FONDAZIONE
BRUNO KESSLER

Privacy Regulations
of Fondazione Bruno Kessler

Processing of personal and corporate data, use of ICT tools and systems.

Approved with Resolution No. 15/17 dated December 20, 2017 of the Board of Directors

This document replaces and integrates the previous Policy on the Use of IT Systems in its latest version update of May 17, 2013

Amended with Resolution No. 08/19 dated January 29, 2019 of the Board of Directors

Amended with Resolution No. 28/22 dated November 18, 2022 of the Board of Directors

(version effective from January 1st, 2023)

TABLE OF CONTENTS

I. INTRODUCTION

1. PRELIMINARY REMARKS

Preserving the confidentiality, integrity and availability of data and information to protect the dignity of individuals, fundamental freedoms and the value of the Foundation's intellectual capital.

Making sure that the computer and telecommunication resources made available by Fondazione Bruno Kessler are used correctly to protect the security of the information processed and the integrity of the Foundation itself.

These are the objective of these Regulations, which are part of the general regulation on Privacy, and of the regulatory system that governs the organization, processes and functions of the Foundation.

2. CONTEXT

Fondazione Bruno Kessler actively supports the ongoing digital and ecological transition and is fully involved in the changes needed to ensure inclusive and sustainable forms of development.

With this in mind, favoring a fluid approach to organizational and operational systems, the Foundation is committed to ensuring and promoting a working environment and infosphere based on the protection of integrity and respect for the principles of lawfulness, fairness and transparency.

3. PROTECTION OF WORKERS

The Foundation ensures the protection of the fundamental rights and freedoms of all employees and collaborators also by ensuring and promoting all reasonable forms of protection of their sphere of confidentiality.

4. SCOPE, RECIPIENTS AND OVERSIGHT

In view of the organizational and operational peculiarities of the Foundation, the contents of these Regulations, while looking at the Provisions of the Data Protection Authority, detail, specify and integrate the provisions of European Regulation No. 2016/679 - General Data Protection Regulation ("GDPR"), Legislative Decree No. 196/2003 - Code on the Protection of Personal Data ("Code") as novated and integrated by Legislative Decree No. 101/2018 - Provisions for the adaptation of national legislation to the GDPR. The recipients of these Regulations are:

A. Internal users:
   - Members of the statutory bodies and other bodies
   - employees
   - in-house consultants
   - leased imployees
   - Staff assigned to FBK premises
   - Province employees assigned to work at FBK premises
   - Occasional consultants
   - Affiliates (High profiles, Affiliated fellows, Visiting fellows, PhD students, Scholars, High School interns).

B. External users:
   - Staff, in any capacity, of contractors providing supplies, services, or works for FBK and their employees or collaborators
   - Staff of other organizations present at FBK due to MoUs or inter-institutional agreements
   - Various visitors and guests.

The responsibility of overseeing the proper compliance with the provisions of these Regulations, and within the limits of their respective competencies and functional responsibilities, lies with the Corruption Prevention, Transparency and Privacy Unit, the IT Infrastructure Service as well as, with a more advisory support-oriented role, with the Data Protection Officer (DPO).

II. DEFINITIONS

5. PRIVACY RELATED DEFINITIONS

Please see the main definitions concerning privacy and data protection below.

Personal data: any information that identifies a natural person or makes him/her identifiable and that may provide details as to their physical, physiological, genetic, mental characteristics, their habits, life style, personal relationships, their health conditions or economic status.

Identifying data: personal data that allow the identification of a natural person.

Special data: personal data suitable for revealing the state of health (relating to physical or mental health, including the provision of health care services) and sexual life, racial and ethnic origin, religious beliefs, philosophical or other beliefs, political opinions, membership in parties, trade unions, religious or philosophical associations, political or trade union organizations of a natural person. Genetic data (personal data relating to the inherited or acquired genetic characteristics of a natural person that provide unambiguous information about his or her physiology or health and that result from the analysis of a biological sample of him or her) and biometric data (personal data obtained by specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person and that enable or confirm his or her unambiguous identification, such as facial image or dactyloscopic data) are also part of special data.

Judicial data: data suitable for the collection of information regarding measures relating to criminal records, the register of administrative penalties related to the offense and the related pending charges, or the status of defendant or suspect in accordance with articles 60 and 61 of the criminal procedure code.

Risky data: personal data other than special and judicial data that present specific risks to the fundamental rights and freedoms, as well as to the dignity of a natural person, in relation to the nature of the data or the manner in which it is processed or the effects it may have (e.g., data identifying behavior, interests, choices, purchases, and movements).

Processing of personal data: any operation performed with or without the use of automated processes and applied to personal data, or sets of personal data, such as collection, registration, organization, structuring, storage, adaptation, the modification, extraction, consultation, use, communication by transmission, diffusion or any other form of making available, comparison or interconnection, limitation, cancellation or destruction.

Profiling: any form of automated processing of personal data consisting of the use of such data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects of professional performance, economic situation, health, personal preferences, interests, reliability, behavior, location or movement of that natural person.

Anonymization: a process by which personal data are irreversibly changed so that the Data Controller, alone or in collaboration with other parties, can no longer directly or indirectly identify a natural person.

Pseudonymization: processing of personal data in such a way that personal data can no longer be attributed to a specific individual without the use of additional information, provided that such additional information is stored separately and subject to technical and organizational measures to ensure that such personal data are not attributed to an identified or identifiable natural person.

Disclosure of personal data: giving knowledge of personal data to one or more specific Users other than the data subject, on the basis of a specific purpose and a certain and safe method of processing, including by making available or consulting them.

Dissemination of personal data: giving knowledge of personal data to indeterminate Users, in any form, including by making available or consulting them.

Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Accountability: a cardinal principle of the GDPR according to which the Data Controller has the overall responsibility and the burden of adopting proactive behaviors and such as to demonstrate the concrete adoption of measures aimed at ensuring the application of the GDPR on any processing of personal data performed directly or carried out by others on its behalf.

6. PRIVACY FIGURES RELATED DEFINITIONS

Please see the definitions concerning privacy figures below.

Data Subject: is the individual whom personal data is about

Data Controller: The Foundation as a whole, in the person of its Legal Representative who exercises completely independent decision-making power over the purposes and methods of processing, including the security profile. The Board of Directors may entrust functions of coordination of all tasks related to the processing of personal data on behalf of the Data Controller to an Internal Data Processor, through special power of attorney for the representation of the Foundation granted by the President.

Joint Controller: Data Controller who jointly determines the purposes and means of processing with another Controller in a transparent manner and through an internal agreement, the respective responsibilities regarding compliance with the obligations deriving from the GDPR.

External Data Processor: natural or legal person, public authority, service or other body that processes personal data on behalf of the Data Controller. The External Data Processor must provide sufficient guarantees to put in place suitable technical and organizational measures so that the processing meet the requirements of the GDPR and guarantee the protection of the rights of the data Subject.

External Sub-Processor: a natural or legal person, public authority, service or other body to which a Data Processor recurs for the execution of specific processing activities on behalf of the Data Controller;

Internal Data Processor: User, within the Foundation, who is entrusted with the responsibility for the processing of personal data attributable to his/her relevant area of concern. This User coincides with a Head of organizational articulation or organizational sub-articulation, Center, Unit, Service, Directorate...). In the case of research projects involving more than one organizational articulation, the Internal Data Processor(s) is identified as the Center Director(s).

Authorized Data Processor: User, within the Foundation, authorized to perform data processing operations on the basis of the regulations adopted by the Data Controller and the instructions given by the Data Processor and/or by the Internal Data Processor.

System Administrator: natural or legal person appointed by the Controller and responsible for the management and security of information systems through the application of the necessary measures to maintain the confidentiality, availability and integrity of the personal data processed.

Independent Administrator of FBK-owned tools and services: a natural person, within the Foundation, who autonomously manages ICT tools and services owned by the Foundation and who provides sufficient guarantees to put in place suitable technical and organizational measures so that the processing meets the requirements of the GDPR and ensures the protection of the rights of the data Subject and data of which FBK is the Controller.

Data Protection Officer (DPO): a natural person appointed by the Controller who, pursuant to art. 37-39 of the aforementioned GDPR, operating independently from the organization, advises the Controller regarding obligations, requirements and regulatory developments, carries out internal audits on the correct application of the regulatory provisions and the privacy management system defined by the Controller, assists the Controller with the privacy impact assessment and risk analysis, and represents the point of contact for data Subjects and Data Protection Authority.

7. ICT RELATED DEFINITIONS

The following are some other definitions useful for the correct management of the processing of personal data.

Account: an identity created for a person in a computer or computer system

Application: (software application, or application, or app for short): a computer program designed to perform a specific task other than that related to the operation of the computer itself.

Badge: card with electronic identification chip.

Public Cloud: data storage model on networked computers where the data is stored on multiple virtual servers generally hosted at third-party facilities or on dedicated servers.

Data Center: a limited-access area hosting servers, computing systems and networking devices, as well as storage systems on which data are stored.

Infrastructure: set of information technology (IT) components that underlie an IT service; typically physical components (computers and hardware and network facilities), but also various software and network components.

Infostructure: infrastructure specifically dedicated to communication**.**

Pass: paper card without identification.

IT Services: information technology services, such as, for example, e-mail, document servers, applications, connection to systems and the Internet, and in general all those services designed to store, process, convert, protect, transmit, and retrieve information.

System or Machine: computer, or set of computers, which includes the hardware, operating system (main software), an application, and peripheral equipment necessary and used for operation.

ICT tools: printers, laptops, desktop computers, landlines, smartphones, tablets, e-book readers, IP cameras, and, in general, any device that can connect to an IP network.

III. ORGANIZATIONAL MODEL

8. INFORMATION CLASSIFICATION

FBK's information assets (consisting of all the data and information processed in the various processes, including personal data) can be classified according to the following criteria:

Public data and information: this information is freely traceable by Users through the means of communication made available by FBK (website, publications, press releases, etc.). This information does not require particular attention to confidentiality from the User. Disclosure of this information has no implications for FBK as it is public information that can be disseminated.

Internal data and information: this is information that can be processed by Users exclusively within the FBK processes and organizational context through the institutional channels made available by FBK (e-mail, intranet, website, areas of exchange on servers and computers, etc.). This information requires the User to pay special attention to the processing, as its disclosure is a violation of the confidentiality constraints to which each User is bound with a possible legal impact (e.g., breach of privacy), unless it is revised so that it is reclassified as public.

Confidential data and information: this is information that can be processed by groups of Users authorized by virtue of the role and a specific processing purpose identified by the Data Controller or the Data Processor. Such information must be disclosed only to entitled Users, evaluating the most appropriate communication tool made available by FBK as their dissemination can have a major legal (e.g. breach of privacy), image and competitiveness impact for FBK.

Strictly confidential data and information: it is information that can only be processed by certain Users based on the role and responsibilities covered in FBK. Disclosure of such information may result in serious legal (e.g. breach of privacy), image and competitiveness damage to FBK.

9. LIABILITY FOR PRIVACY ISSUES

In compliance with the GDPR and in line with its general principle of Accountability, FBK has defined, formalized, and applied an Organizational Model of privacy related liability aimed at the correct processing of personal data. The model is in line with the Foundation's organizational chart.

