# Regolamento Privacy della Fondazione Bruno Kessler

Trattamento dei dati personali e aziendali, uso degli strumenti e dei sistemi informatici.

Approvato con delibera del Consiglio di Amministrazione n. 15/17 del 20 dicembre 2017

Sostituisce ed integra la precedente Policy per l'utilizzo dei sistemi informatici nella sua ultima versione aggiornata al 17 maggio 2013

Modificato con delibera del Consiglio di Amministrazione n. 08/19 del 29 gennaio 2019

Modificato con delibera del Consiglio di Amministrazione n. 28/22 del 18 novembre 2022

(versione in vigore dal 1° gennaio 2023)

## INDICE

# I. INTRODUZIONE

## 1. PREMESSA

Preservare la riservatezza, l'integrità e la disponibilità dei dati e delle informazioni a tutela della dignità delle persone fisiche, delle libertà fondamentali e del valore del capitale intellettuale della Fondazione.

Assicurare un uso corretto delle risorse informatiche e telematiche messe a disposizione dalla Fondazione Bruno Kessler a tutela della sicurezza delle informazioni trattate e dell'integrità della Fondazione stessa.

Questi gli obiettivi che ispirano il presente Regolamento, che si inserisce nel contesto della generale disciplina in materia di Privacy e nel sistema normativo che regola l'organizzazione, i processi e le funzioni della Fondazione.

## 2. CONTESTO

La Fondazione Bruno Kessler sostiene attivamente la transizione digitale ed ecologica in atto ed è pienamente partecipe dei cambiamenti necessari per assicurare forme di sviluppo inclusive e sostenibili.

In quest'ottica, privilegiando un approccio fluido ai sistemi organizzativi ed operativi, la Fondazione è impegnata a garantire e promuovere un ambiente di lavoro e un'infosfera basati sulla tutela dell'integrità e del rispetto dei principi di liceità, correttezza e trasparenza.

## 3. TUTELA DEL LAVORATORE

La Fondazione assicura la tutela dei diritti e delle libertà fondamentali di tutto il personale dipendente e collaboratore anche garantendo e promuovendo ogni ragionevole forma di protezione della sfera di riservatezza.

## 4. CAMPO DI APPLICAZIONE, DESTINATARI E PRESIDI

In considerazione della peculiarità organizzativa e operativa della Fondazione, la disciplina del presente Regolamento, anche guardando ai Provvedimenti del Garante Privacy, declina, specifica o integra quanto previsto dal Regolamento Europeo n. 2016/679 – General Data Protection Regulation ("GDPR"), dal Decreto Legislativo n. 196/2003 - Codice in materia di protezione dei dati personali ("Codice") così come novellato ed integrato dal Decreto Legislativo n. 101/2018 - Disposizioni per l'adeguamento della normativa nazionale al GDPR. Sono destinatari del presente Regolamento:

A. Soggetti interni:
   - componenti degli Organi statutari e degli altri organismi
   - personale dipendente
   - personale collaboratore coordinato e continuativo
   - personale in somministrazione
   - personale presente in FBK a fronte di accordi di distacco o di un comando
   - personale dipendente provinciale messo a disposizione di FBK
   - consulenti e lavoratori/trici autonomi/e occasionali
   - risorse affiliate (Alti profili, Affiliated fellows, Visiting fellows, PhD students, Scholars, High School fellows).

B. Soggetti esterni:
   - imprese fornitrici di beni, servizi o lavori che operino con la Fondazione, indipendentemente dal rapporto giuridico sottostante, ed il loro personale dipendente e collaboratore

- personale di altre entità presente in FBK in forza di convenzioni o accordi inter-istituzionali
- visitatori/trici e ospiti di vario genere.

A presidio della corretta osservanza di quanto disciplinato dal presente Regolamento, e nei limiti delle rispettive competenze e responsabilità funzionali, operano l'Unità Prevenzione della Corruzione, Trasparenza e Privacy, il Servizio Infrastrutture IT nonché, con un ruolo più orientato al supporto consulenziale, la Responsabile della Protezione dei Dati Personali (DPO).

## II. DEFINIZIONI

### 5. DEFINIZIONI PRIVACY

Sono di seguito riportate le principali definizioni in materia di privacy e protezione dei dati personali.

**Dato personale**: qualsiasi informazione che identifica o rende identificabile una persona fisica e che può fornire dettagli sulle sue caratteristiche fisiche, fisiologiche, genetiche o psichiche, sulle sue abitudini, sul suo stile di vita, sulle sue relazioni personali, sul suo stato di salute o sulla sua situazione economica.

**Dati identificativi**: dati personali che permettono l'identificazione diretta di una persona fisica.

**Dati particolari:** dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'etnia, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale di una persona fisica. Fanno parte dei dati particolari anche i **dati genetici** (dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla sua fisiologia o salute e che risultano dall'analisi di un suo campione biologico) ed i **dati biometrici** (dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici).

**Dati giudiziari:** dati idonei a rilevare informazioni riguardo provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

**Dati rischiosi**: dati personali diversi dai dati particolari e giudiziari che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità di una persona fisica, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare (per esempio dati che identificano comportamenti, interessi, scelte, acquisti e spostamenti).

**Trattamento di dati personali:** qualsiasi operazione compiuta con o senza l'ausilio di processi automatizzati e applicata a dati personali, o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento, la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

**Profilazione**: qualsiasi forma di trattamento automatizzato di dati personali che consiste nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

**Anonimizzazione**: processo mediante il quale i dati personali sono modificati in modo irreversibile così che il Titolare del trattamento, da solo o in collaborazione con altre parti, non possa più identificare direttamente o indirettamente una persona fisica.

**Pseudonimizzazione**: trattamento dei dati personali effettuato in modo tale che tali dati non possano più essere attribuibili ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che i dati personali non siano attribuibili a una persona fisica identificata o identificabile.

**Comunicazione di dati personali:** dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in base ad una precisa finalità ed una modalità certa e sicura di trattamento, anche mediante la loro messa a disposizione o consultazione.

**Diffusione di dati personali:** dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

**Violazione di dati personali (Data Breach)**: violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

**Accountability**: principio cardine del GDPR secondo il quale il Titolare ha la responsabilità generale e l'onere di adottare comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del GDPR su qualsiasi trattamento di dati personali effettuato direttamente o che altri effettuano per suo conto.

## 6. DEFINIZIONI DELLE FIGURE PRIVACY

Di seguito sono riportate le definizioni relative alle figure privacy.

**Interessato/a**: persona fisica cui si riferiscono i dati personali trattati.

**Titolare del trattamento:** la Fondazione nel suo complesso che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza. Il Consiglio di Amministrazione può affidare funzioni di coordinamento di tutti gli adempimenti connessi al trattamento dei dati personali per conto del Titolare del trattamento ad un/a Responsabile Interno/a del trattamento, attraverso apposita procura per la rappresentanza della Fondazione conferita dal/la Presidente.

**Contitolare del trattamento:** Titolare del trattamento che determina congiuntamente ad altro Titolare le finalità e i mezzi del trattamento in modo trasparente e mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR.

**Responsabile esterno del trattamento**: persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento. Il Responsabile esterno del trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate affinché il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato.

**Sub-responsabile esterno del trattamento:** persona fisica o giuridica, autorità pubblica, servizio o altro organismo alla quale un Responsabile esterno del trattamento ricorre per l'esecuzione di specifiche attività di trattamento per conto del Titolare.

