MISURE TECNICHE ED ORGANIZZATIVE ADOTTATE DA FBK

TECHNICAL AND ORGANIZATIONAL MEASURES ADOPTED BY FBK

rif. art. 32 del GDPR

REV E DATA	**REDAZIONE** **DRAFTING**	**VERIFICA** **REVIEW**	**APPROVAZIONE** **APPROVAL**	**MODIFICHE RISPETTO ALLA VERSIONE PRECEDENTE** **Changes from the previous version**
Rev. 02 del 04/11/2026	Servizio Soluzioni Digitali e Infrastrutture IT	Joint Lab per la Cybersecurity, DPO, Team Certificazioni	Segretario generale (per conto del Responsabile del Servizio Soluzioni Digitali e Infrastrutture IT) con determina n. 11/26 del 04/11/2026	Integrazione con nuove policy FBK
Rev. 01 del 15/10/2025	Servizio Soluzioni Digitali e Infrastrutture IT	Joint Lab per la Cybersecurity, DPO, Team Certificazioni	Responsabile Servizio Soluzioni Digitali e Infrastrutture IT con determina n. 16/25 del 15/10/2025	Revisioni stilistica e aggiornamento
Rev. 00 del 04/09/2024	Servizio Soluzioni Digitali e Infrastrutture IT	DPO, Team Certificazioni	Responsabile Servizio Soluzioni Digitali e Infrastrutture IT con determina n. 10/24 del 04/09/2024	Nuova adozione / New adoption

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità di ciascun trattamento di dati personali, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, FBK mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, misure che comprendono:
Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, FBK implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk, which include the following:

- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; *the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; *the ability to promptly restore availability and access to personal data in the event of a physical or technical disruption;*
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. *a procedure for regularly testing, evaluating and verifying the effectiveness of technical and organizational measures in order to ensure the security of processing operations.*

Di seguito sono riportate le misure tecniche ed organizzative adottate da FBK per assicurare proporzionalità e necessità del trattamento e prevenire l'accesso illegittimo, la modifica indesiderata, la scomparsa e le violazioni esplicite dei dati personali.
Below are the technical and organizational measures adopted by FBK to ensure proportionality and necessity of processing and to prevent illegitimate access, unwanted modification, erasure, and explicit violations of personal data.

Le misure in atto per minimizzare il rischio informatico seguono un'articolata strategia messa a punto grazie alla proficua collaborazione tra il Servizio Soluzioni Digitali e Infrastrutture IT, il Centro per la Cybersecurity e l'Unità Prevenzione della Corruzione, Trasparenza e Privacy.
The measures in place to minimize cyber risk follow a comprehensive strategy developed thanks to the fruitful collaboration between the Digital Solutions and IT Infrastructures Service, The Center for Cybersecurity and the Unit for Corruption Prevention, Transparency and Privacy.

Grazie a questa sinergia, nel corso del tempo sono state infatti organizzate e promosse iniziative congiunte volte, non solo ad incrementare il livello di sicurezza su sistemi, servizi e infrastrutture della Fondazione, ma anche a sensibilizzare tutto il personale relativamente ai

temi in oggetto e a potenziarne la conoscenza. Alcuni esempi di attività condivise sono il "Censimento dei sistemi, applicativi e servizi gestiti direttamente dai Centri di ricerca" e il Progetto "Gestione responsabile e sicura degli strumenti e dei servizi FBK" confluito nel periodico report annuale sullo "Stato della sicurezza in FBK".

Thanks to this synergy, joint initiatives have been organized and promoted over time, not only to increase the level of security of the Foundation's systems, services and infrastructure, but also to increase staff awareness on these issues and to enhance their knowledge. Examples of shared activities are the "Census of IT systems, applications and services directly managed by the Research Centres" and the Project "Responsible and safe management of FBK tools and services" converged into the periodic annual report on "Safety status in FBK".

