# Policy in materia di protezione dei dati personali e sicurezza delle informazioni

*(approvata nella seduta del Consiglio Federale il 26 settembre 2023 D.F. n. 54/2023)*

**INDICE**

# 1. PREMESSA

## 1.1 Obiettivo del documento

Il presente documento definisce le regole generali adottate dalla Federazione Arrampicata Sportiva Italiana (di seguito, "FASI") per la disciplina degli adempimenti connessi al Trattamento dei Dati Personali.

## 1.2 Quadro normativo di riferimento

- Regolamento UE 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (di seguito anche "**GDPR**");
- Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali, del Garante Italiano della Privacy;
- Guidelines on Personal Data Breach notification under Regulation 2016/679 – wp250 del WP29;
- Guidelines on the right to data portability under Regulation 2016/679 del WP29;
- Decreto Legislativo 30 giugno 2003, n.196 "Codice in materia di protezione dei dati personali" - Testo integrato con le modifiche introdotte dal Decreto legislativo 10 agosto 2018 n.101.

## 1.3 Definizioni

Dato personale (art. 4, n. 1, del GDPR): qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Dati genetici (art. 4, n. 13, del GDPR): i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

Dati relativi alla salute (art. 4, n. 15, del GDPR): i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

Dati biometrici (art. 4, n. 14, del GDPR): i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

Violazione dei dati personali o "data breach" (art. 4, n. 12, del GDPR): 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;

Interessato (art. 4, n. 1, del GDPR): la persona fisica identificata o identificabile. L'interessato si identifica in colui che ha conferito i propri dati personali al Titolare del trattamento;

Autorizzato al trattamento (o Incaricato) (art. 4, n. 10, del GDPR): la persona fisica, dipendenti e collaboratori a qualsiasi titolo, autorizzato a trattare i dati personali dal Titolare del trattamento;

Responsabile della Protezione dei Dati Personali (c.d. Data Protection Officer o DPO) (artt. 37, 38 e 39 del GDPR): il Titolare del trattamento e il Responsabile del trattamento designano sistematicamente un DPO, nei casi espressi dalla normativa di riferimento. Il Titolare del trattamento e il Responsabile del trattamento si assicurano che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali, fornendogli le risorse e gli strumenti necessari per assolvere ai propri compiti;

Responsabile del trattamento (ai sensi dell'art. 4, n. 8, del GDPR): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;

Titolare del trattamento (ai sensi dell'art. 4, n. 7, del GDPR): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

Trattamento (ai sensi dell'art. 4, n. 2, del GDPR): qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto /interconnessione, la limitazione, la cancellazione o la distruzione;

Amministratore di sistema (Provvedimento Garante Privacy del 27.11.2008, modificato il 26.06.2009): la figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, nonché all'amministrazione di base dati, di reti, di apparati di sicurezza e di sistemi software complessi.

## 2. RUOLI E RESPONSABILITÁ NELLA GESTIONE DEI DATI PERSONALI

Le responsabilità interne definite dalla Federazione in materia di protezione dei dati e sicurezza delle informazioni e infrastrutture di supporto sono contenute nella seguente tabella:

| Ruolo in Federazione | Ruolo nel GDPR | Compiti e Responsabilità |
|---|---|---|
| **Consiglio Federale (CF), in persona del Presidente federale** | Titolare del trattamento | - definisce le strategie della Federazione, approva gli obiettivi e le policy e le metodologie per la sicurezza e protezione dei dati personali della Federazione, stanziando le risorse necessarie;<br>- monitora l'adeguatezza e l'efficacia del sistema di protezione e sicurezza dei dati ed è informato sulle principali tematiche in materia privacy;<br>- nomina il DPO su proposta del Presidente;<br>- è responsabile dell'adeguatezza ed efficacia del sistema di protezione dei dati e sicurezza delle informazioni, definendo le policy e le metodologie per la sicurezza e protezione dei dati e il risk appetite della Federazione;<br>- individua i compiti e le responsabilità relative al sistema di protezione dei dati e sicurezza delle informazioni da delegare ai Responsabili delle strutture federali per i trattamenti di propria competenza e nomina i Responsabili del trattamento e gli Amministratori di Sistema;<br>- è informato in caso di data breach e provvede, ove necessario, alla notifica al Garante Privacy nonché alla comunicazione nei confronti dell'Interessato. |
| **Segretario Generale** | Referente privacy<br>(*risk owner)* | - è responsabile della protezione e sicurezza dei dati trattati dalla Federazione e garantisce l'adeguatezza e l'efficacia delle misure di sicurezza;<br>- in caso di acquisizione di nuovi sistemi applicativi ovvero di servizi di sviluppo o manutenzione di software, database e infrastrutture, coinvolge il DPO già in fase precontrattuale, al fine di definire gli aspetti relativi alla privacy e sicurezza IT; ove necessario, informa altresì i Responsabili delle altre strutture coinvolti;<br>- garantisce l'osservanza degli adempimenti privacy sui trattamenti della Federazione (informative, consenso, nomine a responsabile del trattamento, elenco incaricati e relative istruzioni) con il supporto del DPO e l'aggiornamento delle informazioni presenti nel Registro delle attività di trattamento di propria competenza;<br>- aggiorna il DPO in merito all'attività di cancellazione dei dati personali in conformità al termine fissato, per ciascun trattamento di propria competenza, nel Registro dei Trattamenti;<br>- effettua, ove necessario, la Valutazione di impatto sulla protezione dei dati personali (Data Protection Impact Assessment o DPIA) sui nuovi trattamenti, con il supporto del DPO;<br>- comunica al DPO potenziali data breach, qualora ne venisse a conoscenza, fornendo supporto agli stessi nel reperire le informazioni utili alla gestione e valutazione dell'evento, nonché provvede all'implementazione delle misure correttive individuate;<br>- fornisce le istruzioni al proprio personale sulla gestione delle attività in materia di privacy e sul corretto utilizzo dei dispositivi federali, predisponendo l'elenco degli Incaricati al trattamento della propria struttura; |

| Ruolo in Federazione | Ruolo nel GDPR | Compiti e Responsabilità |
|---|---|---|
| | | - aggiorna l'elenco dei Responsabili del trattamento e degli Incaricati al trattamento della Federazione sulla base delle informazioni fornite dai Responsabili delle strutture federali;<br>- provvede all'esercizio dei diritti degli Interessati, in collaborazione con il DPO, predisponendo e inviando la risposta agli Interessati sulla base delle informazioni fornite dalle altre strutture federali;<br>- gestisce il Registro delle Violazioni rispetto alle segnalazioni di data breach e il Registro delle Istanze degli Interessati rispetto alle istanze degli Interessati pervenute, curando l'archiviazione della relativa documentazione. |
| **Personale** | Autorizzato al trattamento (o "Incaricato") | - esegue il trattamento dei dati all'interno delle attività di propria competenza, garantendo la protezione dei dati personali e la sicurezza delle informazioni, in conformità alle procedure federali di riferimento e alle istruzioni fornite dal proprio Responsabile;<br>- segnala al Segretario Generale eventuali inadeguatezze nel processo di trattamento dei dati personali, difformità rispetto alle procedure in materia di privacy ovvero potenziali data breach (in caso di urgenza, informa direttamente il DPO), qualora ne venisse a conoscenza. |
| **Professionista Esterno** | DPO | - fornisce al Titolare del trattamento e ai suoi dipendenti consulenza e chiarimenti in materia di privacy;<br>- monitora il sistema di protezione dei dati e sicurezza delle informazioni all'interno della Federazione attraverso verifiche semestrali;<br>- fornisce, se richiesto, un parere in merito alla DPIA e ne sorveglia lo svolgimento;<br>- aggiorna il Titolare del trattamento mediante relazione annuale sul sistema di protezione dei dati e sicurezza delle informazioni e, in via straordinaria, in caso di sopraggiunte questioni in ambito privacy;<br>- monitora la completa e corretta implementazione delle misure in materia di protezione dei dati personali;<br>- coopera e funge da punto di contatto con l'Autorità Garante per la protezione dei dati personali per questioni connesse al trattamento dei dati personali. |