On the occasion of the annual update of the general organization chart, the Foundation, in its capacity as Personal Data Controller, also updates the line of internal responsibilities regarding the processing of personal data by identifying in the Managers of organizational articulations, and sub-articulations (Centers, Units, Services, Divisions, etc., the Internal Data Processors for personal data relating to processes of their concern solely. These Users are formally appointed after receiving specific training.

All those who are in charge of a project that involves the processing of personal data and have not been included in the Privacy-related Liability Organizational Model - are required to adopt an ad hoc policy tailored on the specific needs of the case (so-called Privacy by Design). These Users shall adopt the above policy in agreement with the Data Controller and through the Corruption Prevention, Transparency and Privacy Unit including as well the Data Protection Officer.

10. FBK AS EXTERNAL DATA PROCESSOR

By virtue of the stipulation of contracts, agreements, projects with external parties, the Foundation can be appointed as "External Data Processor pursuant to Article 28 of the GDPR" when it is entrusted with specific tasks, which involve personal data processing for the specific purposes of a subcontractor (which is the Data Controller therof).

In all these cases, the Foundation - even when signing the aforementioned deeds – shall identify the Internal Data Processor and ensure that appropriate technical and organizational measures are taken to meet the requirements of the GDPR.

11. RECORD OF PROCESSING ACTIVITIES

The Record of Processing activities is a document for the recording and analysis of the processing activities performed by the Data Controller. The Record must be promptly completed and kept constantly updated by each Internal Data Processor as its content must always reflect the effective processing activities performed. Any change, in particular in relation to the methods, purposes, categories of data, categories of data Subjects, must be immediately reported in the Record, and provide the reason for the changes occurred.

12. SYSTEM ADMINISTRATORS

In accordance with the Provisions of the Data Protection Authority, the Foundation identifies the "System Administrator" figures in relation to the types of Networks (indicated in Article 25 of these Regulations) on which the administered systems are present, carefully evaluating the granularity of the different authorizations.

These different figures are as follows:

a. **Administrator of centrally-managed Systems** in type "a" networks and all systems in type "d" networks: IT Infrastructure Service and FBK Digital Unit internal officers.

b. **Administrator of research-managed Systems** in type "b" and "c" networks: internal researcher identified by the Center Director.

c. **Independent Administrator of FBK-owned tools and services** in type "a" networks: internal individual authorized by the immediate Supervisor and the Head of the IT Infrastructure Service (see Chapter V of these Regulations).

The IT Infrastructure Service, in collaboration with the FBK Digital Unit, provides an annual census of centrally managed systems, applications, and services and verifies the census of those managed by entities in the research sector independently for scientific and/or project reasons.

Each Center Director annually takes a census of systems, applications, and services managed by his or her Research Center and, obligatorily, shares the findings with the IT Infrastructure Service.

Each system, machine, application and service of the Foundation must be linked to a "System Administrator," as well as to evidence of the related processing of personal data.

System Administrators are formally appointed by the Data Controller upon completion of mandatory training.

IV. ACCEPTABLE PRACTICES POLICY

13. PROCESSING MAIN PRINCIPLES

Personal data processing is any operation or set of operations performed on a personal data including those carried out without the aid of electronic tools. The processing of personal data, to be lawful, accurate and transparent must always take place according to some general privacy principles. In particular, when processing personal data, users are required to observe the following general principles:

a. **Lawfulness, accuracy and transparency**: personal data must be processed in a lawful, accurate and transparent way, in order to guarantee to the Data Subject adequate security, including protection, through appropriate technical and organizational measures, from unauthorized or unlawful processing and from accidental loss, destruction or damage. With regard to transparency, all information intended for the public or to the Data Subject must be concise, easily accessible and easily understood; the language used must be found simple and clear.

b. **Purpose limitation**: the purposes of the processing must be certain, explicit and legitimate; subsequent processings should not be found incompatible with such purposes. Exceptions shall be granted for further processing for archiving purposes in the public interest or for scientific or historical research purposes, or for statistical purposes.

c. **Data minimization**: the data collected must be adequate, relevant and limited to what is necessary with respect to the purposes for which they are processed. Specifically, information systems and computer programs must be configured by minimizing the use of personal data, so as to exclude their processing when the purposes pursued in individual cases can be achieved through anonymous data or other appropriate ways to identify the data Subject only in case of necessity ('necessity principle').

d. **Accuracy:** the data processed must be accurate and, if necessary, updated, therefore all reasonable steps must be taken to delete or edit inaccurate data in relation to the purposes for which they are processed

e. **Retention limit**: the data processed must be stored in a form that allows identification of the data Subject for a period not longer than the necessary to achieve the purposes for which they are collected and processed unless specific law providing for archiving processing in the public interest or for scientific or historical research purposes, or for statistical purposes.

f. **Integrity and confidentiality**: the data must be processed in such a way as to guarantee adequate security of personal data. Adequate security is achieved when, by means of appropriate technical and organizational actions, personal data are protected from unauthorized or unlawful processing, loss, destruction and accidental damage.

14. PROCESSING OF PERSONAL DATA FOR STATISTICAL AND RESEARCH PURPOSES

Study and research are important ways to broaden the boundaries of knowledge, foster the growth of individuals' personalities and enable social progress.

To ensure these purposes, the regulations governing the processing of personal data include simplified measures in the field of historical, scientific and statistical research. However, the latter do not exempt the Data Controller from adopting suitable measures to prevent possible violations of the rights of the data Subjects. In fact, the informed consent forms that are provided to the data Subjects, shall clearly explain and disclose the aims pursued by the statistical or research investigation.

Personal data processed for statistical and scientific research purposes cannot be used to make decisions or provisions concerning the data Subject, nor for processing for other purposes. They are stored separately from any other personal data processed for purposes that do not require their use.