A gennaio 2025 è stato inoltre costituito il JointLab per la Cybersecurity, laboratorio interno ad FBK composto da un gruppo di ricercatori afferenti al Centro per la Cyber Security e ad alcuni membri del Servizio Soluzioni Digitali e Infrastrutture IT. Esso risponde al duplice mandato di elevare la postura di sicurezza di FBK e, contestualmente, di agire quale motore di innovazione per lo sviluppo di servizi e applicazioni secondo un paradigma di security-by-design. Il JointLab per la Cybersecurity fornisce inoltre consulenza, formazione e supporto specialistico, in particolare nell'analisi e valutazione delle minacce e delle vulnerabilità, nel controllo dei rischi e nell'analisi delle minacce informatiche, anche come servizio a terzi. La funzione del JointLab è pertanto strumentale al conseguimento e al mantenimento della conformità rispetto al quadro normativo cogente, in riferimento alla Direttiva (UE) 2022/2555 (NIS2) e alla normativa italiana di recepimento. A tal proposito, il 17 luglio 2025, tramite delibera n. 12/25 (con aggiornamento del 24 settembre 2026), il Consiglio di Amministrazione ha formalizzato l'Organizzazione per la Sicurezza Informatica (OSI) nella Fondazione Bruno Kessler, che comprende il Chief Information Security Officer (CISO), il Cybersecurity Risk Manager ed i Referenti CSIRT.

Furthermore, in January 2025 the JointLab for Cybersecurity was established as an internal laboratory composed of a group of researchers from the Center for Cybersecurity and members of the Digital Solutions and IT Infrastructure Service. It responds to the dual mandate of elevating FBK's security posture and, concurrently, acting as an engine of innovation for the development of services and applications according to a security-by-design paradigm. The JointLab for Cybersecurity also provides consulting, training, and specialized support, particularly in the analysis and assessment of threats and vulnerabilities, risk control, and the analysis of cyber threats, including as a service to third parties. The function of the JointLab is therefore instrumental to achieving and maintaining compliance with the compelling regulatory framework, with reference to Directive (EU) 2022/2555 (NIS2) and the corresponding Italian implementing legislation. To this end, on July 17, 2025, through resolution no. 12/25 (and update of September 24th 2026), the Board of Directors formalized the Cybersecurity Organization within the Fondazione Bruno Kessler, which includes the Chief Information Security Officer (CISO), the Cybersecurity Risk Manager and CSIRT Representatives.

FBK ha adottato un Regolamento Privacy come strumento in cui sono definite un insieme di norme comportamentali a cui tutti i dipendenti, i collaboratori, le eventuali terze parti e - in

generale - i soggetti interni ed esterni che operano per FBK devono uniformarsi nell'ambito delle attività che implicano un trattamento di dati ed informazioni personali e aziendali, oltre che l'utilizzo degli strumenti e dei sistemi informatici.
FBK has adopted Privacy Regulations as a tool, which defines a set of behavior rules that applies to all employees, collaborators, all third parties and - in general - internal and external individuals who work for FBK for the activities that involve the processing of personal and business data and information, as well as the use of IT tools and systems.

FBK fa sì che chiunque agisca sotto la sua autorità e abbia accesso a dati personali sia istruito in modo opportuno al fine di procedere ad un corretto trattamento di dati personali per conto di FBK. Ogni nuova risorsa - indipendentemente dalla natura e dalla durata contrattuale – riceve le istruzioni per il trattamento di dati personali per il tramite della formazione obbligatoria.
FBK ensures that anyone acting under its authority and having access to personal data is properly trained in order to process personal data on its behalf appropriately. Each new resource - regardless of the nature and duration of the contract - receives the Instructions for the processing of personal data through mandatory training.

Il personale di ricerca della Fondazione è tenuto ad uniformare la propria attività di ricerca e studio alle regole deontologiche promosse dall'Autorità Garante per la Protezione dei Dati Personali che sono allegate al Codice di Comportamento della Fondazione.
The research staff of the Foundation is required to align its research and study activities with the ethical rules promoted by the Authority for the Protection of Personal Data that are attached to the Code of Conduct of the Foundation.

Eventuali casi di violazione di dati personali vengono immediatamente segnalati al DPO, assicurando così l'attivazione della Procedura di gestione delle violazioni di dati personali (Data Breach), che definisce gli attori, i compiti e le modalità di gestione delle violazioni di sicurezza delle informazioni di carattere personale (Data Breach) e delle conseguenti azioni che la Fondazione deve avviare e completare. Indipendentemente dalla valutazione circa la necessità di procedere con le comunicazioni obbligatorie, ogni qualvolta si verifichi una violazione di dati personali, il DPO registra l'evento nell'apposito Registro delle violazioni di dati personali e ne controlla nel tempo l'evoluzione.
Breaches of personal data are immediately reported to the DPO, thus ensuring the activation of the Data Breach Management Procedure, which defines the actors, the duties and the methods for managing security breaches of personal information (Data Breach) and the consequent actions that the Foundation must initiate and complete. Regardless of the assessment whether to proceed with the required communication whenever a personal data breach occurs, the DPO records the event in the dedicated Data Breach Register and monitors its evolution over time.