## 3. LINEE GUIDA SUL TRATTAMENTO DEI DATI

### 3.1 Principi Generali

I referenti federali coinvolti nelle attività di raccolta, conservazione ed utilizzo di Dati Personali operano nel rispetto della normativa interna e del sistema di poteri e responsabilità adottato dalla Federazione, nonché in piena conformità con il GDPR e con il Codice Privacy, ispirandosi ai seguenti principi fondamentali:

**i)** ogni Trattamento dei Dati Personali deve svolgersi nel rispetto dei diritti e delle libertà fondamentali e della dignità dell'Interessato, con particolare riferimento alla riservatezza, all'identità personale ed al diritto alla protezione dei Dati Personali, in coerenza con i principi normativi previsti per il loro esercizio;

**ii)** i Dati Personali devono essere:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato *("liceità, correttezza e trasparenza*");

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità *("limitazione della finalità*");

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("*minimizzazione dei dati*");

d) esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("*esattezza*");

e) conservati in una forma che consenta l'identificazione degli Interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati ("*limitazione della conservazione*");

f) trattati in maniera da garantire un'adeguata sicurezza dei Dati Personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da Trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ("*integrità e riservatezza*");

**iii)** la Federazione collabora con l'Autorità di controllo, anche con riferimento specifico ad eventuali casi di notifica di violazioni di dati personali, allo scopo di garantire il pieno rispetto dei diritti dell'Interessato e di fornire tutte le informazioni necessarie all'Autorità di controllo;

**iv)** ogni Trattamento dei Dati Personali deve essere avviato in maniera trasparente, rendendo all'Interessato idonea informativa in merito alle finalità, tempistiche, comunicazione e diffusione del Trattamento stesso e acquisendone, in tutti i casi previsti dalla legge, il consenso in maniera formale, espressa e libera.

### 3.2 Privacy by Design e Privacy by Default

Il GDPR richiede il rispetto del principio di *Privacy by Design*, che impone di tenere conto dei principi generali di cui al GDPR fin dalle fasi di sviluppo e progettazione di nuove iniziative e/o servizi, nonché del principio di *Privacy by Default* , che prevede che il Titolare debba effettuare il Trattamento con modalità tali da garantire che questo, per impostazione predefinita, sia limitato a quei Dati Personali che siano strettamente necessari al perseguimento delle finalità e strutturato in modo da garantire il più ampio rispetto dei diritti e delle libertà degli Interessati.

### 3.3 Registro dei trattamenti

La Federazione garantisce la piena conoscenza e tracciabilità dei dati personali trattati. In questo contesto FASI ha provveduto alla predisposizione e all'aggiornamento del "Registro delle attività di trattamento" in qualità di Titolare.

All'interno del "Registro delle attività di trattamento" la Federazione riporta le seguenti informazioni minime:

- il nome e i dati di contatto del Titolare, di eventuali contitolari del trattamento e del DPO;
- le finalità del trattamento;
- la descrizione delle categorie di interessati e delle categorie di dati personali trattati;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale, e, per i trasferimenti di cui al secondo comma dell'articolo 49 del Regolamento, la documentazione delle garanzie adeguate;
- i termini previsti per la cancellazione delle diverse categorie di dati personali;
- una descrizione generale delle misure di sicurezza tecniche e organizzative poste in essere per il trattamento in sicurezza dei dati.

Nel caso in cui la Federazione agisca in qualità di Responsabile del trattamento di dati personali provvede alla predisposizione ed all'aggiornamento del "Registro delle attività di trattamento" in qualità di Responsabile, come sancito dall'art. 30 comma 2 del GDPR.

L'aggiornamento del Registro può comportare, a titolo esemplificativo:

- l'eliminazione dei trattamenti di dati personali non più effettuati;
- l'integrazione dei trattamenti in precedenza non censiti i quali dovranno essere prontamente comunicati dagli autorizzati per garantire un aggiornamento continuo;
- la modifica delle informazioni relative ai trattamenti ancora in essere, laddove queste risultino non più corrispondenti ai trattamenti effettuati (ad es. nei casi in cui siano intervenute modifiche organizzative che possano comportare modifiche nell'esecuzione del trattamento).

### 3.4 Misure di sicurezza

La Federazione definisce ed implementa adeguate misure di sicurezza, anche in ambito informatico, per assicurare la tutela dei Dati Personali, tenendo conto – *inter alia* - della natura, dell'oggetto, del contesto e delle finalità del trattamento, del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

La Federazione si assicura che chiunque agisca sotto la sua autorità e abbia accesso a Dati li tratti previe istruzioni in tal senso. Nell'espletamento delle attività poste in essere dalla Federazione, infatti, gli Incaricati devono mettere in atto misure tecniche ed organizzative idonee ad assicurare che, per impostazione predefinita, i Dati Personali non siano resi accessibili ad un numero indefinito di persone e che, al contrario, l'accessibilità agli stessi sia limitata in base ai principi sanciti dal GDPR.

In tal senso, l'accesso deve essere reso disponibile esclusivamente a quei soggetti che sono tenuti al Trattamento di quei Dati Personali per il raggiungimento delle finalità perseguite dalla Federazione.

La Federazione definisce nel capitolo 4 "Utilizzo dei sistemi informatici" le direttive che i soggetti coinvolti nelle attività di Trattamento (ossia, Incaricati e Amministratori di sistema) devono seguire nell'utilizzo dei sistemi informatici che implica qualsivoglia Trattamento dei Dati Personali di dipendenti, collaboratori, tesserati o altri soggetti terzi di cui la Federazione sia Titolare.

## 4. UTILIZZO DEI SISTEMI INFORMATICI

### 4.1 Principi generali

Le risorse informatiche fornite dalla Federazione ai propri dipendenti, collaboratori, incaricati e tesserati che ricoprono un ruolo nelle strutture organizzative federali (di seguito "**Utenti**") devono essere utilizzate per lo svolgimento delle proprie mansioni con modalità e comportamenti adeguati ai compiti e alle responsabilità loro assegnati, nel rispetto dei principi di correttezza e diligenza nonché delle altre normative e direttive federali applicabili.