**Responsabile Interno/a del trattamento dei dati personali:** soggetto interno alla Fondazione cui viene affidata la responsabilità per i trattamenti di dati personali riconducibili al relativo ambito di competenza. Tale soggetto coincide con un/a Responsabile di articolazione o sotto-articolazione organizzativa Centro, Unità, Servizio, Direzione…). Nel caso di progetti di ricerca che coinvolgono più articolazioni organizzative, il/la Responsabile Interno/a del trattamento è individuato nel/i Direttore/i di Centro.

**Personale incaricato/autorizzato al trattamento**: soggetto interno alla Fondazione autorizzato a compiere operazioni di trattamento di dati personali, sulla base dei regolamenti adottati e delle istruzioni impartite dal Titolare e/o dal/la Responsabile Interno/a del trattamento.

**Amministratore di sistema**: persona fisica o giuridica nominata dal Titolare e preposta alla gestione e sicurezza dei sistemi informativi attraverso l'applicazione delle misure necessarie al mantenimento della riservatezza, disponibilità e integrità del dato personale trattato.

**Responsabile della gestione autonoma di strumenti e servizi informatici forniti da FBK**: soggetto interno che gestisce in autonomia strumenti informatici e servizi forniti dalla Fondazione e che presenta 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.

**Responsabile della Protezione dei Dati (Data Protection Officer - DPO)**: persona fisica nominata dal Titolare che, ai sensi degli artt. 37-39 del succitato GDPR, operando in modo indipendente rispetto all'organizzazione, consiglia il Titolare riguardo obblighi, requisiti ed evoluzione normativa, realizza verifiche interne sulla corretta applicazione delle disposizioni normative e del sistema di gestione privacy definite dal Titolare, assiste il Titolare sulla valutazione di impatto privacy e sull'analisi del rischio e rappresenta il punto di contatto per interessati e Garante Privacy.

### 7. DEFINIZIONI IT

Di seguito sono riportate alcune altre definizioni utili alla corretta gestione dei processi di trattamento dei dati personali.

**Account:** identità creata per una persona in un computer o in un sistema informatico.

**Applicativo**: (applicazione software, o applicazione, o app in breve): programma per computer progettato per svolgere un compito specifico diverso da quello relativo al funzionamento del computer stesso.

**Badge**: tesserino con chip elettronico di riconoscimento.

**Cloud Pubblica**: modello di conservazione dati su computer in rete dove i dati stessi sono memorizzati su molteplici server virtuali generalmente ospitati presso strutture di terze parti o su server dedicati.

**Data Center**: locale ad accesso limitato che ospita i server, i sistemi di calcolo e i dispositivi di networking, oltre che i sistemi di storage su cui sono residenti i dati.

**Infrastruttura**: insieme di componenti di tecnologia dell'informazione (IT) che sono alla base di un servizio IT; componenti tipicamente fisici (computer e hardware e strutture di rete), ma anche vari componenti software e di rete.

**Infostruttura**: infrastruttura specificatamente dedicata alla comunicazione.

**Pass**: tesserino cartaceo senza identificativo.

**Servizi IT**: servizi di Information Technology come, ad esempio, la posta elettronica, i server documentali, le applicazioni, la connessione ai sistemi e a Internet, e in generale tutti quei servizi atti a archiviare, elaborare, convertire, proteggere, trasmettere e recuperare informazioni.

**Sistema o Macchina**: computer, o insieme di computer, che include l'hardware, il sistema operativo (software principale), un applicativo e le apparecchiature periferiche necessarie e utilizzate per il funzionamento.

**Strumenti informatici**: stampanti, laptop, computer da tavolo, telefoni fissi, smartphone, tablet, e-book reader, telecamere IP, e, in generale, qualsiasi dispositivo in grado di connettersi a una rete IP.

## III. MODELLO ORGANIZZATIVO

### 8. CLASSIFICAZIONE DELLE INFORMAZIONI

Il patrimonio informativo di FBK (patrimonio costituito da tutti i dati e le informazioni trattati nei diversi processi, tra i quali anche i dati personali) può essere classificato secondo i seguenti criteri:

**Dati e informazioni pubbliche**: sono le informazioni liberamente trattabili da soggetti attraverso i mezzi di comunicazione messi a disposizione da FBK (sito internet, pubblicazioni, comunicati, ecc.). Queste informazioni non richiedono da parte del soggetto particolari attenzioni di riservatezza. La divulgazione di tali informazioni non presenta implicazioni per FBK in quanto si tratta di informazioni pubbliche che possono essere diffuse.

**Dati e informazioni interne**: sono le informazioni che possono essere trattate dai soggetti esclusivamente all'interno dei processi e del contesto organizzativo di FBK attraverso i canali istituzionali messi a disposizione da FBK (e-mail, intranet, aree di scambio su server e computer, ecc.). Queste informazioni richiedono da parte del soggetto una particolare attenzione nel trattamento, in quanto la loro divulgazione rappresenta una

violazione dei vincoli di riservatezza ai quali è legato ogni soggetto con un possibile impatto legale (per esempio, violazione della privacy), a meno di essere rielaborate in modo da essere declassate a livello pubblico.

**Dati e informazioni riservate**: sono le informazioni che possono essere trattate da gruppi di soggetti autorizzati in virtù del ruolo e di una precisa finalità di trattamento individuata dal Titolare o dal Responsabile del trattamento. Tali informazioni devono essere comunicate solo a soggetti legittimati, valutando lo strumento di comunicazione più appropriato messo a disposizione da FBK in quanto la loro diffusione può avere un rilevante impatto legale (per esempio, violazione della privacy), d'immagine e di competitività per FBK.

**Dati e informazioni strettamente riservate**: sono le informazioni che possono essere trattate esclusivamente da determinati soggetti in base al ruolo ed alle responsabilità ricoperte in FBK. La divulgazione di tali informazioni può produrre gravi danni legali (per esempio, violazione della privacy), di immagine e di competitività per FBK.

## 9. RESPONSABILITÀ PRIVACY

In conformità con il GDPR ed in linea con il suo principio generale di Accountability, FBK ha definito, formalizzato e applicato un modello organizzativo di responsabilità privacy finalizzato al corretto trattamento dei dati personali. Tale modello è coerente con l'organigramma della Fondazione.

In occasione dell'aggiornamento annuale dell'organigramma generale, la Fondazione, in qualità di Titolare del trattamento dei dati personali, aggiorna anche la linea delle responsabilità interne in materia di trattamento dei dati personali, individuando nei Responsabili delle articolazioni e delle sotto-articolazioni organizzative (Centri, Unità, Servizi, Direzioni, ecc.) i Responsabili Interni del Trattamento dei dati personali relativamente ai processi riconducibili alla loro esclusiva competenza. Tali soggetti sono nominati formalmente a valle di una formazione specifica.

Coloro che sono a capo di un progetto che implica il trattamento di dati personali, e non sono contemplati nel Modello Organizzativo di responsabilità privacy, sono tenuti ad adottare una policy *ad hoc* configurata sulle specifiche esigenze del caso (c.d. Privacy by Design). Essi adotteranno tale policy in coordinamento con il Titolare e per il tramite dell'Unità Prevenzione della Corruzione, Trasparenza e Privacy e con il coinvolgimento della Responsabile della Protezione dei Dati personali.

## 10. FBK QUALE RESPONSABILE ESTERNO DEL TRATTAMENTO

In ragione della stipula di contratti, convenzioni, accordi, progetti con soggetti esterni la Fondazione può essere nominata "Responsabile esterno del Trattamento dati ai sensi dell'art 28 del GDPR" quando le vengono affidati compiti specifici per i quali è previsto un trattamento di dati personali per finalità proprie di un soggetto affidatario (che risulta essere Titolare degli stessi).

