GDPR - GENERAL DATA PROTECTION REGULATION

Starting May 2018, the new EU Regulation 2016/679 (GDPR - General Data Protection Regulation) on the protection of personal data has imposed new rules and requirements for management of data relating to individuals. These new requirements are also applicable to testing laboratories, not only with regard to the personal data of employees, suppliers and customers, already managed for contributory or accounting purposes, but also for those more operational aspects concerning "technical registration" produced by laboratories test.

A practical example of this statement is chapter 7.5.1 of ISO / IEC 17025: 2017:

ISO/IEC 17025:2017 - § 7.5.1 The laboratory shall ensure that technical records for each laboratory activity contain the report of the results, and sufficient information to facilitate, if possible, identification of factors affecting the measurement uncertainty and enable the repetition of the laboratory activity under conditions as close as possible to the original. The technical records shall include the date and the identity of personnel responsible for each laboratory activity and for checking data and results. Original observations, data and calculations shall be recorded at the time they are made and shall be identifiable with the specific task.

Even more important are the so-called "sensitive" personal data, in accordance with the provisions of GDPR article 9 "Processing of special categories of personal data", which can be managed by the laboratories for some types of staff ‘s technical qualification (for example, the qualification of personnel assigned to non-destructive tests, or operations in the medical-health sector).

The laboratories must therefore familiarize themselves with the terminology introduced by the GDPR and set up appropriate procedures to guarantee the management of personal data on a par with what has been done so far for the technical data.

Some GDPR terms

While recommending a complete reading of GDPR article 4 "Definitions", we report below some key words that the laboratories must know and that will help us to understand the meaning of the following text:

Abstract from GDPR Article 4 “Definitions”:

(1) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

…

(7) ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union

or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

…

(11) ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

(12) ‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

…

Main focus

GDPR establishes a series of rules that must necessarily be adapted to the individual needs of a company that must implement them. There is no such thing as a line of behaviour valid for all realities. There are however two main themes that must be followed by everyone, including laboratories:

- information: the GDPR pays great attention to the concept of information that the controller must provide to the data subject. It is also necessary in many cases to obtain from the data subject an explicit "consent" for the use of personal data for the specific purposes for which they are collected.

- data protection: once the data are collected it is essential to protect them in such a way that the possibility of unauthorized use, loss or theft of the data is reduced to a minimum.

Let's see in detail, below, how to implement in practice the two themes mentioned above.

Information

In short, the GDPR establishes that personal data must be processed for a specific purpose and for a defined period. The aforementioned basic information (purpose and duration of processing) must therefore be specified in a written document called "privacy notice".

Based on the type of data requested, it may be necessary to obtain the consent of the data subject.

The purposes of data collection, of course, can be manifold: work contracts, commercial contracts, marketing, newsletters, sending of documentation. It is therefore possible to draw up, within the same privacy notice, a list of purposes for which the data subject can provide or not give his consent.

Likewise, the treatment period may have a variable duration or be determined as a result of other events; example: until the completion of an activity, a period of time after the closing of a contract, ...

The notice and consent can be made known / collected by any means (paper, web, mail, automatic systems, ...) provided that the data subject who has given consent and the date / time of issue is clearly identifiable.

All consents must be kept available to the national privacy authority.

Data protection

Data protection goes through various topics and different operating modes that are not easy to understand for those who are unfamiliar with IT systems.

A possible solution to dissect the issue, identify any gaps in IT systems and proceed to their safety, can be represented by a careful risks analysis and the subsequent preparation of a disaster recovery procedure.

Let's look at some of the key topics to be considered in a risk analysis below.

Data confidentiality

The personal data being processed must be kept in such a way as to minimize the risks of illegal access, destruction or loss through appropriate security measures, i.e. through all the technical and organizational measures that the laboratory can put into practice to guarantee protection, privacy and confidentiality.

If the Controller chooses to use electronic devices or computer programs for data management, it must provide for controlled access through authorization levels and ensure that no processing contrary to the law or different from those for which the data were collected.

In particular, the Controller must adopt specific criteria and procedures dictated by GDPR Article 33, such as the use of an identifying username and password to access data, the use of antivirus software and for periodic data backup.

Security measures

The processing of personal data by electronic means is allowed only if specific minimum measures are adopted, among which are identified:

- ✓ computer authentication;
- ✓ adoption of procedures for managing authentication credentials;
- ✓ use of an authorization system;
- ✓ protection of electronic tools and data with regard to the unlawful processing of data and unauthorized access;
- ✓ adoption of procedures for the custody of security copies;
- ✓ adoption of encryption techniques or identification codes for certain data processing suitable for revealing the health or sexual life of health organizations.