Gli Utenti devono utilizzare le risorse informatiche solo per finalità di lavoro. Nell'ipotesi di utilizzo delle risorse per scopi non immediatamente correlati alle mansioni federali, fermo il rispetto dei richiamati principi di correttezza e diligenza, gli Utenti si impegnano a non mettere in alcun modo a repentaglio la disponibilità, l'integrità e la riservatezza dei dati, delle informazioni e del sistema informatico della Federazione ovvero a non provocare alla stessa un danno, nonché a impiegare, comunque, modalità che non arrechino intralcio e/o rallentamento alla normale attività propria e di terzi. Gli Utenti sono responsabili del corretto utilizzo delle risorse loro assegnate.

Nell'esecuzione della propria attività lavorativa, gli Utenti devono anzitutto attenersi alle seguenti istruzioni generali:

- effettuare la propria attività lavorativa e professionale uniformandosi alle presenti disposizioni federali e alle istruzioni impartite;
- custodire le risorse informatiche loro affidate in modo appropriato e diligente, segnalando tempestivamente ogni danneggiamento, furto o smarrimento secondo le modalità descritte nelle relative procedure organizzative;
- mantenere la riservatezza sugli argomenti di cui siano venuti a conoscenza o in possesso nello svolgimento della propria attività, astenendosi dalla loro divulgazione a terzi, al di fuori dello svolgimento delle attività stesse, e attenendosi alle procedure o prassi federali vigenti o alle istruzioni ricevute dal segretario generale;
- astenersi, in caso di cessazione dell'attività, dalla diffusione di informazioni e di documentazione di cui siano venuti a conoscenza o con cui siano venuti in contatto durante lo svolgimento dell'attività lavorativa e, in particolare, astenersi dal conservarli, duplicarli, comunicarli o cederli a terzi;
- non detenere o diffondere documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, etnia, opinione e/o appartenenza politica o sindacale;
- adottare tutte le misure di sicurezza indicate nelle disposizioni federali, in modo da evitare i rischi di perdita o distruzione (anche accidentali) dei dati, nel rispetto delle policy federali in tema di sicurezza delle informazioni e privacy;
- non utilizzare abusivamente credenziali altrui e non accedere senza previa autorizzazione a risorse informatiche (artt. 494 e 615-ter del Codice penale);
- non utilizzare sistemi di crittografia, codificazione o protezione dei dati non autorizzati dalla Federazione;
- garantire una corretta custodia di atti e documenti cartacei di cui siano in possesso in ragione dell'attività svolta, tenendo conto che i documenti non possono essere lasciati incustoditi sulla propria scrivania (c.d. clean desk policy) e/o in aree comuni e non devono essere consultati da altri Utenti non abilitati all'attività; inoltre, i documenti non devono essere riprodotti o fotocopiati se non per esigenze connesse all'attività da svolgere;

- procedere alla distruzione della documentazione cartacea di cui non è più necessaria la conservazione, attraverso appositi apparecchi "distruggi documenti", oppure manualmente in modo che non ne sia più ricostruibile il contenuto; in caso di documentazione in formato elettronico, procedere alla cancellazione in modo definitivo dal supporto informatico ove la stessa è registrata;
- evitare accessi non autorizzati alle risorse; non entrare in locali ad accesso limitato, se non previa espressa autorizzazione del segretario generale o di un suo delegato;
- evitare di abusare delle risorse comuni, monopolizzandone l'uso o limitandone la disponibilità agli altri utenti;
- rispettare la normativa in materia di diritto d'autore e proprietà intellettuale, le licenze d'uso e l'integrità di risorse informative basate su computer;
- rispettare, in generale, i diritti degli altri Utenti di risorse informatiche.

### 4.2 Integrità delle risorse informatiche

Gli Utenti devono rispettare l'integrità delle risorse informatiche, secondo quanto di seguito precisato:

a) *inserimento, rimozione o modifica di apparati di rete* – gli Utenti non devono inserire, modificare o rimuovere apparati in rete senza preventiva autorizzazione degli Amministratori di rete;

b) *abusi nell'utilizzo di risorse informatiche* – gli Utenti non devono abusare delle risorse informatiche della FASI, alterandole o facendone un uso improprio. Ciò include, a titolo esemplificativo e non esaustivo:

- tentativi intenzionali di accedere o apportare modifiche ad informazioni di proprietà della FASI per cui l'Utente non possieda idonea autorizzazione;
- tentativi di apportare modifiche a sistemi o altre risorse informatiche per cui l'Utente non possieda idonea autorizzazione;
- invio intensivo di posta elettronica indesiderata o invasiva (c.d. *spam*);
- stampa di copie cartacee per fini non istituzionali di documenti, file, dati o programmi;
- modifiche di configurazioni di sistemi di uso collettivo che non siano state autorizzate dagli Amministratori di sistema o che violino copyright esistenti;
- tentativi di bloccare o creare interferenze a computer, reti, servizi o altre risorse informatiche della FASI;
- attività che portino in qualunque modo alla saturazione dei sistemi di elaborazione e di trasmissione dati, rendendo anche temporaneamente indisponibili risorse di uso comune agli Utenti;
- danneggiamento o vandalismo nei confronti di attrezzature di calcolo, apparati, software, file o altre risorse informatiche;

c) *Programmi pericolosi* – gli Utenti devono assicurarsi e garantire di non sviluppare o usare programmi che interferiscano con l'attività di altri Utenti, o che modifichino parti del sistema o che accedano ad informazioni private o riservate. L'uso di tali programmi espone ad azioni legali di carattere civile o penale da parte dei danneggiati e a richieste di risarcimento da parte della FASI;

d) *Gestione dei dispositivi di elaborazione personali* – gli Utenti sono tenuti ad applicare ai dispositivi di elaborazione personali, di cui hanno disponibilità, le cure necessarie per una corretta manutenzione, includendo tra queste:

- attivazione del controllo d'accesso al dispositivo mediante autenticazione (*username* e password);
- installazione e manutenzione in efficienza dei sistemi antivirus;

- attuazione di *backup* sistematici;
- verifiche di sicurezza relative all'immissione in rete.

e) *Accesso non autorizzato* – gli Utenti che utilizzano le risorse informatiche della FASI non devono accedere a computer, software, dati, informazioni o reti senza appropriata autorizzazione, o abilitare altri all'accesso non autorizzato, indipendentemente dal fatto che le risorse citate appartengano o meno alla FASI. Un Utente che sia stato autorizzato ad utilizzare un account protetto tramite password o altra tecnologia è tenuto a custodire con cura e a mantenere riservate le chiavi d'accesso relative all'account. L'Utente è personalmente soggetto a responsabilità civili e penali, in caso di abusi o incidenti di sicurezza, nel caso divulghi la password o renda accessibile ad altri l'account senza il consenso dell'Amministratore di sistema. Ogni anomalia scoperta in account di sistema o relativa alla sicurezza di sistemi o reti deve essere segnalata tempestivamente all'Amministratore di sistema preposto, in modo che possano essere attuati gli opportuni passi per investigare sui problemi e risolverli;

f) *Diritto d'autore e licenze d'uso* – gli Utenti devono rispettare la normativa in materia di diritto d'autore, copyright e licenze d'uso di software, materiali audiovisivi, documenti ed ogni altra informazione digitale protetta a norma di legge:

- *Copia* – Ogni materiale protetto da diritto d'autore non deve essere copiato al di fuori di quanto specificato dal proprietario dei diritti o di quanto consentito dalla legge sul Diritto d'autore;
- *Uso delle informazioni e dei materiali* – Tutte le informazioni soggette a Diritto d'autore (testi, immagini, icone, programmi, video, audio, etc.) ottenute da computer o risorse di rete devono essere usate in conformità alle leggi vigenti e al presente regolamento. L'origine del materiale copiato deve essere correttamente attribuita ed evidenziata.