The provisions, relating to the statistical secrecy and confidentiality of personal data, do not apply to data from public records, lists, deeds or documents that can be accessed by anyone.

In order to promote and support research and collaboration in the cultural, scientific and statistical fields, the Foundation – excluding particular and judicial data - can disclose and disseminate data related to study and research activities.

Personal data must be kept for as long as is strictly necessary to achieve the purposes for which they were collected and in any case no longer than 5 years after project reporting. After that time, they must be permanently anonymized or deleted by the research staff.

The Foundation's research staff is required to standardize its research and study activities to the ethical rules promoted by the Data Protection Authority[1] and that can be found in the Annex to the Foundation's Code of Conduct.

15. PUBLICATION OF DEEDS AND DOCUMENTS AND THE RIGHT TO PERSONAL DATA PROTECTION

In relation to administrative transparency obligations, the Foundation guarantees the right to confidentiality of personal data (primarily special data and judicial data) wherever possible through the non-direct identifiability of the individuals to whom such data refer or through their obscuration.

16. ACCESS RIGHT VS PROTECTION OF PERSONAL DATA

The conditions, procedures, limits for the exercise of the right to access administrative documents containing personal data and the relative judicial protection are governed by Law 241/1990 as amended and integrated. and by the other regulatory provisions on the Subject, as well as the legislation on transparency governing the right of access, including for what concerns particular and judicial data and processing operations, executable in fulfillment of an access request. The activities aimed at applying this regulation are considered to be of significant public interest.

When the processing concerns data revealing the state of health or sex life, processing is allowed, if the legally relevant situation that is intended to protect with the request for access to administrative documents is at least equal to the rights of the data Subject, i.e., it consists of a personality right or another fundamental or inviolable right or freedom.

As regards restrictions to generalized civic access deriving from the protection of personal data, please see the ANAC guidelines.

17. MANAGEMENT OF PREMISES AND PHYSICAL RESOURCES

All FBK premises and all FBK physical resources must be used and cared for with the utmost diligence in order to guarantee both an efficient working activity and an adequate level of information security.

[1] https://www.garanteprivacy.it/web/guest/home_en/italian-legislation

18. ACCESS TO RESTRICTED OFFICES AND AREAS

Premises and offices. Access to offices, protected areas, and areas reserved to paper archives is allowed to authorized Users as holders of a personal badge, based on precise and motivated work requirements.

The data relating to the transits tracked by the personal badge may be made available to the Heads of the aforesaid offices, areas and archives for purposes of security and property protection.

Further and specific access to offices and protected areas may be granted and enabled only upon a written request including reasons from the officers involved.

Visitors and guests may access the above-mentioned FBK areas only upon registration at check-in, showing the pass received at registration and if accompanied by an Internal Officer.

Data Center. Access to the FBK Data Center premises is permitted only to authorized personnel through biometric system or personal badge.

Exceptionally and for a short periods, visitors and guests can be granted access to the Data Center, provided they are authorized and accompanied by authorized FBK personnel. Visitors and guests must be adequately instructed by authorized personnel regarding the characteristics of the environment, the existing risks, the good practice standards provided for and the procedures to be implemented to prevent or manage emergencies and risks.

For safety reasons and to keep the operating temperature constant, all access gates must remain open only for the time strictly necessary for the passage of people and materials.

For security reasons, a picture is taken to anyone accessing the FBK Data Center and this image is immediately sent to authorized personnel in charge of the Data Center.

The above rules also apply to the "High availability" Data Center identified in the **Disaster Recovery site**.

19. CORRECT USE OF BADGE

Anyone operating or transiting the Foundation's premises and spaces must have an appropriate identification badge.

The badge is considered a strictly personal object; it must therefore be properly kept and cannot be lent, not even temporarily.

In case of unauthorized use, the badge may be withdrawn by the surveillance staff. In such circumstances, the Foundation may decide on further action for its protection.

In case of loss of the badge, the person or person concerned shall give prompt notice to the relevant oversight offices.

Once the prerequisites for its issuance are no longer met, the badge must be immediately returned to the appropriate Unit of the Foundation.

20. VIDEO/AUDIO RECORDINGS AND PHOTOS AT FBK PREMISES

All video/audio recordings and photographs must respect the rights of the individuals involved.

To strengthen internal safety in an organizational setting where the Foundation's offices are accessible to third parties, the personal profile image must meet certain standards and its publication is, by default, mandatory on the Foundation's personal badge and Internal Networks.

Internal Users: for reasons connected to their work activity, video/audio recordings and photographs must be authorized by the User's Supervisor. They must be used exclusively for work purposes and cannot be disclosed outside the institutional context in which they were created.

This is without prejudice to the possibility of making in-person audio-recordings necessary to assert one's right in court, for the period of time strictly necessary for the purpose, respecting in all cases the principle of proportionality and minimization, particularly in terms of space and time.

Audio-video recordings carried out for purposes of communication and enhancement of work activities (e.g., filming for the media, for project-related videos, for documentation of events) must be authorized in advance by one's Supervisor after having consulted with the Communication and External Relations Service.

Outside of these cases, taking into account that the Foundation invests in its staff, and in order to enhance the mutual trust bonds, making video-audio recordings/photos is prohibited in any area of FBK. Violations may result in the initiation of disciplinary proceedings.

Internal Users can be photographed and/or recorded at events, seminars and training sessions as well as for the documenting of institutional activities, especially research-related ones. In these cases, images and footings may be used for institutional purposes and communications.

External Users: Making video/audio recordings or taking photos in any area of FBK is prohibited. Any exceptions must be authorized by the Communication and External relations Service. The Internal User acting as the contact of an External User is required to enforce these provisions.