In tutti questi casi, la Fondazione – anche in fase di stipula degli atti di cui sopra - individua il Responsabile Interno del Trattamento e garantisce l'adozione di misure tecniche e organizzative adeguate atte a soddisfare i requisiti del GDPR.

## 11. REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

Il Registro delle attività di trattamento è un documento di censimento e analisi dei trattamenti effettuati dal Titolare. Il Registro deve essere tempestivamente compilato e mantenuto costantemente aggiornato da ciascun/a Responsabile Interno/a del trattamento dei dati personali poiché il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere. Qualsiasi cambiamento, in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.

## 12. AMMINISTRATORI DI SISTEMA

In conformità ai Provvedimenti del Garante Privacy, la Fondazione individua le figure di "Amministratore di Sistema" in relazione alle tipologie di Reti (indicate all'articolo 25 del presente Regolamento) su cui sono presenti i sistemi amministrati, valutando con attenzione la granularità delle differenti autorizzazioni.

Tali figure si distinguono come di seguito:

a. **Amministratore dei Sistemi gestiti centralmente** nelle reti di tipo "a" e di tutti i sistemi presenti nelle reti di tipo "d": soggetto interno afferente al Servizio Infrastrutture IT e all'Unità FBK Digital.

b. **Amministratore dei Sistemi gestiti dalla ricerca** presenti nelle reti di tipo "b" e "c": soggetto interno afferente alla ricerca individuato dal Direttore di Centro.

c. **Responsabile della gestione autonoma di strumenti e servizi forniti da FBK** e presenti nelle reti di tipo "a": soggetto interno autorizzato dal Responsabile diretto e dal Responsabile del Servizio Infrastrutture IT (rif. Capo V del presente Regolamento).

Il Servizio Infrastrutture IT, in collaborazione con l'Unità FBK Digital, provvede annualmente al censimento di sistemi, applicativi e servizi gestiti centralmente e verifica il censimento di quelli gestiti dai soggetti del comparto della ricerca in modo autonomo per ragioni scientifiche e/o di progetto.

Ogni Direttore di Centro provvede annualmente al censimento di sistemi, applicativi e servizi gestiti dal proprio Centro di Ricerca e, obbligatoriamente, ne condivide le risultanze con il Servizio Infrastrutture IT.

A ciascun sistema, macchina, applicativo e servizio della Fondazione deve corrispondere un "Amministratore di Sistema", nonché l'evidenza del relativo trattamento dei dati personali.

Gli Amministratori di Sistema vengono formalmente nominati dal Titolare del Trattamento a conclusione dell'attività di formazione obbligatoria.

# IV. POLICY DI COMPORTAMENTO

## 13. PRINCIPI GENERALI DEL TRATTAMENTO

Per trattamento di un dato personale si intende ogni operazione, o complesso di operazioni, su un dato personale anche se effettuata senza l'ausilio di strumenti elettronici. Il trattamento di un dato personale, per essere lecito, corretto e trasparente, deve sempre avvenire secondo determinati principi generali privacy. In particolare devono sempre essere rispettati i seguenti principi generali:

a. **principi di liceità, correttezza e trasparenza:** i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato, in modo tale da garantire un'adeguata sicurezza, compresa la protezione - mediante misure tecniche e organizzative adeguate - da trattamenti non autorizzati o illeciti nonché dalla perdita, distruzione o danni accidentali. Quanto alla trasparenza, tutte le informazioni destinate al pubblico o all'interessato devono essere concise, facilmente accessibili e di facile comprensione; il linguaggio utilizzato deve cioè risultare semplice e chiaro.

b. **principio di limitazione della finalità:** gli scopi del trattamento devono essere determinati, espliciti e legittimi; eventuali trattamenti successivi non devono risultare incompatibili con tali scopi. Possono fare eccezione i trattamenti "ulteriori" per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica o storica ovvero per fini statistici.

c. **principio di minimizzazione dei dati e principio di necessità:** i dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto agli scopi per i quali sono trattati. Nello specifico, i sistemi informativi e i programmi informatici devono essere configurati limitando al minimo l'uso di dati personali, in modo da escluderne il trattamento quando gli scopi perseguiti nei singoli casi possano essere realizzate mediante dati anonimi o altre opportune modalità che permettano di identificare l'interessato solo in caso di necessità ('principio di necessità').

d. **principio di esattezza**: i dati trattati devono essere esatti e, se necessario, aggiornati; devono essere, pertanto, adottate tutte le misure ragionevoli per cancellare o rettificare i dati inesatti rispetto agli scopi per i quali sono trattati.

e. **principio di limitazione della conservazione**: fatto salvo per specifici obblighi di legge, trattamenti di archiviazione nel pubblico interesse o per scopi di ricerca scientifica o storica ovvero statistici, i dati trattati devono essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo non superiore a quello necessario al conseguimento degli scopi per cui sono raccolti e trattati.

f. **principio di integrità e riservatezza**: il trattamento deve sempre garantire un'adeguata sicurezza dei dati personali. La sicurezza risulta adeguata quando, anche mediante misure tecniche e organizzative adeguate, la protezione preserva da trattamenti non autorizzati o illeciti, dalla perdita, dalla distruzione e dal danno accidentale.

## 14. TRATTAMENTO DI DATI PERSONALI A FINI STATISTICI E DI RICERCA

L'attività di studio e di ricerca sono importanti vie per ampliare i confini della conoscenza, favorire la crescita delle personalità dei singoli individui e consentire il progresso sociale.

In tale ottica la disciplina in materia di trattamento di dati personali contempla misure semplificate in ambito di ricerca storica, scientifica e statistica. Tuttavia, tali misure non esentano il Titolare dall'adozione di accorgimenti idonei a prevenire possibili violazioni dei diritti degli interessati. Nell'informativa agli interessati, infatti, devono sempre essere chiaramente dichiarati ed esplicitati gli scopi perseguiti dal relativo lavoro statistico o di ricerca.

I dati personali trattati per scopi statistici e di ricerca non possono essere utilizzati per prendere decisioni o provvedimenti relativamente all'interessato, né per trattamenti finalizzati a scopi di altra natura. Tali dati vanno conservati separatamente da ogni altro dato personale trattato per finalità che non richiedano il loro utilizzo.

Le disposizioni relative al segreto statistico e alla riservatezza dei dati personali non si applicano ai dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque.

Al fine di promuovere e sostenere la ricerca e la collaborazione in campo culturale, scientifico e statistico la Fondazione – con esclusione dei dati di natura particolare e giudiziaria - può comunicare e diffondere dati relativi ad attività di studio e di ricerca.

I dati personali devono essere conservati per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti e comunque non oltre 5 anni dalla rendicontazione del progetto. Trascorso tale termine dovranno essere anonimizzati definitivamente oppure cancellati dal personale di ricerca.

Il personale di ricerca della Fondazione è tenuto ad uniformare la propria attività di ricerca e studio alle regole deontologiche promosse dal Garante della Privacy[1] e che sono allegate al Codice di Comportamento della Fondazione.

## 15. PUBBLICAZIONE DI ATTI E DOCUMENTI E DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI

In relazione agli obblighi in materia di trasparenza amministrativa, la Fondazione garantisce il diritto alla riservatezza dei dati personali (in special modo quelli di natura particolare e quelli giudiziaria) ove possibile mediante la non diretta identificabilità dei soggetti cui tali dati si riferiscono o tramite il loro oscuramento.