### 4.3 Composizione del sistema informativo della FASI

Il sistema informativo di FASI è composto da:

- sistemi operativi e applicativi, anche in cloud, di proprietà della Federazione o in housing presso terzi, ad uso di tutta la struttura federale;
- rete LAN che permette la comunicazione dei dispositivi fissi.

### 4.4 Casi di esclusione di utilizzo delle risorse informatiche

Hanno diritto all'utilizzo delle risorse informatiche e ai relativi accessi i soli Utenti. Le esclusioni dall'utilizzo delle risorse informatiche sono strettamente connesse alla destinazione lavorativa degli strumenti stessi, nonché ai principi di limitazione delle finalità e di minimizzazione, di cui all'art. 5, par. 1, lettere b) e c) del GDPR.

I casi di esclusione di utilizzo delle risorse informatiche saranno comunicati individualmente, e potranno riguardare una o più delle seguenti attività:

- utilizzo del PC;
- utilizzo della posta elettronica (ordinaria e certificata);
- accesso a Internet;
- accesso ai sistemi e applicativi di rete federali;
- accesso rete LAN e Wi-Fi.

Tali esclusioni hanno la finalità di ridurre, a titolo cautelativo e preventivo, i pericoli e le minacce esposti nell'introduzione del presente documento, in ottemperanza con l'art. 32 del GDPR in materia di misure

tecniche e organizzative di sicurezza, nonché con quanto previsto dal Provvedimento del Garante Privacy del 1° marzo 2007, recante le *Linee guida per posta elettronica e Internet*, con il quale il datore di lavoro è chiamato ad adottare ogni misura in grado di prevenire il rischio di utilizzi impropri, così da ridurre controlli successivi sui lavoratori.

### 4.5 Modalità d'utilizzo e gestione delle postazioni di lavoro fisse e mobili

#### 4.5.1 Postazione di lavoro fissa

L'assegnatario di una postazione di lavoro ha la responsabilità individuale dell'utilizzo e della gestione della postazione stessa. Pertanto, ogni Utente è tenuto al rispetto delle seguenti regole comportamentali:

a) controllare e custodire la postazione assegnata in modo tale da impedirne l'acceso a persone non autorizzate;

b) utilizzare il codice identificativo (c.d. *user-id*) e la password riservata assegnati per l'accesso alla postazione, modificando quest'ultima periodicamente secondo le politiche di sicurezza federali;

c) custodire la password garantendone la segretezza; a tale fine deve essere evitata la digitazione in presenza di terzi e, se necessario, conservare la password in un luogo non accessibile a terzi (es. deve essere assolutamente vietata l'apposizione sullo schermo del terminale di biglietti o adesivi contenenti riferimenti alla password); deve altresì evitarsi l'uso di sistemi automatici di inserimento della password, ad eccezione delle soluzioni federali comunicate dalle strutture tecniche competenti in materia di sicurezza informatica;

d) bloccare la propria sessione di lavoro in tutti i casi di allontanamento, anche temporaneo, dalla postazione di lavoro (es. pausa pranzo) e comunque, ove non già impostato, attivare la funzione di *screen saver* con password di accesso in caso di mancato utilizzo della postazione per un periodo limitato di tempo (indicativamente, non superiore a 10 minuti);

e) spegnere la postazione di lavoro assegnata e le relative periferiche al termine dell'orario di lavoro (tranne nei casi in cui sia stata impartita un'autorizzazione in senso contrario dal segretario generale);

f) utilizzare la postazione di lavoro con la configurazione hardware e software fornita dalla Federazione; nel caso sia necessario installare ulteriori software, utilizzare solo quelli messi a disposizione dalla Federazione, previa autorizzazione del Segretario Generale, assicurandosi dell'affidabilità della provenienza;

g) salvare dati e documenti di lavoro solo ed esclusivamente sulle aree di memoria autorizzate dalla Federazione ed ivi creare e registrare file o archivi dati;

h) conservare nel disco fisso della postazione di lavoro solamente i dati e i documenti strettamente necessari per l'attività lavorativa, per un tempo non eccedente il loro possibile utilizzo, conservando ove necessario anche copie di documenti condivisi;

i) per tutti i casi riguardanti la riproduzione di documenti contenenti informazioni di particolare rilevanza in termini di riservatezza federale e privacy, in cui venga utilizzata una stampante condivisa da vari Utenti situata al di fuori dei locali ove è posta la singola postazione di lavoro, vanno utilizzate, ove disponibili, le modalità di stampa protetta con codice impostabile dall'Utente; le stampe, inoltre, devono essere immediatamente raccolte e custodite dall'Utente;

j) qualora fosse necessario, inoltrare le richieste di assistenza per la propria postazione di lavoro alla struttura federale preposta;

k) nel caso di interventi di manutenzione e/o assistenza presso la propria postazione di lavoro, garantire la propria presenza o, in assenza, quella di un collega designato dall'Utente o di altro dipendente individuato dal Segretario Generale.

È, inoltre necessario il rispetto di ulteriori regole di carattere più operativo, riguardanti l'utilizzo delle password:

i. Ogni password deve essere composta da una sequenza di otto o più caratteri (normali e speciali) sia numerici che alfabetici o, se il programma in uso non lo consente, dal numero massimo di caratteri comunque consentito;

ii. Nella generazione delle password, è necessario prestare massima attenzione a non utilizzare elementi semplici o notizie facilmente riconducibili all'Utente (sono quindi da evitarsi, ad esempio, riferimenti a nome e cognome, data di nascita, numero di matricola, nomi di familiari, numeri di telefono di casa o dell'ufficio, soprannomi noti, nomi di personaggi famosi, e via dicendo);

iii. La password deve essere modificata al primo utilizzo e ogni volta che viene richiesto dal sistema, così come nel caso in cui vi sia il dubbio che ne sia stata violata la segretezza. Nella generazione della nuova password non devono essere utilizzate sequenze di caratteri già impiegate di recente;

iv. In caso di prima installazione del PC assegnato, e ove tale operazione non sia già stata predisposta, è necessario modificare immediatamente la password associata all'utente locale "Administrator" per evitare accessi non controllati mediante tale utenza;

v. Per ogni necessità federale il settore IT, utilizzando il proprio *login* con privilegi di Amministratore e la *password* di Amministratore, potrà accedere sia alla memoria di massa locale che al server federale nonché, previa comunicazione all'Utente, al dispositivo in remoto.

#### 4.5.2 Postazione di lavoro portatile e dispositivi mobili

Alla eventuale postazione di lavoro portatile assegnata si applicano le medesime regole di utilizzo previste per le postazioni fisse di cui al precedente punto 2.2.1., nonché i divieti di seguito riportati al punto 2.2.3.

Le postazioni di lavoro portatili, utilizzate per motivi di lavoro al di fuori della Federazione, sono maggiormente esposte a rischi di sicurezza, quali danneggiamenti conseguenti agli spostamenti, furti, violazione della riservatezza delle informazioni contenute, attacchi informatici e *malware*.