21. WEB CONFERENCING

Virtual meetings must be carried out with the tools made available by the Foundation (or, if necessary, with those proposed under the circumstances by users involved) and authorized by the IT Infrastructure Service, in protected situations that will ensure the protection of the information shared.

Recordings of virtual meetings are permitted – providing the reasons for doing so - only after all individuals involved have been notified.

22. WORKING STATIONS

Workstations should always be kept tidy and confidential documents and records should never be left unattended.

23. PHYSICAL MEASURES TO SAFEGUARD PAPER DOCUMENTS AND RECORDS

Paper data and paper records necessary to carry out work tasks must be kept in storage cabinets or drawers in the working context in which the User operates. Access to all archives is restricted, thus Users are allowed to access them only when needed and only to take out and put back the documents needed to carry out their tasks. The documents should be put away properly in the storage cabinets when the User steps away from the office and at the end of the working day.

Archives containing particular (former sensitive) documents and records must be kept in locked storage cabinets.

The physical elimination of any paper document or ICT support containing company and/or personal data and information must only be carried out using the appropriate tools.

It is recommended not to leave documents unattended at the printing devices.

24. MANAGEMENT AND PROTECTION OF PERSONAL AND CORPORATE DATA

All staff must consider themselves personally responsible for the data and information that they enter into possession when performing their work for the Foundation (be it in person or remotely). All staff must therefore process data and information by adopting all appropriate security measures in order to protect its confidentiality, security, integrity and correct use.

The data and information may be communicated to third parties exclusively within the scope of the User's function and according to the purposes related to his/her work.

The disclosure of data and information to third parties that may damage the image, reputation, productivity, intellectual property as well as the know-how and profitability of the Foundation or that may violate the contractual and legal obligations related to the work relationship is forbidden.

The disclosure to third parties of confidential, classified or otherwise proprietary information of the Controller is strictly prohibited. In case of breach, the Controller reserves the right to initiate the related disciplinary sanctions, as well as the civil and penal actions allowed.

Users should also be reminded that the illegal dissemination of data and information could, in addition to the violation of these Regulations, result in the violation of rules with both civil and criminal consequences against the perpetrator of illegal activity, as well as violation of the regulations governing the work relationship.

Subject to justified research needs and the specific cases covered in these Regulations, the use of encryption (cryptography) that renders business information unreadable or that may cause systems and applications to crash is prohibited.

Access to data is permitted within the limits of one's organizational function and work duties.

Network disks on local systems and in cloud services managed by FBK are strictly professional information sharing areas and cannot be used for any other purpose in any way. Therefore, any file that is not work-related cannot be stored, even for short periods, on these drives. Regular monitoring and administration tasks are carried out on these drives by authorized personnel.

Please note that disks or other storage units on devices in use by users are not subject to saving by authorized personnel. The responsibility for saving the data contained therein lies therefore with the User.

The IT Infrastructure Service may at any time proceed with the removal of any file or application that it deems to be a security risk both on the Users' IT tools and on the network drives: the individual concerned and his or her immediate supervisor will be informed of this action.

The main network servers are **backed up** by the IT Infrastructure Service, which keeps backups of the last five years. Individuals who keep FBK data in areas for which no backup is performed, are responsible for saving them and for any damage to FBK or third parties, including civil damages caused by their loss or removal.

Without prejudice to existing constraints to protect privacy for their own personnel, Users must be aware that the data they process on FBK's computer systems may be FBK's property or otherwise under FBK's responsibility. Precisely in order to ensure the security and integrity of the information on FBK's computer systems, the secrecy of the information cannot be absolutely guaranteed in the event of inspections.

Temporary storage of data on private computer tools is permitted as long as the said tools are protected so as not to allow access by unauthorized external users and the disks are encrypted.

Saving professional data and information in public cloud systems or storage that are not in the *Catalog of Cloud Services for PA credited by the Agency for Digital Italy*[2] (AGID) and not authorized by the IT Infrastructure Service is prohibited.

The use of file servers, cloud storage systems and Source Code Management (SCM) Servers is regulated by special Guidelines adopted by the Head of the IT Infrastructure Service in order to minimize the risk of damage, including civil damages, caused to FBK or third parties.

Since the Foundation deals with Public Administrations, when developing software, applications and codes that deal with personal data, it is necessary to respect and follow the guidance provided by the *Agency for Digital Italy* (AGID) about ICT security measures, following development methodologies that take into account privacy and IT security issues.

25. ICT TOOLS, SERVICES AND INFOSTRUCTURES

The ICT systems supplied, the services and infostructures to which Users have access to should be used for professional purposes.

[2] https://cloud.italia.it/marketplace/

Notwithstanding this principle, FBK authorizes a moderate and reasonable private use. This use, If and insofar as it is associated with a logic of reciprocity, must be limited and based on criteria of common sense and must not hinder professional use.

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

The instruments must be automatically turned off or put into low-power mode if not used for more than an hour, unless otherwise required by research needs.

The Foundation provides Users with dedicated logical networks and infostructures. The above Networks and infostructures are those certified by the IT Infrastructure Service according to the following logic:

a. **for peripheral computing devices**, reserved for computing devices in use by users such as PCs, phones, tablets, IoT, printers, be they owned by FBK or privately owned, be they centrally managed or self-managed, which will not be able to provide direct or indirect services outside FBK;
b. **for servers self-managed in the Data Center,** reserved for physical servers that shall not provide direct or indirect services outside FBK;
c. **for servers self-managed in Cloud,** reserved for virtual servers that may also offer direct or indirect services externally;
d. **for servers centrally-managed in the Data Center or in Cloud,** reserved for physical or virtual servers that can also provide direct or indirect services outside FBK.

System Administrators with the IT Infrastructure Service are the only individuals authorized to access IT systems connected to networks “a” and “d” with local and network Administrator or "root" privileges.