Dal 2024 la Fondazione è certificata UNI/EN/ISO 9001 (Qualità) e ISO/IEC 27001 (Sicurezza delle informazioni). Maggior informazioni al link https://howto.fbk.eu/documenti/certificazione-iso/).

From 2024, the Foundation is certified UNI/EN/ISO 9001 (Quality) and ISO/IEC 27001 (Information Security). More info at the link https://howto.fbk.eu/en/documenti/iso-certification/ .

Per quanto concerne la seconda, questa certificazione è volta a garantire la continuità operativa, ossia l'insieme di attività volte a minimizzare gli effetti distruttivi o comunque dannosi, di un evento che potrebbe colpire l'organizzazione o parte di essa, garantendo la continuità delle attività in generale; in termini di sicurezza delle informazioni, a fronte di interruzioni o danni, l'obiettivo è quello di evitare perdite significative delle stesse, mantenere o ripristinare il funzionamento dei processi ed assicurare la disponibilità dei dati necessari a garantire un livello di servizio accettabile. La continuità operativa comprende sia gli aspetti strettamente organizzativi, logistici e comunicativi che permettono la prosecuzione delle funzionalità dell'organizzazione, sia la continuità tecnologica, che riguarda l'infrastruttura informatica e telecomunicativa (ICT) ed è nota come "disaster recovery" (DR). Pertanto, le soluzioni per garantire la continuità dei servizi non considerano soltanto le componenti tecnologiche utilizzate, ma anche tutte le altre risorse messe in campo (personale, impianti, infrastrutture, ecc.).
A seguito di un'approfondita analisi (Inventario sistemi informatici rilevanti) da cui si evince che la Fondazione, tra le altre cose, non ha servizi critici al suo interno né offre prestazioni al pubblico, è stato quindi scelto di avere una strategia mista che combina soluzioni di Alta Disponibilità (High Availability - HA) per l'infrastruttura di rete (router/firewall/switch) e procedure di ripristino e failover programmato per i cluster di virtualizzazione in replica sincrona. Un sistema High Availability si basa sui principi di ridondanza (presenza di più componenti o sistemi in grado di svolgere la stessa funzione), distribuzione (di componenti o sistemi su più siti o infrastrutture) e automazione (strumenti automatici per il rilevamento e la risoluzione dei problemi) ed implica monitoraggio e rapido ripristino.

Tutto ciò è stato raccolto nel "Piano di Continuità Operativa e ripristino" (riservata) e delle derivate policy "Politica per sicurezza IT di FBK" e "Procedura di gestione degli incidenti relativi alla sicurezza delle informazioni" (interne) che forniscono una panoramica dettagliata su politiche, strategie e misure preventive implementate in FBK per affrontare le sfide relative alla sicurezza informatica ed alla protezione dei dati sensibili.
With regard to the second, this certification has the purpose to ensuring business continuity, that is, the set of activities aimed at minimizing the destructive or otherwise harmful effects of an event that could affect the organization or part of it, ensuring the continuity of activities in general; in terms of information security, in the event of disruption or damage, the objective is to avoid significant losses of information, maintaining or restoring the functioning of processes and assuring the availability of data necessary to guarantee an acceptable level of service. The operating continuity comprises both the strictly organizational, logistic and communicative aspects that allow the maintenance of the organization's functionalities, and the technological continuity, that regards the computer and telecommunication infrastructure (ICT) and is known as "disaster recovery" (DR). Therefore, the solutions to guarantee the continuity of the services do not consider only the technological components used, but also all the other deployed resources (staff, systems, infrastructures, etc.).

Following an in-depth analysis (Inventory of Relevant IT Sustems) showing that the Foundation, among other things, does not have any critical services in-house nor offers services to the public, it was decided to adopt a hybrid strategy that combines High Availability (HA), for the network infrastructure (routers/firewalls/switches) with recovery procedures and scheduled failover for virtualization clusters in synchronous replication. An HA system is based on the principles of redundancy (presence of several components or systems capable of performing the same functions), distribution (of components or systems on multiple sites or infrastructures) and automation (automatic problem detection and resolution tools) and implies monitoring and rapid recovery. All this was gathered in the "Business Continuity and Recovery Plan" (confidential) and the derived policies "Policy for IT Security of FBK" and "Information Security Incident Management Procedure" (confidential) which provide a detailed overview of policies, preventive strategies and measures implemented in FBK to address IT security and sensitive data protection challenges.