Ciascun Utente, pertanto, deve custodire la postazione di lavoro portatile con cura e diligenza, sia durante la permanenza nel luogo di lavoro sia negli spostamenti all'esterno dello stesso.

Con riferimento ad altri dispositivi mobili assegnati dalla Federazione o privati di proprietà dell'Utente, quali cellulari, smartphone, tablet e SIM card, utilizzati per motivi di lavoro e per l'invio di posta elettronica federale, valgono le medesime regole comportamentali sopra citate (e, ove applicabili, i divieti che seguono), nonché l'ulteriore disposizione di proteggere tali dispositivi e l'eventuale *smart card* SIM associata attraverso l'utilizzo di codici di sicurezza (PIN, PUK).

### 4.6 Comportamenti vietati

All'Utente non è consentito:

a) comunicare le password personali, per alcun motivo, a terzi o altri Utenti;

b) modificare le configurazioni della postazione di lavoro in dotazione quali, a titolo esemplificativo, le impostazioni di connessione di rete;

c) installare e utilizzare qualsiasi programma o strumento o supporto estraneo a quelli messi a disposizione o autorizzati dalla FASI senza preventiva e formale autorizzazione del Segretario Generale;

d) registrare qualsiasi file o software o archivio dati, nel disco fisso o memoria di massa dei Dispositivi assegnati all'Utente, che non abbia relazione con l'attività federale. È consentito utilizzare solo ed esclusivamente le aree di memoria indicate nell'allegato "Aree di memoria autorizzate per salvataggio di file ed applicazioni federali";

e) utilizzare programmi e/o sistemi di criptazione senza la preventiva autorizzazione scritta del diretto superiore gerarchico e del settore IT;

f) installare alcun software di cui la FASI non possieda la licenza, né installare alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sui Dispositivi, senza l'espressa autorizzazione del settore IT;

g) effettuare copie del software installato per uso personale;

h) caricare documenti, giochi, file audio e/o video diversi da quelli necessari allo svolgimento delle proprie mansioni;

i) aggiungere o collegare dispositivi hardware o periferiche (a titolo esemplificativo ma non esaustivo: telecamere, macchine fotografiche, chiavi USB, lettori MP3, smartphone personali, *access point*, ecc.) diversi da quelli consegnati, senza l'autorizzazione espressa del settore IT;

j) creare o diffondere programmi idonei a danneggiare il sistema informatico della FASI, quali ad esempio virus o *malware*;

k) reperire, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte.

Dal momento che la violazione delle regole di cui sopra potrebbe esporre la FASI al rischio di danneggiamento del sistema informatico o, eventualmente, a responsabilità penale in caso di uso di programmi senza licenza, la FASI si riserva il diritto di controllare, attraverso verifiche periodiche, il contenuto della memoria di massa dei Dispositivi di lavoro assegnati agli Utenti.

### 4.7 Modalità d'utilizzo dei servizi Internet

Gli accessi alla rete, ai servizi e alle risorse informatiche federali sono gestiti mediante sistemi di autenticazione/autorizzazione.

Al riguardo, sono applicate dalla FASI le seguenti regole:

- ciascun Utente deve essere attestato sui suddetti sistemi federali;
- ad ogni Utente è attribuito un profilo di autorizzazione, in relazione al ruolo svolto, che abilita all'utilizzo dei servizi necessari all'attività lavorativa;
- l'accesso ai servizi di rete avviene fornendo le proprie credenziali di autenticazione (codice utente e password);
- l'accesso di collaboratori esterni tramite PC o altri dispositivi mobili non federali deve avvenire in conformità alle procedure della FASI e deve essere preventivamente autorizzato dal Segretario Generale, che deve richiedere la creazione dell'utenza di dominio necessaria al settore IT.

#### 4.7.1 Navigazione Internet

La rete Internet è una risorsa messa a disposizione degli Utenti quale fonte di informazione per finalità di documentazione, ricerca e studio eventualmente utili allo svolgimento delle proprie mansioni lavorative.

La connessione a Internet e tutti gli accessi alla rete operati dai Dispositivi federali vengono registrati dai rispettivi *Internet Service Provider* per motivi di sicurezza. La connessione a Internet dai Dispositivi nella rete LAN e Wi-Fi della Segreteria Generale è ammessa esclusivamente per motivi attinenti all'attività lavorativa e, pertanto, ne è vietato l'utilizzo per scopi personali.

Al fine di prevenire l'accesso a siti web e risorse Internet non autorizzati, la FASI può adottare soluzioni di sicurezza basate su filtri della navigazione Internet, attraverso i quali l'accesso a specifiche e determinate

categorie di siti è bloccato *a priori*.

Al fine di prevenire download di file o pagine web contenenti codici malevoli, la Federazione può adottare soluzioni di sicurezza basate su tecnologie *anti-malware* che effettuano l'analisi della navigazione Internet e bloccano il download del contenuto in caso di rilevazione di codice malevolo, dandone comunicazione all'Utente.

4.7.2 Comportamenti vietati

All'Utente non è consentito:

a) scaricare contenuti (download) per ragioni che esulano dall'attività lavorativa;

b) effettuare il download di contenuti provenienti da siti web non verificati e/o non affidabili;

c) effettuare il download di software gratuiti (*freeware*) o messi a disposizione in rete per essere provati (*shareware*, demo), e comunque il download di qualsiasi software senza l'espressa autorizzazione dell'IT;

d) accedere a siti Internet dal contenuto non attinente allo svolgimento dell'attività lavorativa, in particolare laddove la navigazione sia idonea a rivelare dati particolari (o sensibili) ex art. 9 del GDPR;

e) accedere a siti Internet evitando l'azione o comunque superando, tentando di superare o disabilitando i sistemi adottati dalla FASI per bloccare l'accesso ad alcuni siti ed in ogni caso utilizzare siti o altri strumenti (es. *cracking programs*) che realizzino tale fine;

f) accedere a siti Internet che abbiano contenuto rilevante ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap;

g) utilizzare qualsivoglia gruppo di discussione o conferenza in rete (*chat line*, forum o altro), social network o altri strumenti di comunicazione e trasferimento di dati per scopi che esulano dall'attività lavorativa o per scambiare informazioni riservate o lesive dell'immagine della Federazione, degli individui che la compongono o di coloro che interagiscono con la stessa;

h) accedere o banche dati esterne per finalità non pertinenti all'attività lavorativa, con la sola esclusione di quelle per cui si è espressamente autorizzati;

i) registrarsi e/o accedere mediante credenziali federali (es. indirizzo di posta elettronica della Federazione) a siti Internet non attinenti allo svolgimento delle mansioni assegnate;

j) utilizzare i servizi Internet per promuovere utile o guadagno personale;

k) utilizzare i servizi Internet in violazione della normativa vigente in materia di Diritto d'autore (Legge 22 aprile 1941, n. 633 e ss.mm.ii.);

l) creare siti web personali sui sistemi della FASI.

Dal momento che la violazione delle summenzionate regole potrebbe esporre la FASI al rischio di danneggiamento o malfunzionamento del sistema informatico, il rispetto di tali regole potrà essere oggetto di controllo anche mediante accesso in remoto, attraverso periodiche verifiche del contenuto della memoria di massa del *server* e dei Dispositivi.