## 16. RAPPORTI TRA DIRITTO D'ACCESSO E PROTEZIONE DI DATI PERSONALI

I presupposti, le modalità, i limiti per l'esercizio del diritto d'accesso a documenti amministrativi contenenti dati personali e la relativa tutela giurisdizionale restano disciplinati dalla L. 241/1990 e s.m.i. e dalle altre disposizioni di legge in materia, nonché dalla normativa in materia di trasparenza che disciplina il diritto di accesso, anche per ciò che concerne i dati particolari e giudiziari e le operazioni di trattamento, eseguibili in adempimento di una

[1] https://www.garanteprivacy.it/codice

richiesta di accesso. Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.

Quando il trattamento concerne dati idonei a rilevare lo stato di salute o la vita sessuale, il trattamento è consentito, se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

Per quanto riguarda i limiti all'accesso civico generalizzato derivanti dalla protezione dei dati personali, si rinvia alle linee guida ANAC in materia.

## 17. GESTIONE DEI LOCALI E DELLE RISORSE FISICHE

Tutti i locali e tutte le risorse fisiche di FBK devono essere utilizzati e custoditi con la massima diligenza al fine di garantire sia un'efficiente conduzione dell'attività lavorativa sia un adeguato livello di sicurezza delle informazioni.

## 18. ACCESSO AGLI UFFICI E ALLE AREE PROTETTE

**Sede e uffici.** L'accesso agli uffici, alle aree protette, alle aree riservate ed agli archivi cartacei, è permesso ai soggetti autorizzati in quanto muniti di badge personale e solo in base a precise e motivate esigenze lavorative.

Per finalità di sicurezza e tutela del patrimonio della Fondazione, i dati relativi ai transiti tracciati dal badge personale potranno essere resi disponibili ai responsabili dei suddetti uffici, aree e archivi.

Ulteriori e specifici accessi ad uffici ed aree protette potranno essere concessi e abilitati solo a seguito di preventiva e motivata richiesta scritta da parte dei soggetti interessati.

I visitatori e gli ospiti di vario genere potranno avere accesso alle suddette aree di FBK esclusivamente previa registrazione all'accettazione, esibendo il pass di riconoscimento ricevuto all'atto di registrazione e accompagnati da un soggetto interno.

**Data Center.** L'accesso ai locali Data Center di FBK è permesso esclusivamente a personale autorizzato mediante sistema biometrico e badge personale.

In via eccezionale e per breve tempo, nel Data Center è consentito l'accesso anche a visitatori e ospiti di vario genere, purché autorizzati e accompagnati da personale FBK autorizzato. I visitatori e gli ospiti di vario genere dovranno essere adeguatamente istruiti dal personale autorizzato in merito alle caratteristiche dell'ambiente, ai rischi presenti, alle norme comportamentali previste e alle procedure da attuare per prevenire o gestire situazioni di emergenza e di rischio.

Per motivi di sicurezza e per conservare la temperatura costante di esercizio, tutti i varchi di accesso devono restare aperti solamente per il tempo strettamente necessario al passaggio di persone e materiali.

Per motivi di sicurezza è inoltre previsto lo scatto di un'immagine fotografica a chiunque acceda al Data Center di FBK e tale immagine è immediatamente inviata al personale autorizzato al presidio del Data Center.

Le suddette regole valgono anche per il Data Center "di alta disponibilità" identificato nel **sito di Disaster Recovery**.

## 19. GESTIONE E CUSTODIA DEL BADGE

Chiunque operi o transiti nei locali e negli spazi della Fondazione deve essere munito di apposito badge di riconoscimento.

Il badge è considerato un oggetto strettamente personale; esso dovrà quindi essere custodito in modo adeguato e non potrà essere ceduto neppure temporaneamente.

In caso di utilizzo non consentito, il badge potrà essere ritirato dal personale addetto alla sorveglianza. In tali circostanze la Fondazione potrà decidere ulteriori azioni a sua tutela.

In caso di smarrimento del badge, l'interessato o l'interessata dovrà dare pronta comunicazione ai presidi competenti.

Venuti meno i presupposti del relativo rilascio, il badge dovrà essere immediatamente restituito alla competente Unità della Fondazione.

## 20. RIPRESE E REGISTRAZIONI VIDEO-AUDIO-FOTOGRAFICHE ALL'INTERNO DI FBK

Qualsiasi ripresa e registrazione video-audio-fotografica deve essere realizzata rispettando i diritti delle singole persone coinvolte e dei principi generali che ispirano il presente Regolamento.

Per rafforzare la sicurezza interna in un contesto organizzativo in cui le sedi della Fondazione sono accessibili a terzi, l'immagine del profilo personale deve rispettare standard determinati e la sua pubblicazione è, per impostazione predefinita, obbligatoria sul badge personale e sulle Reti interne della Fondazione.

**Soggetti interni**: per ragioni connesse alla propria attività lavorativa le riprese e le registrazioni video-audio-fotografiche devono essere previamente autorizzate dal proprio Responsabile. Tali riprese possono essere utilizzate esclusivamente per finalità lavorative e non possono essere divulgate al di fuori del contesto istituzionale in cui sono state realizzate.

Rimane salva la possibilità di effettuare in prima persona audio-registrazioni necessarie per far valere un proprio diritto in giudizio, per il periodo strettamente necessario allo scopo, rispettando in ogni caso il principio di proporzionalità e minimizzazione, in particolare sotto il profilo spazio-temporale.

In caso di riprese audio-video realizzate per scopi di comunicazione e valorizzazione delle attività lavorative (ad es. riprese per i media, per video di progetto, per documentazione di eventi), esse devono essere previamente autorizzate dal proprio Responsabile d'intesa con il Servizio Comunicazione e Relazioni Esterne.

Al di fuori di questi casi, tenuto conto che la Fondazione investe nel proprio personale, anche al fine di valorizzare il vincolo fiduciario reciproco, è vietato effettuare riprese video-audio-fotografiche in qualunque area di FBK. Le violazioni potranno dare luogo all'attivazione di un procedimento disciplinare.

I soggetti interni potranno essere fotografati e/o ripresi in occasione di eventi, seminari e momenti di formazione e per la documentazione di attività istituzionali con particolare riferimento alle attività di ricerca. In questi casi, le immagini e le riprese potranno essere utilizzate per scopi e comunicazioni istituzionali.

**Soggetti esterni**: è vietato effettuare riprese e registrazioni video-audio-fotografiche in qualunque area di FBK. Eventuali eccezioni devono essere autorizzate dal Servizio Comunicazione e Relazioni Esterne. Il soggetto interno referente dei soggetti esterni presenti in Fondazione è tenuto a far rispettare queste prescrizioni.

## 21. VIDEOCONFERENZE

Le riunioni in videoconferenza devono essere realizzate con gli strumenti messi a disposizione dalla Fondazione (o eventualmente con quelli che si propongono nelle circostanze da parte dei soggetti coinvolti) ed autorizzati dal Servizio Infrastrutture IT, in situazioni protette che garantiscano la tutela delle informazioni condivise.

Le registrazioni delle videoconferenze sono permesse - motivandone le finalità - esclusivamente previo avviso di tutte le persone coinvolte.

## 22. POSTAZIONI DI LAVORO

Le postazioni di lavoro devono essere sempre mantenute in ordine avendo cura di non lasciare mai incustoditi documenti e atti riservati.

## 23. MISURE FISICHE DI CUSTODIA DI DOCUMENTI E ATTI CARTACEI

I dati cartacei ed i supporti cartacei necessari per lo svolgimento delle mansioni lavorative devono essere custoditi in armadi o cassettiere del contesto organizzativo in cui si opera. 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. I documenti dovranno essere 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) dovranno essere custoditi in armadi chiusi a chiave.

