords is an essential element for security and protection of personal data processed through the use of electronic means, as one of the most used methods for illegal access to a system or an application is to obtain and use the username and password of an authorized user. In order to minimize this risk it is necessary, therefore, keep in mind that:

- the password is personal and the user is responsible for its proper conservation and management;
- the password must have a length of no less than eight (8) characters or the maximum number of characters allowed by the system or application;
- the password must be changed at least every six months and at least every three months when designed to ensure the access to computers, systems, applications (databases, folders or documents) that contain sensitive personal data;

- in the selection of the password personal references must be avoided (first or last name,
- family members, address, etc ...) or real words in any language;
- the user is required to take all measures necessary and appropriate in order to avoid that third parties have access to his computer, even if he walks away during a work session: in this case, for example, he should exit from the application in use and activate a password-protected screen saver;
- the user must take care not to communicate to others the passwords, and not to write them down on papers that others could easily read (for example placed in the vicinity of the computer);
- the user must take care, if there are multiple authentication systems, not to use the same password and to not make known the old ones, even if no longer in use, as they may be able to identify the rules used for their creation.

The proper identification, custody and password management allows the user to protect himself from any incorrect activities, or even illegal activities, carried out by others through the computer assigned to him.

5.1.2 Keeper of the password

Data Processor provides in writing the identification of one or more Keepers of the passwords, depending on organizational complexity of the Structure, Management or Service that he directs. The role of the keeper is to ensure data availability in the event of prolonged absence or impediment of the Person tasked with processing, when it is essential and urgent to intervene because of operational needs and system security.
The Keeper of the keys can change the password of the Person tasked with processing as he knows the privileged passwords of all the systems involved. When is necessary to intervene in the computer of the Person tasked with processing, if he is absent, the Keeper changes the password and allows the necessary intervention. He shall then inform the Person tasked with processing, once back in service, who will restore a new personal password.
Additional methods, also computerized, for password management, can be identified by each Data Processor provided that they guarantee the availability of data only if, in the absence of the Person tasked with processing, it is necessary to immediately intervene to ensure the operability and safety of the system, with the obligation of a timely notification to the Person tasked with processing the intervention that was made and the recovery of the new passwords.

5.1.3 Hardware and software protection measures

Data Processors shall ensure that the available servers in their Structure, Departments or Service are anchored to walls or floors, located in an environment with controlled access (locked rooms) and equipped with air conditioning systems, fire protection systems and anti-flooding systems. The resources considered critical must also be protected by installing systems that ensure the continuity of electricity.
Data Processors ensure, also through the Calculation Services and Networks, that anti intrusion computer systems are installed, making sure that the updating is carried out at least every six months.
Data Processors must observe that anti-virus programs are installed on all the computers, through the Computing Services and Networks, or companies that offer IT support, as to

provide real-time protection. The programs must be configured to automatically update at least once a week.
In order to protect computers from cyber threats the Persons tasked with processing are required, in any case, to comply with the "*Regulation for the use of INFN information technology resource*" available at the following website address:
http://www.ac.infn.it/accesso_risorse_informatiche/disciplinare_en.pdf

5.1.4 Back-up copies

The Persons tasked with processing are required to make the backup of their files, creating backup copies in order to allow the restoration of the situation prior to the harmful event , in case of data loss.
The backup can be made, as indicated by the Computing Services and Networks, on specific servers, or on disks, tapes or other removable media.
Removable media containing backup copies must be kept in locked cabinets. The same media can not be reused by other Persons tasked with processing, if not the information contained in them has not been made unintelligible or not reconstructable.
Periodically, and at least monthly, Persons tasked with processing are required to make restoration test, to check the ongoing adequacy of the methods adopted and the backup media used.

5.2 Processing of data without electronic instruments

If personal data are contained in documents or papers, the Persons tasked with processing must preserve such documents and papers so that no unauthorized persons will have access.
For this purpose the Persons tasked with processing are required to:

1. use the documents containing personal data only for the time necessary to perform their work, taking care to place the documents in the archives after the completion of the relevant operation;
2. do not leave documents unattended on desks or other furniture when they leave the office, taking care to close the room, in case of a prolonged absence;
3. keep documents containing sensitive or judicial data in locked cabinets or otherwise in access-controlled archives;
4. preserve, in particular, documents containing data relating to health and sex life separately from the others.

6. Liability and penalties

Legislative Decree 30 June 2003 - Code regarding the protection of personal data - provides that anyone who causes damage to another as a result of the processing of personal data shall compensate in accordance with art. 2050 of the Civil Code, unless he can prove that he has adopted all technical and organizational measures to avoid the damage: in order to provide such proof it is therefore absolutely necessary to strictly observe all safety measures in accordance with the regulation concerning the protection of personal data.
The same Decree N. 196/03 also provides for criminal penalties if the minimum security measures are not respected or for the unlawful processing of personal data and provides administrative penalties in case of failure or unsuitable information to the parties involved.

Please note, finally, that the failure to adopt the indicated measures, constitutes non-compliance with service requirements, and may determine liability to disciplinary sanctions.