On centrally managed devices, it is not permitted to modify in any way the operating system or the applications installed by the System Administrators.

When using portable privately-owned tools for work purposes, it is mandatory to implement protection of personal or corporate data through authentication systems, disk encryption, and it is strongly recommended to use the clientless web tools provided by the Foundation for accessing FBK services, so as to avoid saving data on privately-owned devices.

Furthermore, FBK has signed a specific agreement with the Consortium of the Italian Network of Universities and Research, which manages a network commonly known as the "GARR Network". The use of IT devices is subject to compliance with the *Acceptable Use Policy* of the GARR network available at the following link*:* https://www.garr.it/it/regole-di-utilizzo-della-rete-aup.

26. CARE OF ICT TOOLS

Users should take good care of Foundation-owned IT tools, avoiding any damage that could hinder their proper functioning and avoiding leaving them unattended in public areas.

In case of theft or damage, the User should file a formal complaint with the Public Safety Authorities and send it immediately to the Corporate Assets Service, which, in coordination with the IT Infrastructure Service and the Corruption Prevention, Transparency and Privacy Unit, will activate the necessary internal procedures.

27. MANAGEMENT OF ACCESS CREDENTIALS AND PASSWORDS

The authentication credentials for access to the network and to other services are provided by the IT, Infrastructure Service and delivered to the User at the time he or she joins the organization.

Authentication credentials consist of a code identifying the User (username), associated with a reserved key (password) that can be modified by the User on first use, and must be protected with the utmost diligence and not be disclosed.

The Foundation may also configure additional mandatory access control systems (two-factor authentication, biometric authentication, etc.).

Each User is responsible for security and for any operation performed using his/her credentials.

Accessing the networks, services or infrastructures with credentials other than one's own or anonymously is prohibited.

It is forbidden to use Foundation credentials to authenticate on private services such as, for example, e-commerce sites.

Where available, it is mandatory to enable multi-factor authentication (MFA), both for credentials provided by the Foundation and for credentials used to connect to third-party services on behalf of the Foundation.

The credentialing rules expressed in this article also apply to accounts used to manage Foundation websites (e.g., Center, project, and event sites) and to manage social network accounts related to or linked to the Foundation. In particular, it is mandatory to adhere to internal policies and enable, where available, multi-factor authentication (MFA) for credentials used to connect to these services.

In case of need to renew the credentials at the end of the employment relationship, the related requests must be connected with an affiliation relationship.

28. MANAGEMENT OF ELECTRONIC MAIL

FBK grants e-mail accounts (hereinafter "FBK e-mail") to its staff for professional use. Notwithstanding this principle, FBK authorizes a moderate and reasonable private use. This use must be limited and based on criteria of common sense and must not hinder professional use. The space used for "private" purposes must therefore be limited and must not preclude and limit that dedicated to professional use.

In accordance with privacy regulations, a short text warning the recipient of the potentially confidential nature of the message is automatically added to each outgoing e-mail message.

FBK e-mail account holders are responsible for its use and must make use of e-mail in an acceptable manner.

In particular, Users must comply with the following provisions:

a. do not send or store emails and/or attachments with offensive, harassing, vulgar, blasphemous, xenophobic, racial, pornographic or otherwise inappropriate or illegal content, unless specific research needs require so;
b. pay the utmost attention when sending e-mails containing personal data, which should be adequate, relevant, and limited to what is strictly necessary for the purposes for which they are sent;
c. pay the utmost attention when forwarding e-mails containing contents and e-mail addresses of previous communications;
d. take the utmost care when sending and forwarding e-mails with attachments, which, if containing personal data, must be adequately protected;
e. pay the utmost attention to suspicious e-mails, and report them to the IT Infrastructure Service in case of concerns about their origin/content;
f. create a section called "Personal Mail" in your inbox, which the System Administrators will not be permitted to access except for serious cybersecurity reasons.

In the event of the sudden or prolonged absence of the FBK e-mail account holder, for serious cybersecurity reasons and urgent and unpostponable work needs, access to and management of the relevant mailbox may be taken over by the Foundation's System Administrators at the request of his or her Internal Data Processor.

Certified Electronic Mail (Posta Elettronica Certificata, PEC) may be used by employees in charge/authorized staff for professional purposes only.

29. INTERNET BROWSING

Internet access is provided primarily for professional purposes, to access information and content necessary for conducting work activities. All authorized Users are responsible for its correct use. As for e-mail, FBK authorizes

a moderate and reasonable private use, limited and based on criteria of common sense without hindering professional activity.

The number and duration of Internet browsing activities are constantly recorded. The consultation of these recordings can only take place anonymously and in aggregate except in the cases provided for by law and failure to comply with these Regulations. Any checks by the IT Infrastructure Service may be carried out by means of a system for analyzing log files.

Users must abide by the following Internet browsing rules:

a. it is strictly forbidden to download materials and programs in violation of copyright law, whether they are materials or programs belonging to persons or companies covered by copyright, patent or intellectual property, or materials and programs not specifically licensed.

b. it is strictly forbidden to browse sites and to download dangerous/forbidden or illegal contents (offensive, harassing, vulgar, blasphemous, xenophobic, racial, pornographic, child pornography, terrorism or otherwise inappropriate or illegal content), except for specific research needs formally authorized by the IT Infrastructure Service;

c. it is forbidden to make unauthorized copies of copyrighted material and to digitize and distribute photos from journals, books or other sources, music or video material;

d. it is forbidden to use the Foundation's technological infrastructure to procure and disseminate material in violation of the current regulations;

e. it is forbidden to carry out activities that may generate security problems or damage communications on the network;

f. it is forbidden to conduct any form of monitoring of the network that allows to capture data not expressly sent to the user host (sniffing) unless this activity is part of the user's duties and therefore formally authorized by the system administrators;

g. it is forbidden to bypass the authentication procedures or the security of any host, network, account.