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.

Si raccomanda di non lasciare documenti incustoditi presso i dispositivi di stampa.

## 24. GESTIONE E PROTEZIONE DEI DATI PERSONALI E AZIENDALI

**Tutti devono considerarsi personalmente responsabili dei dati e delle informazioni delle quali entrano in possesso per lo svolgimento delle prestazioni assicurate alla Fondazione ovunque queste siano assicurata (in presenza o da remoto).** Tutti devono quindi trattare i dati e le informazioni adottando ogni idonea misura di sicurezza al fine di tutelarne la riservatezza, la sicurezza, l'integrità ed il corretto utilizzo.

I dati e le informazioni potranno essere comunicati a terze parti esclusivamente nell'ambito della propria funzione e secondo le finalità connesse alla propria attività lavorativa.

È vietata la comunicazione di dati e informazioni verso terzi che possano arrecare danno all'immagine, alla reputazione, alla produttività, alla proprietà intellettuale, al *know-how* ed alla redditività della Fondazione o che possano violare i vincoli contrattuali e di legge connessi al rapporto di lavoro.

È assolutamente vietata la divulgazione a terzi di informazioni riservate, confidenziali o comunque di proprietà del Titolare. In caso di violazione, il Titolare si riserva di avviare i relativi provvedimenti disciplinari, nonché le azioni civili e penali consentite.

Si ricorda, inoltre, che la diffusione illecita di dati e informazioni potrebbe configurare, oltre alla violazione del presente Regolamento, la violazione di norme con conseguenze sia civili che penali a carico del responsabile dell'illecita diffusione, nonché come violazione della normativa che regola il rapporto di lavoro.

Fatte salve motivate esigenze di ricerca e le specifiche casistiche contemplate nel presente Regolamento, è vietato l'utilizzo di cifratura (crittografia) che renda illeggibili le informazioni aziendali o che possa causare il blocco di sistemi e applicazioni.

L'accesso ai dati è consentito nei limiti della propria funzione organizzativa e della propria attività lavorativa.

I dischi di rete presenti sui sistemi locali e in servizi cloud gestiti da FBK sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia inerente all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo e amministrazione da parte del personale autorizzato.

Si ricorda che i dischi o altre unità di memorizzazione sui dispositivi in uso agli utenti non sono soggette a salvataggio da parte del personale autorizzato. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo soggetto.

Il Servizio Infrastrutture IT può in qualunque momento procedere alla rimozione di ogni file o applicazione che reputerà pericolosa per la sicurezza sia sugli strumenti informatici dei soggetti, sia sulle unità di rete: di tale intervento ne sono informati il soggetto interessato e il suo diretto Responsabile.

Il **backup** dei principali server di rete viene effettuato dal Servizio Infrastrutture IT, che conserva i backup degli ultimi cinque anni. I soggetti che trattengono dati di FBK in aree per cui non è previsto backup sono responsabili

del salvataggio degli stessi e di eventuali danni a FBK o a terzi anche di natura civilistica causati dalla loro perdita o sottrazione.

Fermi restando i vincoli esistenti a tutela della privacy per il proprio personale, i soggetti devono essere consapevoli che i dati da loro trattati sui sistemi informatici di FBK possono essere di proprietà di FBK o comunque sotto la responsabilità della stessa. Proprio per garantire la sicurezza e l'integrità delle informazioni presenti sui sistemi informatici di FBK, non è possibile garantire in maniera assoluta, in caso di controlli, la segretezza delle informazioni.

La memorizzazione temporanea di dati su strumenti informatici privati è consentita a patto che i suddetti strumenti siano protetti in modo da non consentire l'accesso di estranei non autorizzati e che i dischi siano crittografati.

È vietato il salvataggio di dati e informazioni di carattere professionale in sistemi o *storage* di ***cloud pubblica*** non presenti nel Catalogo dei servizi Cloud per la PA qualificati dall'Agenzia per l'Italia Digitale[2] (AGID) e non autorizzati dal Servizio Infrastrutture IT.

L'utilizzo dei file server, dei sistemi di archiviazione in cloud e dei Source Code Management Server (SCM) è normato da apposite Linee Guida adottate dal Responsabile del Servizio Infrastrutture IT allo scopo di minimizzare il rischio di danni, anche di natura civilistica, causati a FBK o a terzi.

In considerazione del fatto che la Fondazione si relaziona con Pubbliche Amministrazioni, quando si sviluppano software, applicazioni e codici che trattano dati personali, è necessario rispettare ed adottare le indicazioni fornite dall'Agenzia per l'Italia Digitale (AGID) circa le misure di sicurezza ICT, seguendo metodologie di sviluppo che tengano conto dei problemi di privacy e sicurezza informatica.

## 25. STRUMENTI, SERVIZI INFORMATICI E INFOSTRUTTURE

L'utilizzo degli strumenti informatici in dotazione, dei servizi informatici e delle infostrutture a cui il soggetto ha accesso, è di carattere professionale.

In deroga a tale principio FBK consente un moderato e ragionevole utilizzo privato. Tale utilizzo, se e in quanto associato ad una logica di reciprocità, deve essere limitato ed ispirato a criteri di buon senso e non dovrà mai ostacolare l'utilizzo professionale o generare costi per FBK.

Quando lasciati incustoditi, tutti gli strumenti informatici dovranno essere bloccati e protetti da password.

Se non utilizzati per più di un'ora e fatte salve motivate esigenze di ricerca e studio, gli strumenti informatici dovranno essere automaticamente spenti o messi in modalità a basso consumo.

La Fondazione mette a disposizione degli utenti reti logiche e infostrutture dedicate. Le Reti e infostrutture in questione sono quelle certificate dal Servizio Infrastrutture IT secondo la seguente logica:

a. **Per i dispositivi informatici periferici**, riservata ai dispositivi informatici in uso agli utenti quali PC, telefoni, tablet, IoT, stampanti, sia di proprietà di FBK che personali, sia gestiti centralmente che autogestiti, che non potranno offrire servizi diretti o indiretti all'esterno
b. **Per i server autogestiti nel Data Center**, riservata ai server fisici che non devono offrire servizi diretti o indiretti all'esterno;
c. **Per i server autogestiti su cloud**, riservata ai server virtuali che possono offrire anche servizi diretti o indiretti all'esterno;
d. **Per i server gestiti centralmente nel Data Center o su cloud** riservata ai server fisici o virtuali che possono offrire anche servizi diretti o indiretti all'esterno.

Gli Amministratori di Sistema del Servizio Infrastrutture IT sono gli unici soggetti autorizzati all'accesso ai sistemi informatici collegati alle reti a) e d) con privilegi di Amministratore o "root", sia locale che di rete.

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

Sui dispositivi gestiti centralmente, non è consentito modificare in alcun modo il sistema operativo o le applicazioni installate dal Servizio Infrastrutture IT.

Nel caso di utilizzo per finalità lavorative di strumenti privati di tipo portatile, è obbligatorio implementare la protezione dei dati personali o aziendali attraverso sistemi di autenticazione, crittografia dei dischi ed è fortemente consigliato l'utilizzo degli strumenti web clientless messi a disposizione dalla Fondazione per l'accesso ai servizi FBK, in modo da evitare il salvataggio di dati sui dispositivi privati.

La Fondazione ha inoltre, siglato un'apposita Convenzione con il Consorzio della Rete Italiana dell'Università e della Ricerca, che gestisce una rete denominata comunemente "Rete GARR". L'utilizzo dei dispositivi informatici è soggetto al rispetto delle *Acceptable Use Policy* della rete GARR disponibili al seguente link*:* https://www.garr.it/it/regole-di-utilizzo-della-rete-aup.