For sensitive and judicial data, further measures are planned in addition to what has already been mentioned as the Security Policy Document.

GDPR Article 34 expressly provides that procedures are adopted for the construction and safekeeping of backup copies and the restoration of the availability of data and systems. In practice, the Controller, through the IT System Administrator, must provide for the production and storage of system backup copies or backup copies of the data and information contained in single electronic devices.

The cause of data and information loss may depend on:

- ✓ destructive events, natural or artificial;
- ✓ system failures;
- ✓ malfunctions or degradation of electronic components;
- ✓ carelessness or inattention.

The risk of data loss can be represented by:

- ✓ unfair and fraudulent behaviour;
- ✓ computer viruses;
- ✓ theft of mobile devices containing data.

In these situations, a backup can limit the loss of stored information. Also in this case, however, the data entered in the backups must be kept and protected from unwanted access by means of procedures that inhibit the reading of the data contained therein, perhaps using a cryptographic application.

If a data storage server is used, it must be connected to an uninterruptible power supply that allows data loss due to voltage fluctuations or power failure.

In case of data loss, it is necessary to promptly adopt every possible data recovery procedure.

Digital signature

The digital signature allows the exchange of digital documents having legal validity because it allows verification of the identity of the sender, makes it impossible for the sender to disregard a signed document, makes it impossible for the recipient to modify a document signed by someone else.

From a technical point of view, the digital signature is a sequence of bytes able to univocally associate an electronic document with the person who generated it, guaranteeing its origin, authenticity and integrity.

Systems security

The law provides that the processing of personal data by electronic means is allowed to persons who have been trained and have been provided with specific authorization profiles, in order to limit access to the data strictly required for carrying out assigned processing operations. Periodically, and in any case annually, it is necessary to verify the existence of the conditions for the conservation of authorization profiles.

Personal data must also be protected from the risk of external intrusion and from the action of programs that can violate privacy. For this reason, suitable electronic tools must be set up to prevent the vulnerability of the systems and correct any defects, such as antivirus, antispyware and firewalls, to be updated at least every six months.

At least once a year it is necessary to update the systems in order to correct errors. This operation can be easily accomplished also by downloading patches or service packs from the Internet, i.e. new versions of the operating systems and the various application programs.

Password management

The parties authorized to access the systems can do so if they have authentication credentials that consist of a code associated to the person in charge and a confidential and secret keyword, known only by the person in charge, or with the use of individual smart cards. The code associated to the entrant or the user-id or user-name, once used, can not be assigned to other subjects, even at different times.

Employees must be made aware of the necessary precautions to ensure the secrecy of the keyword and the diligent custody of the devices in exclusive use of the person in charge and not to leave the electronic instrument unattended and accessible during a treatment session (the systems, for this purpose) , allow to set up a screen saver with password request).

It is a good idea to deactivate unused authentication credentials after a certain period of time (example 6 months).

Security of paper archives

Particular importance is given to paper archives, especially in cases where sensitive data relating to employees, information concerning disciplinary proceedings, judicial data relating to tenders or information related to commercial transactions, such as invoices or contracts, are contained within them.

The controllers must be given specific written instructions that provide for the custody of documents and documents. Access to archives containing sensitive or judicial data must be allowed only to personnel who have been expressly trained and authorized and must be checked. Therefore, it is necessary to adopt policies aimed at managing the paper data contained in the archives. In this case it is necessary to check the accesses of workers, previously authorized, in the rooms where these databases are kept. This operation can be performed by installing a badge reader that allows recognition of the authorized subject and allows access.

End of treatment

It is essential to define the methods for managing personal data at the end of the treatment period.

Taking into account the type of data processed it may be necessary to define different methods, also referring to the same data subject, for different purposes; let's see some examples:

at the time of the resignation of an employee, some types of personal data (company email address, access to information systems, emergency references of family members, etc.) can be immediately cancelled or anonymized, while other types of data may be deleted or made anonymous within a certain period of time (home address, personal telephone number, ...) and some other data, such as the name and surname and data related to the technical qualifications of the personnel who have signed a test report must be maintained over a very long period of time (10 years or more).

In any case, upon expiration of the deadlines set by the regulations in force and contained in the privacy notice, personal data must be made unavailable for elaboration and for consultations. Therefore, the information contained in the databases and in the supports for the creation of backup copies (backup or other means of disaster recovery) will have to be erased or made anonymous too.