Nello specifico, FBK utilizza un proprio Data Center ed un sito di Disaster Recovery, entrambi ad accesso limitato e controllato, dove sono ospitati i server, i sistemi di calcolo ed i dispositivi di networking, oltre che i sistemi di storage su cui sono residenti i dati.
Specifically, FBK uses its own Data Center and a Disaster Recovery site, both with restricted and supervised access, where the servers, computing systems and networking devices, as well as the storage systems on which the data is resident, are hosted.

Con riferimento ai cloud utilizzati da FBK, Google è il cloud server istituzionale per i servizi di posta elettronica e collaboration, mentre Microsoft Azure per l'infrastruttura.
With reference to the clouds used by FBK, Google is the institutional cloud server for email and collaboration services, while Microsoft Azure for infrastructure.

Con riferimento ai cloud utilizzabili dalla ricerca, si predilige la scelta dei cloud Microsoft Azure e Amazon Web Services (acquistabili attraverso la centrale di committenza CRUI). Eventuali servizi di cloud alternativi devono essere giustificati e comunque GDPR compliant e certificati ACN.
As for the clouds that can be used for research, FBK's preferred choices are Microsoft Azure and Amazon Web Services clouds (which can be purchased through the CRUI central purchasing office). The use of cloud services other than the above must be justified and always GDPR compliant and ACN certified.

In considerazione del fatto che FBK si relaziona con Pubbliche Amministrazioni, quando sviluppa software, applicazioni e codici che trattano dati personali, rispetta ed adotta le indicazioni fornite dall'Agenzia per l'Italia Digitale (AGID) circa le misure di sicurezza ICT (circolare AGID n. 2/2017 *Misure minime di sicurezza ICT per le pubbliche amministrazioni* e successive modifiche e integrazioni), seguendo metodologie di sviluppo che tengano conto dei problemi di privacy e sicurezza informatica. Per le specifiche procedure dell'Unità FBK Digital, è stato adottato il documento "Linee Guida in materia di qualità e sicurezza delle informazioni e dei processi di sviluppo software" ed in generale, per tutta la Fondazione, la "Policy per lo sviluppo e il ciclo di vita dei prodotti e servizi digitali".
In consideration of the fact that FBK interacts with Public Administrations, when developing software, applications and codes that process personal data, it respects and adopts the directives provided by the Agency for Digital Italy (AGID) regarding ICT security measures (Agid circular n. 2/2017 Minimum ICT security

measures for public administrations and subsequent changes and additions), following development methodologies that take into account privacy and IT security issues. For the specific procedures of the FBK Digital Unit, the document "Guidelines on quality and security of information and software development processes" and in general, for all FBK, the "Policy for the development and life cycle of digital products and services" has been adopted.

FBK è anche impegnata nella protezione dei minori che sono destinatari dei servizi da essa erogati o che, a qualsiasi titolo, vengono coinvolti nelle proprie attività di ricerca e studio ed ha adottato una Policy per la tutela e la promozione dei diritti dei bambini e degli adolescenti per assicurare e promuovere in ogni ambito (anche quello legato alla protezione dei dati personali) la tutela e la dignità dei minori tenendo conto della disciplina vigente e dei principi in materia sanciti a livello internazionale, europeo e nazionale.
FBK is also committed to the protection of minors who are recipients of its services or who, for whatever reason, are involved in their research and study activities and has adopted a Policy for the protection and promotion of the rights of children and adolescents to ensure and promote in all areas (including the protection of personal data) the protection and dignity of minors, taking into account the existing rules and principles laid down in this field at international, European and national level.

A seguito di un significativo aumento delle email di phishing, minaccia per la sicurezza dei sistemi e dei dati sensibili, la Fondazione propone campagne di informazione sul phishing e formazione dedicata per mitigare questi rischi e garantire la sicurezza delle informazioni. L'obiettivo è quello di preparare il personale ad un'evenienza concreta ed identificare eventuali punti deboli, migliorando la globale capacità di riconoscere e gestire situazioni potenzialmente pericolose.
Following a significant increase in phishing emails, a possible threat for sensitive data and systems' security, the Foundation proposes phishing information campaigns and dedicated training to mitigate these risks and ensure information security. The aim is to prepare the staff for a real event and identify any weaknesses, Improving the global ability to recognise and manage potentially dangerous situations.