## 26. CUSTODIA DEGLI STRUMENTI INFORMATICI

Gli strumenti informatici di proprietà della Fondazione devono essere custoditi dagli utenti con cura e diligenza prevenendo possibili danneggiamenti che ne compromettano il corretto funzionamento ed evitando di lasciarli incustoditi soprattutto in ambienti pubblici.

In caso di furto o danneggiamento, l'utente interessato dovrà presentare formale denuncia alle Autorità di pubblica sicurezza e inviarla immediatamente al Servizio Patrimonio che, in coordinamento con il Servizio Infrastrutture IT e l'Unità Prevenzione della Corruzione, Trasparenza e Privacy, attiverà le necessarie procedure interne.

## 27. GESTIONE DELLE CREDENZIALI DI ACCESSO E DELLE PASSWORD

Le credenziali di autenticazione per l'accesso alla rete, alla posta elettronica e ad altri servizi collegati vengono assegnate dal Servizio Infrastrutture IT e consegnate all'utente interessato in occasione del suo primo inserimento nell'organizzazione.

Le credenziali di autentificazione consistono in un codice per l'identificazione degli utenti (username), associato ad una parola chiave riservata (password) che può essere modificata dall'utente al primo utilizzo, dovrà venir custodita dallo stesso con la massima diligenza e non divulgata.

La Fondazione può inoltre configurare ulteriori sistemi obbligatori di controllo degli accessi - doppia autenticazione, biometrici, ecc.

**Tutti gli utenti sono considerati responsabili della sicurezza e di qualunque operazione effettuata utilizzando le proprie credenziali.**

È vietato accedere alle reti, ai servizi o alle infostrutture della Fondazione con credenziali diverse dalle proprie o in maniera anonima.

È vietato usare le credenziali della Fondazione per autenticarsi su servizi di tipo privato quali, ad esempio, siti di commercio elettronico.

Ove disponibile, è obbligatorio attivare l'autenticazione multi fattore (MFA), sia per le credenziali fornite dalla Fondazione sia per le credenziali utilizzate per connettersi a servizi di terze parti per conto della Fondazione.

Le regole relative alle credenziali espresse in questo articolo valgono anche per gli account utilizzati per la gestione di siti web della Fondazione (es. siti di Centro, di progetto e di eventi) e per la gestione di account di social network collegati o riconducibili alla Fondazione. In particolare è obbligatorio attenersi alle politiche interne ed attivare, ove disponibile, l'autenticazione multi fattore (MFA) per le credenziali utilizzate per connettersi ai servizi in parola.

In caso di necessità di rinnovo delle credenziali alla scadenza del rapporto di lavoro, le relative richieste dovranno essere associate ad un rapporto di affiliazione.

## 28. GESTIONE DELLA POSTA ELETTRONICA

L'assegnazione di una casella di posta elettronica della Fondazione ("e-mail FBK") è di carattere professionale. In deroga a tale principio la Fondazione autorizza un moderato e ragionevole utilizzo privato. Tale utilizzo deve essere limitato ed ispirato a criteri di buon senso e non dovrà mai ostacolare l'utilizzo professionale. Lo spazio della casella di posta utilizzato a fini "privati" dovrà perciò essere limitato e non dovrà precludere e limitare quello dedicato all'utilizzo professionale.

In conformità alla disciplina in materia di privacy, ad ogni messaggio e-mail in uscita viene automaticamente aggiunto un breve testo di avviso al ricevente della natura potenzialmente riservata del messaggio.

I titolari dell'e-mail FBK sono responsabili dell'utilizzo della stessa e devono mantenere un corretto comportamento nell'utilizzo della posta elettronica. In particolare, devono essere rispettate le seguenti disposizioni:

a. non inviare né conservare messaggi di posta elettronica e/o allegati dal contenuto offensivo, molesto, volgare, blasfemo, xenofobo, razziale, pornografico o comunque inappropriato o illegale, salvo specifiche esigenze di ricerca;
b. prestare la massima attenzione nell'invio di e-mail contenenti dati personali, che devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alla finalità per la quale sono inviati;
c. prestare la massima attenzione nell'inoltro di e-mail riportanti contenuti e indirizzi e-mail di precedenti comunicazioni;
d. prestare la massima attenzione nell'invio e nell'inoltro di e-mail con allegati che, se contenenti dati personali, devono essere adeguatamente protetti;
e. prestare la massima attenzione ad e-mail sospette, avvisando il Servizio Infrastrutture IT in caso di dubbi sulla provenienza o sul contenuto delle stesse;
f. creare una sezione denominata "Posta personale" all'interno della propria casella di posta, alla quale gli Amministratori di Sistema del Servizio Infrastrutture IT non potranno accedere se non per gravi motivi di sicurezza informatica.

In caso di assenza improvvisa o prolungata del titolare dell'e-mail FBK, per gravi motivi di sicurezza informatica e per urgenti ed improrogabili necessità lavorative, l'accesso e la gestione della relativa casella di posta potrà essere presa in carico dagli Amministratori di Sistema della Fondazione su richiesta del Responsabile Interno del Trattamento dello stesso.

La **Posta Elettronica Certificata (PEC)** può essere utilizzata dagli Incaricati/Autorizzati solamente per motivi professionali.

## 29. UTILIZZO DELLA NAVIGAZIONE INTERNET

L'accesso a Internet è fornito principalmente per scopo professionale, per accedere a informazioni e contenuti necessari allo svolgimento dell'attività lavorativa. Tutti gli utenti abilitati all'accesso sono dunque responsabili del suo corretto utilizzo. Come per la posta elettronica, la Fondazione autorizza un moderato e ragionevole utilizzo privato di Internet, limitato ed ispirato a criteri di buon senso e senza mai ostacolare l'attività professionale.

Il numero e la durata degli accessi a Internet sono costantemente registrati. La consultazione di tali registrazioni può avvenire solo in forma anonima e aggregata salvo i casi previsti dalla legge e dal mancato rispetto del presente Regolamento. Gli eventuali controlli compiuti dal Servizio Infrastrutture IT potranno avvenire mediante un sistema di analisi dei file giornale.

Gli utenti abilitati devono seguire le seguenti regole di navigazione della rete Internet:

a. è tassativamente vietato scaricare materiale e programmi in violazione della legislazione sui diritti di autore, sia che si tratti di materiali o programmi appartenenti a persone o aziende coperti da copyright, brevetto o proprietà intellettuale, sia che si tratti di materiali e programmi non specificatamente licenziato.

b. è tassativamente vietato navigare siti e scaricare materiale pericolosi/vietati o aventi contenuti illegali (contenuto offensivo, molesto, volgare, blasfemo, xenofobo, razziale, pornografico, pedopornografico, terrorismo o comunque inappropriato o illegale), salvo specifiche esigenze di ricerca formalmente autorizzate dal Servizio Infrastrutture IT;

c. è vietato effettuare copia non autorizzata di materiale coperto da copyright nonché la digitalizzazione e la distribuzione di foto da riviste, libri o altre fonti, musica o materiale video;

d. è vietato utilizzare l'infrastruttura tecnologica della Fondazione per procurarsi e diffondere materiale in violazione con le normative vigenti;

e. è vietato effettuare attività che possano generare dei problemi di sicurezza o danneggiare le comunicazioni sulla rete;

f. è vietato eseguire qualsiasi forma di monitoraggio della rete che permetta di catturare dati non espressamente inviati all'host del soggetto (sniffing) a meno che questa attività non faccia parte dei compiti del soggetto e quindi formalmente autorizzata dagli amministratori di sistema;

g. è vietato aggirare le procedure di autenticazione o la sicurezza di qualunque host, rete, account.