30. INTERNET ACCESS FOR NON-FBK USERS

Under the conditions and with the constraints set forth in Article 29, the Foundation may, for justified reasons, allow outside parties to access and browse the Internet.

31. REMOTE ACCESS TO FBK NETWORKS

Access from outside the Foundation's network is permitted only through precise secure connection modes identified by the IT Infrastructure Service and available on the Foundation's website. Any other access is expressly prohibited.

32. COMUNICATION OF DATA AND INFORMATION THROUGH SOCIAL MEDIA

Publishing on the Internet through personal social media, forums, chats, blogs, websites, professional data and information (information, documents, notes, personal or third-party comments, photos, videos, audio, etc.) that may damage the Foundation's image, reputation, productivity or profitability, intellectual property and know-how, or that may violate the contractual and legal obligations associated with the User's employment relationship with the Foundation is strictly forbidden.

The dissemination of false information is strictly forbidden.

The disclosure of information that has already been made public by FBK is authorized; in case of any concerns in this regard, the structure of reference is the Communication and External Relations Service, which, in order to ensure the proper use of these tools by users, has drawn up a Social Media Policy and special Guidelines.

33. DIGITAL SIGNATURE USAGE

The Digital Signature must be used exclusively by the owner of the signature.

34. MONITORING SYSTEMS

In compliance with privacy regulations and for reasons that shall be unrelated to any purpose of work activity control, the Foundation may directly access all IT tools for the following reasons: computer system security or maintenance (e.g., updating, replacement, program deployment, hardware maintenance, etc.), cost control and planning (e.g., checking Internet connection costs, telephone traffic, etc.).

Periodically, and in the event of anomalies, the IT Infrastructure Service will carry out in-depth functional checks that will determine generalized notifications and warnings to the Users of the organizational function in which the anomaly has been detected and will invite the parties concerned to scrupulously follow the assigned tasks and the instructions given.

Checks on an individual basis may be performed only in case of further anomalies.

The IT Infrastructure Service also carry out non-personal network checks and on all the devices that compose it. Details of the checks carried out are available in Annex A.

In no case will prolonged, constant or indiscriminate inspections be performed.

Controls must respond to a principle of sustainability and cannot be prolonged, constant or indiscriminate.

The Foundation has the power to report to the judicial authorities all conduct contrary to the law even when detected by impersonal analysis.

35. VIDEOSURVEILLANCE SYSTEM

The sole purpose of the video surveillance system is to ensure the safety of individuals who work at/visit the Foundation's premises against unlawful and fraudulent behavior as well as to control and protect property and assets against theft and vandalism or, additionally, to control unauthorized access.

The system is operational in certain areas of the Foundation that are to be properly marked by appropriate information signs.

Access to the video-recorded images is allowed solely for the above-mentioned purposes to the persons in charge/authorized to process them and, in case of need, to the appropriate law enforcement agencies.

The Video Surveillance Document is adopted and updated by the Video Surveillance Manager, in consultation with the Company Trade Union Representatives.

36. REVOCATION OF AUTHORIZED DATA PROCESSOR STATUS

In case of revocation of the status of Authorized Data Processor or termination of the employment relationship with FBK, the following operating rules apply:

a. Credentials for system and e-mail access are disabled.
b. For justifiable reasons, FBK has the right to retain professional e-mails. E-mails in the "Personal Mail" folder will, on the contrary, be deleted.

These activities can be performed by System Administrators with the IT Infrastructures Service who are the only officers authorized to manage e-mail accounts. They may therefore have access, for exclusive technical reasons and only where it is not avoidable, to personal data stored in e-mail accounts.

Users are required to set up, with due advance, the auto responder to notify any suppliers, partners, customers or other interested parties, about the interruption of their work relationship with FBK and - if applicable - to propose an alternative internal contact.

With regard to returning ICT tools owned by the Foundation, the following operating rules apply:

a. Smartphones must be returned to the Corporate Assets Service.

b. Other ICT tools entrusted to Users of the Research Centers must be returned to the Head of the Research Unit they worked in.

c. ICT tools entrusted to non-research division Users will be returned to the IT Infrastructures Service.

In the event of a User's death, unless otherwise provided for by him/her, the Foundation shall ensure the exercise of the rights provided for in Chapter III of the GDPR to those who have a recognized self-interest, or act as proxies of the deceased, or for family reasons deserving protection.

37. DATA BREACH

"**Data Breach**" means the security breach that involves unintentionally or unlawfully the destruction, loss, modification, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed.

All cases of personal data related violations must immediately be reported to the Data Protection Officer (privacy@fbk.eu) thus ensuring the activation of the procedure for handling personal data breaches.

V. POSSIBILITY OF INDEPENDENT MANAGEMENT OF FBK-OWNED ICT TOOLS AND SERVICES

38. PURPOSE

To the end of ensuring maximum flexibility to research, Internal Users working for the Research Divisions only may obtain, upon authorization of their immediate Supervisor and of the IT Infrastructure Service and based on the provisions set out below, the full delegation to the management of FBK-owned ICT devices for the sole purpose of conducting research activities, taking full responsibility for the use of the tools and services.

39. LIABILITY

The Internal User shall follow preparatory and periodic training with the ultimate aim, on the one hand, to provide basic concepts regarding adequate security measures and general obligations under current legislation on the protection of personal data, and on the other hand, to clarify that he/she is personally liable for any violations put in place through the self-managed tool (e.g.: regulatory violations to personal data protection, intellectual property, copyright, etc...)