Di seguito si sintetizzano le misure tecniche ed organizzative adottate da FBK:
Below there is a summary of the technical and organizational measures adopted by FBK:

SISTEMI GESTITI CENTRALMENTE *SELF-MANAGED SYSTEMS*

Principi generali ***General principles*** Misure per assicurare proporzionalità e necessità del trattamento *Measures to ensure processing proportionality and necessity*	- Regolamento Privacy. *Privacy Regulations.* - Guida pratica FBK alla protezione dei dati personali. *FBK Practical Privacy Guide.* - Procedura per la valutazione d'impatto sulla protezione dei dati (DPIA). *Data Protection Impact Assessment (DPIA) Procedure.* - Linee Guida per la corretta gestione dei PC e dei Server autogestiti. *Guidelines for the proper use of PCs and self-managed Servers.* - Policy per la tutela e la promozione dei diritti dei bambini e degli adolescenti. *Policy for the protection and promotion of children's rights.* - Politica per la sicurezza IT di FBK. *Policy for IT security of FBK.* - Policy per lo sviluppo e il ciclo di vita dei prodotti e servizi digitali. *Policy for the development and life cycle of digital products and services.* - Linee Guida per la Formazione in materia di Gestione e Prevenzione degli Incidenti. *Guidelines for training in incident management and prevention.* - Base giuridica del trattamento definita. *Legal basis for the processing identified.* - Accesso consentito ai soli dati personali la cui conoscenza sia strettamente indispensabile per adempiere ai compiti affidati. *Access allowed only to personal data whose knowledge is strictly essential to fulfill the assigned tasks.* - Pseudonimizzazione/cifratura dei dati in transito e a riposo. *Pseudonymization/encryption of data in transit and at rest.* - Dati corretti e aggiornati. *Correct and up-to-date data.* - Valutazione del requisito dell'adeguatezza per il trasferimento dei dati extra EU. *Assessment of compliance with requirements for the transfer of data outside the EU.* - Accordi specifici con le Rappresentanze Sindacali. *Agreements with trade union representatives.*

Riservatezza ***Confidentiality*** Misure per prevenire l'accesso illegittimo ai dati personali *Measures to prevent unlawful access to personal data*	- Organizzazione per la sicurezza informatica in FBK. *Cybersecurity Organization in FBK* - Regolamento Privacy. *Privacy Policy.* - Guida pratica FBK alla protezione dei dati personali. *FBK Practical Privacy Guide.* - Procedura per la valutazione d'impatto sulla protezione dei dati (DPIA). - *Data Protection Impact Assessment (DPIA) Procedure.* - Linee Guida per la corretta gestione dei PC e dei Server autogestiti. *Guidelines for the proper use of PCs and self-managed Servers.* - Policy per la tutela e la promozione dei diritti dei bambini e degli adolescenti. *Policy for the protection and promotion of children's rights.* - Utilizzo esclusivamente personale della password di accesso ai sistemi informativi. *Personal use only of the information systems access credentials.* - Strumenti bloccati e protetti da password se lasciati incustoditi. *Tools locked and password protected if left unattended.* - Salvaschermo. *Screensaver.* - Data Center dotato di specifiche modalità di accesso, interconnesso tramite percorsi distinti, ad altri due data center locati in posizioni separate. *Data Center equipped with specific access methods, interconnected via separate paths to two other data centers located in separate locations.* - Standard di Google. *Google standards.* - Autenticazione a più fattori (MFA). *Multi-factor authentication (MFA).* - Applicazione del Principle of least privilege per l'accesso alle informazioni ed ai sistemi. *Application of the Principle of least privilege for access to information and systems.* - Uso di sistemi di autorizzazione basati sui ruoli (RBAC) o attributi (ABAC). *Using role-based authorization systems (RBAC) or attributes (ABAC).* - Risk based Authentication con Single sign-on (SSO).