### 4.8 Modalità d'utilizzo della posta elettronica

A ciascun Utente che ne abbia necessità ai fini dello svolgimento della propria attività lavorativa, sono attribuiti uno o più indirizzi di posta elettronica federale di settore ed eventualmente uno individuale, configurato come segue: nome.cognome@federclimb.it.

L'indirizzo di posta elettronica federale di settore è abbinato ad un unico utente, il quale non può in alcun modo consentire ad altri soggetti (interni ed esterni alla Federazione) di accedere al medesimo indirizzo di posta elettronica

Gli Utenti abilitati all'uso della posta elettronica dovranno attenersi alle direttive impartite dal Segretario Generale.

I messaggi inviati o ricevuti dall'Utente sono raccolti sui server dei Provider del servizio di posta elettronica federale, in cui rimangono conservati in base allo spazio di memoria disponibile per la casella assegnata a ciascun Utente, secondo le prassi federali. I messaggi potranno essere consultati mediante client di posta elettronica configurati in modalità IMAP, e conservati nei sistemi di archiviazione federale, o nella memoria della postazione di lavoro assegnata (ad esempio con configurazione del client di posta in modalità POP3) previa autorizzazione del responsabile IT, o del Segretario Generale.

### 4.8.1 Utilizzo e gestione della posta elettronica ordinaria e certificata

Utilizzando gli indirizzi e le caselle di posta elettronica ordinaria e certificata (di seguito "*posta elettronica federale*"), l'Utente è a conoscenza e consapevole che:

1. tutti i messaggi in entrata e in uscita dagli indirizzi di posta elettronica federale sono di proprietà della FASI;

2. l'uso degli indirizzi di posta elettronica aziendale è ammesso esclusivamente per motivi attinenti all'attività lavorativa; l'uso per motivi personali è pertanto espressamente vietato. Resta ferma la possibilità per la Federazione di effettuare controlli atti a verificare il rispetto delle regole di utilizzo della posta elettronica da parte degli Utenti, sempre nel rispetto della normativa in materia di protezione dei dati personali e dello Statuto dei Lavoratori.

3. le informazioni inviate attraverso la posta elettronica non possono essere fermate o richiamate, una volta che siano state spedite all'esterno della FASI;

4. le comunicazioni di posta elettronica sono considerate a tutti gli effetti posta in partenza e pertanto in caso di assenza programmata dal lavoro (ad es. ferie, attività di lavoro fuori ufficio, etc.), l'Utente ha la possibilità di attivare il servizio di risposta automatica (*Out of office*), seguendo le istruzioni ricevute dall'IT, utilizzando il messaggio concordato con il proprio superiore gerarchico. Per effettive ragioni di continuità dell'attività lavorativa, in caso di prolungata assenza dal lavoro, sia essa programmata o non prevista, l'Utente che non abbia conferito l'accesso al proprio account di posta elettronica ad apposito delegato deve comunicare, a richiesta del Responsabile IT e/o del Personale o di loro incaricati, la propria password di accesso all'account di posta elettronica (o la password di rete se l'account di posta non prevede una specifica password). Successivamente al suo ritorno dall'assenza, l'Utente deve modificare la password. Qualora l'Utente assente sia irraggiungibile, o comunque in caso di effettiva urgenza, nei limiti di quanto necessario al fine di assicurare la continuità dell'attività della Federazione e/o per effettuare interventi per garantire la sicurezza del sistema informatico, il Responsabile IT, su autorizzazione del Segretario Generale, potrà altresì accedere alla posta elettronica dell'Utente forzando il cambiamento della password con le credenziali di amministratore, e successivamente darne informazioni all'Utente, che provvederà al ripristino sulla casella con una nuova password;

5. in caso di assenza non programmata dal lavoro (ad es. malattia etc.), l'Utente ha la facoltà di attivare o far attivare il servizio di risposta automatica (*Out of office*), o eseguendo le istruzioni ricevute dall' IT, conferire l'accesso al proprio account di posta elettronica ad apposito delegato.

4.8.2 Comportamenti vietati

In ogni caso di uso della posta elettronica contenente il dominio federale (@federclimb.it), sia con l'esterno che all'interno della FASI, all'Utente non è consentito:

a) inviare o ricevere messaggi a carattere personale;

b) iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta del Segretario Generale, nonché per partecipare a qualunque genere di richieste, petizioni, *mailing* di massa di ogni contenuto o, in generale, a qualunque pubblico dibattito su qualsivoglia tema;

c) promuovere utile o guadagno personale;

d) redigere messaggi diretti a destinatari esterni alla FASI senza l'indicazione del nome, cognome, carica e ufficio sotto la ragione sociale della FASI (per i procuratori) ovvero senza la sola indicazione di nome, cognome e ufficio (per gli altri);

e) trasmettere, a soggetti esterni alla FASI, informazioni riservate o comunque documenti federali, tranne nel caso in cui ciò sia necessario in ragione delle mansioni svolte;

f) trasmettere messaggi a gruppi numerosi di dipendenti (es. a tutto un ufficio o ad un'intera divisione) senza previa autorizzazione;

g) accedere a caselle di posta elettronica personali attraverso la rete e i Dispositivi della FASI; l'Utente non potrà, peraltro, inoltrare automaticamente i messaggi ricevuti all'indirizzo di posta elettronica federale su indirizzi personali;

h) creare, archiviare o spedire, anche all'interno della rete federale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) in nessun modo connessi con lo svolgimento della propria attività lavorativa;

i) sollecitare donazioni di beneficenza o altre voci non legate al lavoro;

j) inviare messaggi, anche all'interno della rete aziendale, a contenuto violento, sessuale o comunque offensivo dei principi di dignità personale;

k) inviare messaggi, anche all'interno della rete della Federazione, che abbiano contenuti contrari a norme di legge, che siano rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap; qualora l'Utente riceva messaggi aventi tali contenuti, è tenuto a cancellarli immediatamente e a darne comunicazione tempestiva al responsabile dell'IT/Segretario Generale;

l) spedire una e-mail con allegato un file eseguibile (*.exe*) senza la previa autorizzazione scritta del Segretario Generale;

m) violare le norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore;

n) inviare a indirizzi di posta elettronica privata e-mail con allegati documenti federali o, anche senza allegati, e-mail di contenuto attinente all'attività lavorativa;

o) aprire messaggi e, soprattutto, eventuali allegati sospetti e/o inviati da mittenti sconosciuti senza aver preventivamente accertato l'identità del mittente e verificato il contenuto del messaggio a mezzo di software antivirus;

4.8.3 Gestione account di posta elettronica successivamente alla cessazione del rapporto di lavoro

Successivamente alla cessazione del rapporto di lavoro, la casella di posta elettronica individuale è disattivata. È, inoltre, predisposto temporaneamente un sistema di risposta automatica per informare il

mittente dell'avvenuta disattivazione dell'account di posta elettronica e dare indicazione del nuovo referente federale.