## 30. ACCESSO INTERNET PER SOGGETTI ESTERNI

Alle condizioni e con i vincoli di cui all'articolo 29, la Fondazione può motivatamente consentire l'accesso e la navigazione in Internet anche a soggetti esterni.

## 31. ACCESSO ESTERNO ALLE RETI FBK

L'accesso dall'esterno alla rete della Fondazione è consentito esclusivamente attraverso precise modalità di connessione sicura individuate dal Servizio Infrastrutture IT e consultabili sul sito web della Fondazione. Ogni altro accesso è espressamente vietato.

## 32. COMUNICAZIONE DI DATI E INFORMAZIONI ATTRAVERSO SOCIAL MEDIA

È assolutamente vietato pubblicare in internet attraverso social media personali, forum, chat, blog, siti internet, dati ed informazioni di carattere professionale (informazioni, documenti, appunti, commenti personali o di terzi, foto, video, audio, ecc..) che possano arrecare danno all'immagine, alla reputazione, alla produttività e redditività, alla proprietà intellettuale o al know-how della Fondazione ovvero che possano violare i vincoli contrattuali e di legge connessi al rapporto con la Fondazione.

È assolutamente vietato divulgare notizie false.

È autorizzata la divulgazione di informazioni già rese pubbliche da FBK; in caso di dubbi in proposito, la struttura di riferimento è il Servizio Comunicazione e Relazioni Esterne che, per garantire il corretto utilizzo di tali strumenti da parte degli utenti, ha redatto una Social Media Policy e apposite Linee Guida.

## 33. UTILIZZO DELLA FIRMA DIGITALE

La Firma Digitale deve essere utilizzata esclusivamente dal titolare.

## 34. SISTEMI DI MONITORAGGIO

Nel rispetto della normativa sulla privacy e per ragioni comunque estranee a qualsiasi finalità di controllo dell'attività lavorativa, la Fondazione può accedere direttamente a tutti gli strumenti informatici per i seguenti motivi: sicurezza del sistema informatico o manutenzione (ad esempio, aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware, ecc.), controllo e programmazione dei costi (ad esempio, verifica costi di connessione ad Internet, traffico telefonico, ecc.).

Periodicamente e in presenza di anomalie, il Servizio Infrastrutture IT effettua verifiche di funzionalità approfondite che potranno determinare segnalazioni ed avvisi generalizzati diretti ai soggetti della funzione organizzativa in cui è stata rilevata l'anomalia stessa e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.

Il Servizio Infrastrutture IT può inoltre effettuare controlli di carattere impersonale sulla rete e su tutti i dispositivi che la compongono. I dettagli relativi ai controlli effettuati sono disponibili nell'Appendice A.

I controlli devono rispondere ad un principio di sostenibilità e non possono risultare prolungati, costanti o indiscriminati.

La Fondazione ha facoltà di denunciare all'autorità giudiziaria tutti i comportamenti contrari alla legge anche quando rilevati da analisi di tipo impersonale.

## 35. SISTEMA DI VIDEOSORVEGLIANZA

Il sistema di videosorveglianza ha l'esclusivo scopo di salvaguardare l'incolumità delle persone fisiche che frequentano le sedi della Fondazione contro comportamenti illeciti e fraudolenti nonché di controllo e tutela dei beni e del patrimonio contro furti e atti vandalici o, ancora, di controllo degli accessi non autorizzati.

Il sistema è operativo in determinate aree della Fondazione che devono essere adeguatamente segnalate da appositi cartelli informativi,

L'accesso alle immagini videoregistrate è permesso esclusivamente per le finalità sopra indicate agli incaricati/autorizzati al trattamento e, in caso di necessità, agli organi preposti delle forze dell'ordine.

Il Documento sulla Videosorveglianza viene adottato ed aggiornato dal Responsabile della Videosorveglianza, previo accordo con le Rappresentanze Sindacali Aziendali.

## 36. PERDITA DELLE CONDIZIONI DI INCARICATO/AUTORIZZATO

In caso di perdita delle condizioni di Incaricato o Autorizzato al Trattamento o di cessazione del rapporto di lavoro o dell'incarico con la Fondazione valgono le seguenti regole operative:

a. Le credenziali per l'accesso ai sistemi e alla posta elettronica vengono disattivate.
b. Sempre motivando, è facoltà della Fondazione effettuare operazioni di conservazione di e-mail di carattere professionale. Tale facoltà è invece assolutamente esclusa per le e-mail della "Posta personale" che saranno cancellate.

Tali attività possono essere effettuate solo dagli Amministratori di Sistema del Servizio Infrastrutture IT in quanto autorizzati alla gestione della posta elettronica. Essi quindi potranno avere accesso - sempre motivatamente e ove non sia evitabile per esclusive ragioni di carattere tecnico - a dati personali conservati all'interno delle caselle di posta.

Con il dovuto anticipo, ogni utente è tenuto ad attivare il risponditore automatico per notificare ad eventuali fornitori, partner, clienti od altri soggetti interessati, l'interruzione del proprio rapporto con FBK e - se del caso - per proporre un contatto interno alternativo.

Per quanto riguarda la restituzione degli strumenti informatici di proprietà della Fondazione, valgono le seguenti regole operative:

a. Gli smartphone devono essere restituiti al Servizio Patrimonio.
b. Gli strumenti informatici affidati al personale di ricerca comunque inquadrato devono essere resi al Responsabile dell'Unità di Ricerca di appartenenza.
c. Gli strumenti informatici affidati al personale non di ricerca andranno resi al Servizio Infrastrutture IT.

In caso di decesso, salvo diverse disposizioni dello stesso, la Fondazione garantisce l'esercizio dei diritti previsti al Capo III del GDPR a coloro che hanno un interesse proprio riconosciuto, o agiscono a tutela de deceduto, in qualità di mandatari, o per ragioni familiari meritevoli di protezione.

### 37. VIOLAZIONE DI DATI PERSONALI (DATA BREACH)

Per **"violazione di dati personali**" si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

I casi di violazione di dati personali devono immediatamente essere segnalati alla Responsabile della Protezione dei Dati personali (privacy@fbk.eu) assicurando così l'attivazione della procedura di gestione delle violazioni di dati personali.

## V. POSSIBILITÀ DI GESTIONE AUTONOMA DEGLI STRUMENTI E SERVIZI INFORMATICI FORNITI DA FBK

### 38. FINALITÀ

Per assicurare la massima flessibilità alla ricerca, il soggetto interno afferente alle sole articolazioni organizzative di ricerca, previa autorizzazione del/la suo/a diretto/a Responsabile e del Responsabile del Servizio Infrastrutture IT, può ricevere, secondo le disposizioni previste qui di seguito, la completa delega della gestione di strumenti e servizi informatici forniti da FBK per esclusive finalità di ricerca scientifica, assumendo la piena responsabilità dell'utilizzo degli strumenti e servizi.

### 39. RESPONSABILITÀ

Il soggetto interno dovrà effettuare una attività propedeutica e periodica di formazione con il fine ultimo, da un lato di fornire concetti base riguardanti le misure adeguate di sicurezza ed i generali obblighi previsti dalla normativa vigente in materia di protezione dei dati personali, e dall'altro di chiarire che risponde personalmente di eventuali violazioni poste in essere mediante lo strumento gestito in autonomia (es: violazioni normative a tutela della protezione dei dati personali, della proprietà intellettuale, del diritto d'autore, etc…)

Il soggetto interno accetta la conseguente designazione quale "Responsabile della gestione autonoma di strumenti e servizi informatici forniti da FBK" figura che deve 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 il mantenimento di un adeguato livello di sicurezza dei dati di cui FBK è Titolare.