	Risk based Authentication with Single sign-on (SSO).
Integrità ***Integrity*** Misure per prevenire la modifica indesiderata dei dati personali *Measures to prevent unwanted modification of personal data*	- Organizzazione per la sicurezza informatica in FBK. *Cybersecurity Organization in FBK* - Piano di Gestione delle Vulnerabilità *Vulnerability Management Plan* - Piano di gestione delle crisi *Crisis Management Plan* - Regolamento Privacy. *Privacy Policy.* - Guida pratica FBK alla protezione dei dati personali. *FBK Practical Privacy Guide.* - Procedura per la valutazione d'impatto sulla protezione dei dati (DPIA). *Data Protection Impact Assessment (DPIA) Procedure.* - Linee Guida per la corretta gestione dei PC e dei Server autogestiti. *Guidelines for the proper use of PCs and self-managed Servers.* - Procedura di gestione degli incidenti relativi alla sicurezza delle informazioni. *Information security incident management procedure.* - Accesso esclusivo del personale autorizzato. *Access granted to authorized staff only.* - Utilizzo esclusivamente personale della password di accesso ai sistemi informativi. *Personal use only of the information systems access credentials.* - Presenza di un UPS (generatore) per l'erogazione dell'energia in caso di blackout. *UPS (generator) for power supply in the event of a blackout.* - Uso di sistemi di autorizzazione basati sui ruoli (RBAC) o attributi (ABAC). *Using role-based authorization systems (RBAC) or attributes (ABAC).* - Risk based Authentication con Single sign-on (SSO). *Risk based Authentication with Single sign-on (SSO).* - Versioning (tramite sistema di controllo Git). *Versioning (via Git control system).* - Validazione dell'input. *Input validation.* - Uso di algoritmi di hashing e CRC equivalenti considerati sicuri

	dalle linee guida europee ENISA. *Use of equivalent hashing and CRC algorithms considered safe by ENISA European guidelines.* - Uso di sistemi di autorizzazione basati sui ruoli (RBAC) o attributi (ABAC). *Using role-based authorization systems (RBAC) or attributes (ABAC).* - Log immutabili degli accessi (al dato o al sistema). *Immutable log accesses (to data or system).*
Disponibilità ***Availability*** Misure per prevenire la scomparsa dei dati personali *Measures to prevent the erasure of personal data*	- Organizzazione per la sicurezza informatica in FBK. *Cybersecurity Organization in FBK* - Regolamento Privacy. *Privacy Policy.* - Guida pratica FBK alla protezione dei dati personali. *FBK Practical Privacy Guide.* - Procedura per la valutazione d'impatto sulla protezione dei dati (DPIA). *Data Protection Impact Assessment (DPIA) Procedure.* - Linee Guida per la corretta gestione dei PC e dei Server autogestiti. *Guidelines for the proper use of PCs and self-managed Servers.* - Backup (paradigma 3-2-1). *Backup (paradigm 3-2-1).* - Data Center dotato di specifiche modalità di accesso, interconnesso tramite percorsi distinti, ad altri due data center locati in posizioni separate. *Data Center equipped with specific access methods, interconnected via separate paths to two other data centers located in separate locations.* - Presenza di un UPS (generatore) per l'erogazione dell'energia in caso di blackout. *UPS (generator) for power supply in the event of a blackout.* - Archivi cartacei in armadi chiusi a chiave. *Paper archives in locked cabinets.* - Locali dotati di sistema antincendio. *Premises equipped with fire protection systems.* - Versioning (tramite sistema di controllo Git). *Versioning (via Git control system).*

	- Protezione da attacchi Denial Of Service. *Protection from Denial Of Service attacks.* - Politiche di conservazione. *Conservation policies.*
Sicurezza ***Data security*** Misure per prevenire violazioni esplicite dei dati personali *Measures to prevent explicit breaches of personal data*	- Organizzazione per la sicurezza informatica in FBK. *Cybersecurity Organization in FBK.* - Piano di Gestione delle Vulnerabilità. *Vulnerability Management Plan.* - Piano di gestione delle crisi. *Crisis Management Plan.* - Politica per la sicurezza IT di FBK. *Policy for IT security of FBK.* - Piano di Continuità Operativa e ripristino. *Business continuity and recovery plan.* - Policy per lo sviluppo e il ciclo di vita dei prodotti e servizi digitali. *Policy for the development and life cycle of digital products and services.* - Procedura di gestione degli incidenti relativi alla sicurezza delle informazioni. *Information security incident management procedure.* - Regolamento Privacy. *Privacy Policy.* - Procedura di gestione Data Breach. *Data Breach Management procedure.* - Guida pratica FBK alla protezione dei dati personali. *FBK Practical Privacy Guide.* - Procedura per la valutazione d'impatto sulla protezione dei dati (DPIA). *Data Protection Impact Assessment (DPIA) Procedure.* - Linee Guida per la corretta gestione dei PC e dei Server autogestiti. *Guidelines for the proper use of PCs and self-managed Servers.* - Policy per la tutela e la promozione dei diritti dei bambini e degli adolescenti. *Policy for the protection and promotion of children's rights.* - Linee Guida per la Formazione in materia di Gestione e Prevenzione degli Incidenti. *Guidelines for training in incident management and prevention.* - Formazione all'assunzione, periodica e obbligatoria. *Training upon hiring, periodic and mandatory.*