The Internal User accepts the consequent designation as "Independent Administrator of FBK-owned tools and services", a figure who must prove they can put in place adequate technical and organizational measures so that the processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject and the maintenance of an adequate level of security of the data of which FBK is the Controller.

In the event that multiple Users share the IT device, the Unit Head will act as the User in charge of the independent management.

40. USAGE RULES

The following are the rules for using the aforementioned self-managed IT tools and services:

a. Access to the Internet will be allowed.

b. Access to the above tools and services will be possible through the remote connection systems provided by the Foundation and will follow the same rules that apply to private tools.

c. Tools and services configured in this way shall not be connected to the type "d" network set out in Article 25 of these Regulations.

d. Computer tools and services may not offer services to the Internet either directly or indirectly unless they are connected to the type "c" network set out in Article 25 of these Regulations.

e. IT tools should not interfere with the normal functioning of the network.

f. Independent management implies the ability to manage and debug IT tools. The installation of the operating system will be carried out by the User. Backup services by the IT Infrastructures Service are not provided. The support of the IT Infrastructure Service will be limited to the hardware part only as provided by the warranty. No support with software issues will be provided.

g. The instructions for connecting the systems to the networks and the debug methods for connecting to the network can be found on the Foundation's website.

h. The aforementioned tools and services should be continuously updated, both the operating system part and the application part, in order to mitigate any security issues. In the event that, for whatever reason, the operating systems or applications are not updated, the tools shall be shut down immediately. Otherwise, the IT Infrastructure Service will disable, upon warning, access to the networks by the said systems. This rule applies, as far as research-managed tools and services are concerned, to centrally managed systems as well.

i. Self-managed or privately-owned portable tools shall be protected through the implementation of authentication systems - password, biometric, dual factor, etc. - and the use of the clientless web tools provided by the Foundation for access to FBK services is recommended, so as to avoid saving data on the devices. Should users, solely for work purposes, need to process personal data or important information on the local memories of the tools, they are required to use disk encryption.

VI. SPECIFIC PROHIBITIONS

41. PROHIBITIONS

The specific prohibitions for the recipients of these Regulations are as follows:

a. altering IT documents, public or private, having evidential value;

b. illegally accessing the IT or telecommunications system of public or private Users;

c. illegally accessing one's own computer or telecommunications system in order to alter and/or delete data and/or information;

d. illegally keeping and misusing codes, keywords or other means suitable for access to one's computer or telecommunications system or those of public or private competitors in order to acquire confidential information;

e. carrying out activities of procurement and/or production and/or deployment of equipment and/or software in order to damage an IT or electronic system of public or private Users, the information, data or programs contained therein, or to favor its total or partial disruption, or the alteration of its operation;

f. carrying out fraudulent activities intended to intercept, prevent or disrupt communications;

g. editing and/or cancelling data, information or programs of private Users or public entities or in any case of public benefit;

h. carrying out activities that damage information, data and computer programs or other people's programs;

i. destroying, damaging, making IT or telecommunications systems of public benefit unusable;

j. uploading programs not originating from a source that is reliable and has been authorized by the Company;

k. purchasing software licenses from a source (retailer or other) that is not certified and cannot guarantee the originality/authenticity of the software;

l. owning storage media for non-original programs (DVD\CD\floppy discs);

m. installing a number of copies of each licensed program higher than the copies authorized by the license itself, in order to avoid falling into possible underlicensing situations;

n. illegally using computer passwords, access codes or similar information to perform any of the above-mentioned actions;

o. using tools or equipment, including computer programs, to decrypt software or other IT data;

p. distributing FBK-owned software to third parties;

q. creating software code that infringes third party copyrights;

r. illegally accessing and duplicating databases.

VII. FURTHER PRESCRIPTION

42. LIABILITY AND SANCTIONS

Failure to comply with or breach to these Rules may result in the initiation of disciplinary and compensatory measures as well as applicable civil and criminal law actions.

Failure to comply with or breach to these Regulations may also justify the immediate revocation of access to ICT tools and services provided by the Foundation.

43. UPDATE AND REVISION

These Regulations are reviewed periodically, either as a result of organizational and regulatory changes or institutional needs. All future amendments to these Rules will be communicated and published on the Foundation's website.

Annex A

Details relating to check activities carried out by IT Infrastructure Service System Administrators

FBK manages the computer systems and networks through tools that can temporarily store data related to internet browsing and network traffic. In particular, the following are listed:

1. Electronic mail account- Stored data:
    a. log of SMTP traffic generated by the e-mail server;
    b. log of messages not forwarded correctly (delays and/or non-delivered);
    c. log of messages intercepted by the antivirus system;

2. IP traffic – proper functioning of the system, SLA monitoring, security checks:
    a. log of http/https traffic generated on IT devices. This log shall also include the navigation point data related to the internal IP of origin of the request. Data shall be kept for about 26 weeks in a system accessible only by authorized system administrators, and not normally used for other activities of the Foundation. However they might be stored for longer periods due to justified technical/organizational reasons, to ensure the exercise or defense of a legal action and in all cases where it is required by court authorities.
3. Telephone system – proper functioning of the system:
    a. Log of calls (calling number, called number, duration).
4. Access to networks - proper functioning of the system, SLA monitoring, security checks:
    a. Log of internal and external access to networks.

FBK conducts spot checks on tools operated independently by research staff in order to verify effective compliance with the Privacy Regulations and the application of FBK's standard security measures.

As stated in the Privacy Protection Authority's Guidelines applying to the use of e-mails and the Internet in employments context[3], FBK will not, under any circumstances, proceed with impermissible monitoring, such as:
- Accurate reading and recording of e-mail messages;
- Reproduction and storage of the web pages Users visit;
- Capture of typed characters through the keyboard (physical or virtual);
- Hidden analysis of personal computers assigned for use.

[3] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1408680