Nel caso in cui lo strumento o il servizio informatico sia condiviso tra più soggetti, il Responsabile della gestione in autonomia sarà il Responsabile dell'Unità di Ricerca.

### 40. REGOLE DI UTILIZZO

Quelle che seguono sono le regole di utilizzo dei suddetti strumenti e servizi informatici gestiti in autonomia:

a. Sarà consentito l'accesso ad Internet.

b. L'accesso ai suddetti strumenti e servizi sarà possibile attraverso i sistemi di collegamento remoto messi a disposizione dalla Fondazione e seguirà le stesse regole valide per gli strumenti privati.

c. Gli strumenti ed i servizi così configurati non potranno essere collegati alla rete di tipo "d" indicata all'articolo 25 di questo Regolamento.

d. Gli strumenti e i servizi informatici non potranno offrire servizi verso Internet né diretti né indiretti a meno che non siano collegati alla rete di tipo “c” indicata all’articolo 25 di questo Regolamento.

e. Gli strumenti non dovranno interferire con il normale funzionamento della rete.

f. La gestione in autonomia implica capacità di gestione e debug degli strumenti informatici. L’installazione del sistema operativo sarà a cura del richiedente. Non è previsto il backup da parte del Servizio Infrastrutture IT. Il supporto del Servizio Infrastrutture IT sarà limitato alla sola parte hardware come previsto dalla garanzia. Nessun supporto sarà previsto per problemi software.

g. Sul sito web della Fondazione sono presenti le istruzioni per il collegamento e le modalità di debug per la connessione alle diverse reti.

h. I suddetti strumenti e servizi dovranno essere continuamente aggiornati, sia per la parte di sistema operativo sia per la parte relativa alle applicazioni, in modo da mitigare eventuali problemi di sicurezza. Nel caso in cui i sistemi operativi o le applicazioni non vengano aggiornati per qualsiasi motivo, gli strumenti dovranno essere immediatamente spenti. In caso contrario il Servizio Infrastrutture IT disabiliterà, previo avvertimento, l’accesso alle reti dei suddetti sistemi. Questa regola è valida, per quanto riguarda gli strumenti e i servizi gestiti dalla ricerca, anche per i sistemi gestiti centralmente.

i. Sugli strumenti autogestiti o privati di tipo portatile è obbligatorio implementare la protezione attraverso sistemi di autenticazione - password, biometrica, doppio fattore, ecc. - ed è fortemente consigliato l’utilizzo degli strumenti web clientless messi a disposizione dalla Fondazione per l’accesso ai servizi FBK, in modo da evitare il salvataggio di dati sui dispositivi. Nel caso in cui, esclusivamente per finalità lavorative, sia necessario trattare dati personali o informazioni importanti sulle memorie locali degli strumenti, è obbligatoria la crittografia dei dischi.

## VI. SPECIFICI DIVIETI

### 41. DIVIETI

Di seguito sono riportati specifici divieti per i destinatari di questo Regolamento:

a. alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;

b. accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;

c. accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e /o cancellare dati e/o informazioni;

d. detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico o di soggetti concorrenti, pubblici o privati al fine di acquisire informazioni riservate;

e. svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l’interruzione, totale o parziale, o l’alterazione del suo funzionamento;

f. svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni;

g. svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;

h. svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;

i. distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità;

j. caricare programmi non provenienti da una fonte certa e autorizzata dalla Fondazione;

k. acquistare licenze software da una fonte (rivenditore o altro) non certificata e non in grado di fornire garanzie in merito all’originalità/autenticità del software;

l. detenere supporti di memorizzazione di programmi non originali;

m. installare un numero di copie di ciascun programma ottenuto in licenza superiore alle copie autorizzate dalla licenza stessa, al fine di evitare di ricadere in possibili situazioni di *underlicensing*;

n. utilizzare illegalmente password di computer, codici di accesso o informazioni simili per compiere una delle condotte sopra indicate;

o. utilizzare strumenti o apparecchiature, inclusi programmi informatici, per decriptare software o altri dati informatici;

p. distribuire software di proprietà della Fondazione a soggetti terzi;

q. realizzare codice software che violi copyright di terzi;

r. accedere illegalmente e duplicare banche dati.

## VII. DISPOSIZIONI FINALI

### 42. RESPONSABILITÀ E SANZIONI

Il mancato rispetto o la violazione di quanto stabilito dal presente Regolamento potrà comportare l'attivazione di procedimenti disciplinari e risarcitori, nonché eventuali azioni civili e penali.

Il mancato rispetto o la violazione del presente Regolamento può inoltre giustificare l'immediata sospensione dell'uso e dell'accesso agli strumenti e ai servizi informatici della Fondazione.

### 43. AGGIORNAMENTO E REVISIONE

Il presente Regolamento è soggetto a revisione periodica, che potrà avvenire a seguito di cambiamenti organizzativi e normativi o necessità istituzionali. Tutte le future modifiche al presente Regolamento verranno opportunamente comunicate e rese pubbliche sul sito internet della Fondazione.

Letto ed approvato il 18 novembre 2022

- prof. Francesco Profumo -

Presidente della Fondazione Bruno Kessler

FIRMATO IN ORIGINALE

## Appendice A

### Dettagli relativi alle attività di controllo svolte dagli Amministratori di Sistema del Servizio Infrastrutture IT

FBK gestisce i sistemi informatici e le reti anche attraverso strumenti che possono memorizzare temporaneamente dati relativi alla navigazione internet e al traffico telematico. In particolare si elencano:

1. Posta Elettronica - dati conservati:
   a. log del traffico SMTP generato dai server di posta elettronica;
   b. log dei messaggi non correttamente inoltrati (ritardi e/o mancate consegne);
   c. log dei messaggi intercettati dal sistema antivirus.
2. Traffico IP – corretto funzionamento del sistema, monitoraggio SLA, controlli di sicurezza:
   a. Log del traffico IP generato dai dispositivi informatici. Tale log comprende anche dati puntuali di navigazione riferibili all'indirizzo IP interno di provenienza della richiesta. I dati sono conservati per circa 26 settimane in un sistema accessibile solo dagli Amministratori di sistema autorizzati, e non utilizzato normalmente per altre attività di FBK. Tuttavia potranno essere conservati per tempi superiori per giustificate ragioni tecnico/organizzative, per garantire l'esercizio o la difesa di un diritto in sede giudiziarie e in tutti i casi in cui sia richiesto dall'autorità giudiziaria.
3. Telefonia – corretto funzionamento del sistema:
   a. Log delle chiamate (numero chiamante, numero chiamato, durata).
4. Accesso alle reti - corretto funzionamento del sistema, monitoraggio SLA e controlli di sicurezza:
   a. Log di accesso alle reti dall'esterno e dall'interno.

FBK effettua controlli a campione sugli strumenti gestiti in autonomia dal personale di ricerca al fine di verificare l'effettivo rispetto del Regolamento Privacy e l'applicazione delle misure standard di sicurezza di FBK.

Come indicato nelle Linee Guida del Garante Privacy per posta elettronica e internet[3], FBK non procederà in nessun caso a controlli non consentiti, quali:

- lettura e registrazione puntuale di messaggi di posta;
- riproduzione e memorizzazione delle pagine internet visitate;
- cattura dei caratteri digitati attraverso tastiera (fisica o virtuale);
- analisi occulta dei pc affidati in uso.

[3] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1387522