	- Formazione ad hoc (utenti ed admin). *Ad hoc training (users and admin).* - Progetto “Gestione responsabile e sicura degli strumenti e dei servizi FBK”. *Project "Responsible and safe management of FBK tools and services".* - Campagne di informazione sul phishing. *Phishing information campaigns.* - Audit interni. *Internal audits.* - Antivirus. *Antivirus protection.* - Standard di Google. *Google standards.* - Sistemi antimalware cloud based. *Antimalware cloud based systems.* - Reti trusted. *Trusted networks.* - Autenticazione a più fattori (MFA). *Multi-factor authentication (MFA).* - Firewall di ultima generazione a Layer 7. *Next generation Firewall a Layer 7.* - uso di WAF, IDS e IPS CrowdSec. *WAF, IDS and IPS with CrowdSec solution.* - Risk based Authentication con Single sign-on (SSO). *Risk based Authentication with Single sign-on (SSO).* - Passkey obbligatoria per gli Amministratori Centrali. *Mandatory Passkey for Central Administrators.* - Risk Assessment con intrusion detection/prevention systems (Microsoft Attack Surface Management (EASM), sistemi di Data Loss Prevention ed altri. *Risk Assessment with intrusion detection/prevention systems (Microsoft Attack Surface Management (EASM), Data Loss Prevention systems and others).* - Applicazione del Principle of least privilege e Separazione delle Funzioni per l’accesso alle informazioni ed ai sistemi. *Application of the Principle of least privilege and Separation of Duties for access to information and systems.* - Sistemi di notifiche per monitoraggio continuo. *Notification systems for continuous monitoring.* - Microsegmentazione e Segmentazione della Rete utenti per prevenire la pervasività di attacchi informatici. *Microsegmentation and*

	Segmentation of end-user networks to prevent the pervasiveness of cyber attacks. - Software installabili solo dall'Amministratore di Sistema. *Software that can only be installed by the System Administrator.* - Salvaschermo. *Screensaver.* - Dismissione sicura e ri-utilizzo sicuro degli strumenti informatici con eliminazione di ogni dato da parte degli Amministratori di Sistema. *Safe disposal and safe re-use of IT tools with deletion of all data by the System Administrators.* - Tecniche di sviluppo software sicuro. *Secure software development techniques.* - Segregazione delle reti (wi-fi/LAN). *Network segregation (wi-fi/LAN).* - VPN con controllo degli accessi basato sul ruolo con Zero Trust e minimo privilegio. *VPN Role-Based Access Control with Zero Trust and least privilege*. - Crittografia di tutti i siti gestiti centralmente da FBK (https). *Encryption of all sites managed centrally by FBK (https).* - Scrivania pulita. *Clean desk.* - Versioning (tramite sistema di controllo Git). *Versioning (via Git control system).* - Protezione da attacchi Denial Of Service. *Protection from Denial Of Service attacks.* - Vulnerability Assessment/Penetration Testing periodici. *Vulnerability Assessment/periodic Penetration Testing.* - Uso di algoritmi di hashing e CRC equivalenti considerati sicuri dalle linee guida europee ENISA. *Use of equivalent hashing and CRC algorithms considered safe by ENISA European guidelines.* - Installazione XDR (endpoint security and server security). *XDR installation (endpoint security and server security).* - Uso di SIEM (security information and event management). *SIEM use (security information and event management).*

STRUMENTI AUTOGESTITI *SELF-MANAGED TOOLS*

I Responsabili della gestione autonoma di strumenti e servizi forniti da FBK devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato e dei dati di cui FBK è Titolare.
FBK-owned ICT tools Administrator must produce evidence that they can put in place appropriate technical and organizational measures so that the processing meets the requirements of the GDPR and protect the rights of the data subject and of the data of which FBK is the Controller.