Il contenuto degli account di posta elettronica disattivati è registrato in un *file* di *backup*. Successivamente alla cessazione del rapporto di lavoro, la FASI può liberamente accedere al contenuto del *file* di *backup*, del dispositivo nonché alla casella di posta elettronica assegnata all'Utente durante il rapporto di lavoro per ragioni di continuità dell'attività della FASI, per finalità di sicurezza del sistema informatico, nonché quando ciò sia necessario nei casi descritti nei paragrafi precedenti.

Le regole stabilite nei precedenti paragrafi sono applicabili, in relazione alle sole applicazioni federali, anche per l'utilizzo della posta elettronica.

### 4.9 Modalità di uso di dispositivi e altri supporti

Dispositivi e altri supporti possono essere concessi in uso dalla FASI agli Utenti che durante gli spostamenti sul territorio necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla casella di posta elettronica federale, o, ove possibile, alla rete LAN della Federazione.

Per lo svolgimento di qualunque mansione lavorativa federale, possono essere utilizzati esclusivamente i dispositivi e i supporti che siano stati messi a disposizione dalla Federazione, previa richiesta da presentarsi al superiore gerarchico e conseguente autorizzazione.

I dispositivi e i supporti ritenuti affidabili devono essere collegati esclusivamente ad attrezzature informatiche federali dotate di protezioni *anti-malware o antivirus* attive e aggiornate, al fine di impedire la diffusione di virus o altro *malware* all'interno del sistema informativo.

I dispositivi e i supporti dovranno essere verificati mediante soluzioni *anti-malware o antivirus* federali prima del loro impiego e, nel caso in cui si rinvenga un *malware* non eliminabile, non potranno essere utilizzati. Circa l'uso dei dispositivi e degli altri supporti, l'Utente è inoltre informato che:

a) la sottrazione dei dispositivi e dei supporti può provocare una perdita di informazioni importanti per la FASI e, in ogni caso, del valore intrinseco dei beni, causando un danno economico alla Federazione. Si richiede, quindi, di utilizzare particolare diligenza nella custodia di tali strumenti;

b) in caso di furto o smarrimento di dispositivi e supporti, l'Utente deve denunciare l'accaduto alle competenti autorità di Pubblica Sicurezza e comunicare immediatamente lo *user ID* all'IT, in modo da impedirne tempestivamente l'altrui utilizzo. Copia della denuncia deve essere consegnata, entro tre giorni dall'evento, al Segretario Generale della FASI;

c) a discrezione della FASI, in caso di smarrimento fuori dei locali federali, l'Utente potrà essere ritenuto responsabile del risarcimento del danno pari al valore di mercato del bene al momento dell'accaduto. In caso di danneggiamento, a discrezione della FASI, potranno essere addebitate le spese di riparazione;

d) in caso di cessazione del rapporto lavorativo e in tutti gli altri casi in cui ciò sia richiesto dalla FASI (quali ad esempio il venir meno delle ragioni di servizio che avevano determinato l'assegnazione o la sostituzione dello strumento), i dispositivi e i supporti devono essere restituiti all'IT nella loro interezza, comprese eventuali periferiche interne ed esterne.

L'assegnazione di dispositivi e supporti può, comunque, essere revocata dalla FASI.

#### 4.9.1 Modalità di uso dei telefoni cellulari di proprietà della Federazione

Qualora la FASI abbia deciso di dare in dotazione agli Utenti, in via fiduciaria, telefoni cellulari di sua proprietà, confida nel fatto che essi ne facciano un uso corretto, secondo quanto precisato di seguito:

a) È fatto divieto di utilizzare i telefoni cellulari federali per fini diversi da quelli legati allo svolgimento della prestazione lavorativa e degli altri espressamente consentiti, in contrasto con disposizioni di legge o

regolamenti e comunque in contrasto con gli usi e la buona fede;

b) Le comunicazioni telefoniche eseguite o ricevute per motivi professionali devono intendersi effettuate esclusivamente nell'interesse della FASI;

c) Il telefono cellulare può essere rubato o smarrito: a tal fine occorre proteggerlo dai furti mediante l'inserimento del PIN e/o altre misure di sicurezza;

d) l'Utente è tenuto ad un uso corretto del telefono cellulare che non dovrà essere utilizzato per scaricare dati di alcun genere (loghi, suonerie, servizi informativi) se non su specifica autorizzazione.

#### 4.9.2 Modalità di uso dei supporti di memorizzazione removibili

Dietro apposita autorizzazione, l'Utente può utilizzare supporti di memorizzazione removibili personali (es. *hard disk* esterni, CD-ROM, DVD, chiavette USB o altri supporti magnetici, elettronici o ottici), a condizione che ne abbia preventivamente verificato affidabilità e provenienza (ad esempio, non possono essere utilizzate chiavette USB rinvenute accidentalmente).

L'utilizzo di supporti di memorizzazione removibili è limitato al solo uso lavorativo per finalità di trasferimento e di *backup* di dati e documenti informatici, in ottemperanza alla vigente normativa sulla tutela dei dati personali, del software e del diritto d'autore.

L'Utente deve assicurarne la cancellazione sicura al termine dell'esigenza e, in caso di trattamento di dati personali o federali, curare la riservatezza del contenuto mediante l'adozione di idonee misure crittografiche federali.

Nel caso di dismissione di supporti contenenti dati personali o dati federali, agli Utenti è fatto obbligo di distruggere i supporti di tipo removibile nel caso in cui non sia possibile rendere irrecuperabili i dati in essi contenuti.

## 5. GESTIONE DELL'ESERCIZIO DEI DIRITTI DEGLI INTERESSATI

Gli Interessati possono esercitare in qualsiasi momento i loro diritti privacy nei confronti della Federazione, anche utilizzato il modulo presente nel sito istituzionale del Garante per la protezione dei dati personali, attraverso:

- Raccomandata al Titolare del trattamento presso "Federazione Italiana Arrampicata Sportiva" in via Piranesi, n. 46 - Milano;
- Mail al DPO all'indirizzo "dpo@federclimb.it";
- Mail a Referente privacy all'indirizzo "segretariogenerale@federclimb.it" (esclusivamente per Interessati in qualità di dipendenti a vario livello della Federazione).

Il Titolare del trattamento e il DPO trasmettono l'istanza a loro pervenuta al Referente privacy che coinvolge i Responsabili delle strutture federali competenti per gli approfondimenti necessari a valutare l'esito della richiesta.

Il Referente privacy sulla base delle informazioni raccolte e sentito il DPO determina l'esito della richiesta e predispone e invia il riscontro all'interessato.

La risposta deve essere trasmessa senza ingiustificato ritardo entro il termine di un mese dalla data di ricezione della richiesta; tale limite temporale può essere prorogato di due mesi, ove necessario, tenuto conto della complessità e del numero delle richieste ricevute.

Il Referente privacy aggiorna il Registro delle Istanze curando l'archiviazione di tutta la documentazione cartacea ed elettronica relativa all'istanza.

### 5.1 Diritto di accesso

Articolo 15 del GDPR

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;

b) le categorie di dati personali in questione;

c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

f) il diritto di proporre reclamo a un'autorità di controllo;

g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

4. Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.

In caso di esercizio di tale diritto, il Referente privacy verifica la presenza dei dati personali dell'Interessato richiedente nei propri archivi e sistemi fornendo tempestivo riscontro al Referente privacy sulle informazioni oggetto di richiesta.

