INSTRUCTIONS FOR PERSONS AUTHORISED TO PROCESS PERSONAL DATA

This document contains the instructions that the Veneto Oncology Institute - IRCCS, as data controller of the processing of personal data (hereinafter, the "Controller"), gives to persons authorised to carry out processing operations under its authority.

Processing operations.

In order to avoid risks of unauthorised or prohibited access, loss, destruction or damage of data (even accidental), the persons authorised to process personal data must comply with all the provisions and security measures that are set out below.

1) Check and keep the electronic tools used for data processing and documents containing personal data, of which you are aware or in possession for the performance of the activities and tasks assigned, in such a way as to prevent access to unauthorised persons or prohibited processing.

2) Carefully manage authentication credentials according to the specific procedures and operating instructions provided by the company manuals and documents, also complying with the following provisions:

   a) use the identification code (user-id) and the reserved password assigned to access the data processed by electronic means and keep them diligently, guaranteeing their secrecy;
   b) the password must consist of a sequence of at least eight characters (normal and special) both numeric and alphabetic (or, if the program in use does not allow it, the maximum number of characters permitted);
   c) when generating the password, the utmost attention must be paid not to use elements or information that can be easily traced back to the user. Therefore, for example, references to: first name and surname, date of birth, registration number, name of family members, home or office telephone number, known nicknames, as well as names of famous people, etc. must be avoided;
   d) the password must be changed on first use and every time it is requested by the system (at most: 6 months for personal data and 3 months for particular data[1]) or whenever it is suspected that their secrecy may have been compromised. When generating the new password, no previously used character sequences must be used;
   e) the password must remain absolutely confidential. For this purpose, typing in the presence of third parties must be avoided and storage in a place not accessible to others is essential (the affixing of post-its or stickers containing references to the password on the screen-terminal must therefore be absolutely avoided). The use of automatic password entry systems (e.g. macro or function key preparation) should also be avoided;
   f) the password cannot be communicated, for any reason, to colleagues in own or other offices.

3) In all cases of absence, even temporary, from the workstation (e.g.: lunch break), it is necessary to lock your work session. This precaution must above all be adopted in the case of use by more than one authorised person of the same workstation.

4) All persons authorised to process data must actively participate in any training sessions on privacy organised by the Data Controller and must report to the manager of the area/office to which they are assigned or, failing that, to the appointed privacy delegate or to the legal representative any and all anomalies found in the exercise of their activity.

[1]These are the following categories of data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data intended to uniquely identify a natural person, data relating to the health or sexual life or sexual orientation of the person (art. 9 of the GDPR).

5) The processing of data contained in paper-based deeds and documents must be carried out always guaranteeing correct keeping of the same. The documents cannot, therefore, be left unattended on one's desk and/or in places open to the public in the absence of other authorised persons involved in the same processing; they must not be consulted by other authorised subjects who are not authorised to perform processing; they cannot be reproduced or photocopied except for needs related to the purpose of the processing; they cannot be taken off the premises identified for their storage except in very exceptional cases and, if this happens, the removal must be reduced to the minimum time necessary to perform the processing operations. At the end of working hours, the person authorised to process must also return all paper-based documents containing personal data to the premises identified for their storage.

6) If it is necessary to destroy paper-based documents containing personal data, these must be destroyed using appropriate "document shredders" or, in their absence, they must be shredded so that they can no longer be reassembled.

7) It is forbidden to communicate personal data by telephone if it is uncertain that the recipient is a person authorised to process the personal data in question.

8) In all cases in which a printer shared by various users located outside the premises where the single workstation is located is used, printing operations can only be carried out after checking the absence, at the premises where the printer is located, of subjects not authorised to process. The print-outs must be collected immediately and kept in the manner described in the previous sections.

9) It is absolutely forbidden to enter areas with limited access, unless with the express authorisation of the relative manager.

10) If any particular categories of personal data and/or personal data relating to criminal convictions and offences are processed, each person authorised to process is also required to:

    a) keep all the removable media on which any particular categories of personal data and personal data relating to criminal convictions and offences are stored (USB pen drive, DVD ROM, CD ROM, etc.) in order to avoid unauthorised access and processing;
    b) destroy the afore-mentioned removable media at the end of their use, or permanently delete the information recorded therein before their reuse;
    c) keep documents containing details of personal data and personal data relating to criminal convictions and crimes in locked archives and limiting access only to persons previously authorised;
    d) return the documents containing such data at the end of the processing operations to the persons assigned to the relative filing.

Response to requests for the exercise of rights.

1) The person authorised for processing who receives the request must immediately notify (and in any case within the same day) the manager of the area/office to which they assigned or, failing that, the privacy delegate possibly appointed or the legal representative.

2) The person in charge of the reference structure/office or, failing that, the privacy delegate possibly appointed or the legal representative, has the following obligations, which they will possibly observe with the collaboration of the authorised person who received the request:
    a. ascertain the admissibility of the request;
    b. if there are reasonable doubts about the identity of the natural person submitting the request, further information must be requested to confirm the identity of the data subject, in particular by requesting the production of an identity document of the applicant or the transmission of a copy of the same, unless it is a person already known;

c. in the case of a request presented by a third party on behalf of the data subject, acquire a copy of the proxy or power of attorney signed by the data subject, which must be presented together with a copy of an identity document of the data subject and a copy of an identity document of the delegate;
d. once the steps described above have been successfully completed, verify the processing of personal data subject to the request in order to process it promptly. In particular, in case of exercising the right of access, it will be necessary to identify the personal data requested in the electronic and/or paper-based archives of interest, extrapolate them and insert a copy on a specific electronic or paper-based medium and, if necessary, to send them to the data subject to the address indicated by the same in a manner that ensures adequate documentation of such sending and, if possible, of receipt by the data subject. In relation to the exercise of the other rights it will be necessary to proceed in the following manner: if the request is well founded, clear and specific attestation of the intervention carried out must be given *(e.g.: confirmation of correction or deletion of the disputed data*); otherwise, the reasons for which it was not possible to respond must be acknowledged.

General indications:
- the request must be answered within one month, which in particularly complex cases may be extended for a maximum of two more months: within one month of receipt of the request, the data subject must in any case receive a response;
- if the request is inadmissible or unfounded, the sender must be informed of the reasons for the non-compliance and of the possibility to lodge a complaint with a supervisory authority or to propose a judicial appeal: this communication must be sent without delay and in any case within one month of receipt. of the request;
- the exercise of rights is generally free: in the event of manifestly unfounded, excessive or repetitive requests, however, the amount of the contribution to be requested can be established due to the complexity of the response; furthermore, if additional copies of the personal data being processed are requested, a reasonable fee may be charged, based on the administrative costs incurred.

Last updated: 12.09.2019