Per tali soggetti responsabili è prevista una attività propedeutica e periodica di formazione obbligatoria, con esame finale e conseguente abilitazione da parte del diretto/a Responsabile del/la richiedente e l'Amministratore di Sistema FBK (Responsabile del Servizio Soluzioni Digitali e Infrastrutture IT). I soggetti in questione si attengono alle Linee Guida per la corretta gestione dei PC e dei Server autogestiti, assicurando che venga mantenuto e non diminuito l'attuale livello standard FBK.
For these responsible parties a preparatory and periodic compulsory training is provided, with final examination and subsequent enabling by the direct Responsible of the applicant and the System Administrator FBK (Head of Digital Solutions and IT Infrastructure Service). These individuals comply with the Guidelines for the correct management of the PC and the self-managed servers, ensuring that the current FBK standard level is maintained and not decreased.

Gli strumenti così configurati possono essere connessi alle reti per i dispositivi informatici periferici, per i server autogestiti nel Data Center e per i server autogestiti su cloud, come indicato nell'articolo 25 del Regolamento Privacy della Fondazione Bruno Kessler.
The tools thus configured can be connected to networks for peripheral computer devices, for self-managed servers in the Data Center and for self-managed cloud servers, as indicated in Article 25 of the Privacy Regulation of the Bruno Kessler Foundation.

Nell'ambito del progetto "Gestione responsabile e sicura degli strumenti e dei servizi FBK", la Fondazione pianifica annualmente una serie incontri destinati agli Amministratori di Sistemi, allo scopo di far crescere la consapevolezza nell'ambito della gestione degli strumenti informatici e della cybersecurity, e contemporaneamente mettere a punto un modello condiviso per l'analisi ed il controllo degli strumenti gestiti in autonomia.
As part of the project "Responsible and safe management of FBK tools and services", the Foundation plans an annual series of meetings for System Administrators, with the aim of raising awareness about the management of IT tools and cybersecurity, and at the same time, developing a shared model for analysis and supervision of self-managed tools.

Ulteriori dettagli sono reperibili nel Regolamento Privacy.
More details are available in the Privacy Regulations.

DOCUMENTI CARTACEI *PAPER DOCUMENTS*

I dati cartacei ed i supporti cartacei necessari per lo svolgimento delle mansioni lavorative sono custoditi in armadi o cassettiere del contesto organizzativo in cui si opera.
Paper data and paper support material necessary for the performance of work duties are kept in cabinets or drawers in the organizational context in which the worker operates.

I documenti vengono riposti correttamente durante i periodi di temporanea assenza ed al termine dell'attività lavorativa negli appositi archivi. Gli archivi di documenti e atti contenenti dati particolari (ex sensibili) sono custoditi in armadi chiusi a chiave. Tutti gli archivi sono ad accesso limitato, per cui è possibile accedervi nei limiti della necessità per prelevare e riporre i documenti necessari per lo svolgimento delle mansioni lavorative.
Documents are stored correctly during temporary absence and, at the end of the work activity, in the appropriate archives.
The archives of documents and deeds containing sensitive data are kept in locked cabinets. Access to archives is restricted, so it is possible to access them when necessary only to pick up and put away the documents needed for the execution of work duties.

L'eliminazione fisica di ogni documento cartaceo o supporto informatico contenente dati e informazioni aziendali e/o personali deve essere effettuata solo utilizzando gli appositi strumenti.
The physical elimination of any paper document or IT device containing company and/or personal data and information must only be carried out using the appropriate tools.

Non vengono lasciati documenti incustoditi presso i dispositivi di stampa.
No documents are left unattended at the printers.

La trasmissione di documenti contenenti dati personali tra le varie articolazioni organizzative di FBK avviene in buste chiuse.
The transmission between the various FBK organizational units of documents containing personal data takes place in closed envelopes.

La postazione di lavoro viene mantenuta in ordine, verificando di non lasciare documenti e atti riservati senza un proprio controllo all'accesso di terzi, in momenti di pausa, terminata la giornata di lavoro e/o in periodi di assenza.
The workstation is kept tidy, making sure not to leave confidential documents unattended during breaks, at the end of the work day and/or in periods of absence.

Ulteriori dettagli sono reperibili nel Regolamento Privacy.
More details are available in the Privacy Regulations.

Tutte le informazioni sul sistema di gestione dei dati personali della Fondazione Bruno Kessler sono disponibili sul portale HowTo.

All information on the Bruno Kessler Foundation's personal data management system is available on HowTo portal.