FONDAZIONE BRUNO KESSLER

Instructions for the processing of personal data

1. General instructions for all processing methods

Data processing, pursuant to articles 5 and 25 of the GDPR, must comply with the principle of "minimization" (once defined as "of relevance and non-excess"), i.e. the restriction of the quantity of personal data processed, the processing operations, the disclosure time window, the conservation of the data, the purposes of the processing.

Therefore, access is allowed only to those data that are strictly necessary to complete the tasks assigned.

Personal data must be processed in a lawful, appropriate and transparent manner, and be correct and up-to-date.

The person authorized for the processing (hereinafter, the "Authorized Processor"), when performing processing operations, is required to:

- ascertain that the privacy policy, complete in all its parts, is delivered to the party concerned pursuant to art. 13 and 14 of the GDPR and verify that each particular processing operation contained therein (for example, sharing, disclosing, or profiling) is true and complies with the provisions of law and regulations;
- allow the exercise of the rights and powers provided for in Chapter III of the GDPR (right to access, right to rectification, right to erasure, right to restriction, right to object, right to human intervention and appeal in case of decision based exclusively on automated processing, right to access the basic contents of the joint Data Controller agreement);
- share, communicate and/or send personal data on the "*need to know*" principle basis, i.e. only to internal users who need them for performing their duties;
- not to transmit to third parties information about personal data processed: communication and disclosure is allowed only if it is functional to the performance of the tasks assigned or in compliance with regulatory obligations, and with the authorization of the internal data processor;
- ascertain the identity of the data subject before providing information about his/her personal data or the related processing performed (limited to verifying the identification document without having to keep a copy);
- store in locked cabinets any storage devices or documents - even if not final (drafts) - containing personal data at the end of the processing period;
- do not leave prints of documents containing personal data unattended at the photocopiers;
- use the appropriate paper shredders when there is the need to destroy documents containing personal data. When such tools are not available, tear or cut into strips the documents so that they cannot be recreated;
- keep processed personal data for a period of time not exceeding that necessary for the purposes for which they were collected and processed, in compliance with the terms provided for by law;
- lower the tone of voice in the conversations and adopt an adequate distance (so-called "courtesy distance") in order to avoid that third parties can, even involuntarily, process personal data and/or professional information;
- for any concerns regarding the processing of personal data, contact the Internal Data Processor and/or the Corruption Prevention, Transparency and Privacy Unit;
- immediately report any anomalies, incidents, thefts, accidental losses of data affecting the processing of personal data to the Internal Data Processor, in order to initiate - through the Data Protection Officer - the procedure for the communication of the Data Breach to the Data Protection Authority and to the parties concerned;
- fulfil the confidentiality obligation also in the period following the termination, if applicable, of the activities carried out on behalf of the Foundation.

It is recalled hereby that the consultation of the data contained in the databases does not allow any form of data sharing, disclosing and further processing that is not strictly necessary and functional to the fulfillment of the tasks and functions assigned. Even when data are "public", namely accessible to anyone, Authorized Processors are not allowed to share or disclose them.

With regard to document flows between the organizational structures of the Foundation, Authorized Processors must adopt suitable organizational measures to protect the confidentiality of personal data (e.g. sending documents in closed envelopes).

FONDAZIONE BRUNO KESSLER

Instructions for the processing of personal data

2. General instructions for IT systems based data processing

With regard data searches and other processing steps performed by means of IT tools, the Authorized Processor will have a strictly personal login credential to access data.

The Authorized Processor will:

- not share his/her login credentials with other Users, except for the cases expressly allowed;
- not access services that are not permitted;
- not attempt to obtain System Administrator privileges;
- verify that the devices used are virus-free;
- not connect devices that allow uncontrollable access to the Foundation's network devices;
- store work-related data on the FBK server or on Google Team Drive;
- erase all personal data from any storage devices (disks, USB flash drives, etc.) before reusing them; if this is not possible, the latter must be destroyed.

All tools must be locked and password protected if left unattended.

3. General instructions to be followed in case guests or contractors are present

In case of presence of guests or contractor staff, the Authorized Processor is required to:

- have guests or contractors wait in areas where confidential information or personal data are not present, lowering the tone of voice and/or closing the doors in case of verbal or telephone communications;
- avoid walking away from his/her desk;
- store documents containing personal data and start the screen saver on his/her PC;
- keep his/her login credentials secret and properly stored, in compliance with the security measures set forth in the FBK Privacy Policy;
- refrain from revealing or having his/her password entered even by technical assistance staff;
- report any anomaly to your Internal Data Processor.

4. Specific instructions for the processing of particular categories of data (as per article 9 of the GDPR) and data relating to criminal convictions and offenses (as per article 10 of the GDPR)

Without prejudice to the foregoing, for the processing of personal data referred to in this paragraph the following additional instructions are prescribed:

- do not provide such personal data by telephone when not absolutely certain about the identity of the recipient;
- avoid faxing documents containing such data when other identifying information is present: in this case it is preferable to send the documentation without explicit reference to the party concerned (for example, by simply marking the documents with a code);
- replace the name of the Data Subject with a code and keep the "name - code" association in a separate archive, which access is limited to a small number of Authorized processors (so called "pseudonymization");
- do not leave the documents - including not final ones - or any devices containing such data unattended and keep them in furniture fitted with a lock, whose keys must be properly stored;
- keep documents containing data on health, sex life and sexual orientation in the aforementioned lockable containers, separately from any other document;
- request - based on the specific needs and purposes of the processing - the self-certification of criminal records or the certificate of pending charges exclusively to the subjects identified in the FBK Three-year Plan of Corruption Prevention and Transparency or in the Procurement Code.

These instructions integrate the elements of evaluation of the worker's conduct. The violation of the prescriptions contained herein can result, in addition to criminal and civil liability, in disciplinary sanctions, based on the seriousness of the conduct.