Sulla base delle informazioni acquisite, il Referente privacy predispone la relativa risposta, riportando i punti del paragrafo 1 del sopra indicato articolo di riferimento.

### 5.2 Diritto di rettifica

Articolo 16 del GDPR

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

In caso di esercizio di tale diritto, il Referente privacy verifica la presenza dei dati personali dell'Interessato richiedente nei propri archivi e sistemi e dà seguito alle indicazioni del Referente privacy in merito alla rettifica e/o integrazione dei dati personali secondo la richiesta, fornendo tempestivo riscontro allo stesso Referente privacy e al DPO.

Il Referente Privacy comunica le rettifiche e/o integrazioni apportate a tutti i soggetti a cui i dati personali sono stati precedentemente trasmessi, salvo che risulti impossibile o che implichi uno sforzo sproporzionato.

***

Indipendentemente dal ricevimento di un'espressa richiesta da parte dell'Interessato, il referente privacy rettifica od integra i dati personali laddove nel corso del trattamento dovesse verificarne la non accuratezza o correttezza. In tal caso, resta fermo l'obbligo di comunicare le rettifiche e/o integrazioni a tutti i soggetti a cui i dati personali oggetto di modifica sono stati trasmessi.

### 5.3 Diritto alla cancellazione

Articolo 17 del GDPR

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

a. i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b. l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;

c. l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;

d. i dati personali sono stati trattati illecitamente;

e. i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

f. i dati personali sono stati raccolti relativamente all'offerta di servizi della Federazione dell'informazione di cui all'articolo 8, paragrafo 1.

2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:

a. per l'esercizio del diritto alla libertà di espressione e di informazione;

b. per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

c. per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;

d. a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;

e. o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Il Referente privacy, con il supporto del DPO, determina un termine per la conservazione dei dati personali sulla base del tempo necessario a realizzare la finalità perseguita, riportandolo nelle schede di trattamento di propria competenza.

Al termine del periodo individuato, il Referente privacy effettua la cancellazione dei dati personali tenendo traccia dell'attività. In caso di esercizio di tale diritto, il referente privacy verifica la presenza dei dati personali dell'Interessato richiedente nei propri archivi e sistemi.

Il Referente privacy verifica la sussistenza di una delle condizioni di cancellazione dei dati previste dal sopra indicato articolo di riferimento. In caso di esito positivo, il Referente privacy cancella i dati personali nei propri sistemi, applicativi, database e archivi e ne dà riscontro. Il Referente Privacy comunica le cancellazioni apportate a tutti i soggetti a cui i dati personali sono stati precedentemente trasmessi, salvo che risulti impossibile o che implichi uno sforzo sproporzionato.

***

La cancellazione dei dati personali deve essere definitiva ed avere riguardo ad ogni copia o riproduzione; pertanto, è compito dei Responsabili del trattamento eventualmente coinvolti, comunicare al DPO e al referente privacy la cancellazione definitiva all'interno dei sistemi informativi federali di propria competenza.

### 5.4 Diritto di limitazione del trattamento

Articolo 18 del GDPR

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

a. l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;

b. il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

c. benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

d. l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

2. Se il trattamento è limitato a norma del paragrafo 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

3. L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal titolare del trattamento prima che detta limitazione sia revocata.

In caso di esercizio di tale diritto, il referente privacy verifica la presenza dei dati personali dell'Interessato richiedente nei propri archivi e sistemi.

Il Referente privacy verifica la sussistenza delle condizioni di limitazione di trattamento previste dal sopra indicato articolo di riferimento.

Il Referente privacy, con il supporto dei Responsabili del trattamento interessati, effettua le operazioni di limitazione necessarie al fine di ottemperare alla richiesta e ne dà riscontro al Referente Privacy e al DPO.

Il Referente Privacy comunica la limitazione di trattamento apportata a tutti i soggetti a cui i dati personali sono stati precedentemente trasmessi, salvo che risulti impossibile o che implichi uno sforzo sproporzionato.

### 5.5 Diritto alla portabilità dei dati

Articolo 20 del GDPR

1. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e

b) il trattamento sia effettuato con mezzi automatizzato.

2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

In caso di esercizio di tale diritto, il Referente privacy verifica la presenza dei dati personali dell'Interessato richiedente nei propri archivi e sistemi.

Il Referente Privacy verifica la sussistenza delle condizioni per l'esercizio del diritto alla portabilità dei dati previste dal sopra indicato articolo di riferimento, se tecnicamente fattibile.

Il Referente privacy e con il supporto dei Responsabili del trattamento interessati, fornisce i dati personali all'interessato o al titolare indicato dallo stesso in un formato strutturato e leggibile e cancella degli stessi dai propri archivi e sistemi se richiesto.

### 5.6 Diritto di opposizione

Articolo 21 del GDPR

1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

2. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.

3. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.

4. Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.

5. Nel contesto dell'utilizzo di servizi della Federazione dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.

6. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

In caso di esercizio di tale diritto, il Referente privacy verifica la presenza dei dati personali dell'Interessato richiedente nei propri archivi e sistemi.

Il Referente Privacy verifica la sussistenza delle condizioni per l'esercizio del diritto di opposizione previste dal sopra indicato articolo di riferimento.

Il Referente privacy e con il supporto dei Responsabili del trattamento interessati, segnala ai vari Responsabili delle strutture federali coinvolte che i dati personali dell'Interessato non possono più essere oggetto di determinati trattamenti.

## 6. GESTIONE E NOTIFICA DEL DATA BREACH

Il data breach può riguardare una o più combinate violazioni:

- "*la violazione di riservatezza dei dati personali*", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
- "*la violazione d'integrità dei dati personali*", in caso di modifica non autorizzata o accidentale dei dati personali;
- "*la violazione della disponibilità dei dati personali*", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

### 6.1 Segnalazione del data breach

La rilevazione di un potenziale evento data breach può derivare da:

1) la segnalazione di un dipendente, un cliente, un fornitore, un collaboratore, un consulente;
2) la segnalazione da parte del Responsabile del trattamento;
3) la comunicazione da parte delle Forze di Polizia o da altre Autorità;
4) l'*alert* automatico dei sistemi informatici.

In caso di un potenziale data breach, il personale, i collaboratori e i fornitori che ne sono venuti a conoscenza, devono riferire senza alcun indugio o ritardo al Referente Privacy e al DPO attraverso l'indirizzo mail: dpo@federclimb.it.

- coinvolgimento in prima persona;
- osservazione diretta;
- possesso o presa visione di evidenze documentali;
- divulgazione di notizie da parte dei media;
- altro.

A titolo esemplificativo, di seguito alcuni esempi di evento che possono implicare un data breach, qualora siano coinvolti dati personali:

1. Perdita o furto di dispositivi federali;
2. Perdita o furto di supporti mobili quali *pen-drive* USB o hard disk della Federazione;
3. Perdita o furto di fascicoli cartacei o altra documentazione federale;
4. Phishing (*es. installazione di software non autorizzata, ricezione di una mail con mittente avente dominio sconosciuto, apertura di allegati a mail che nascondono ransomware o malware*);
5. Invio erroneo di comunicazioni/informazioni verso l'esterno (*es. errato inserimento del destinatario in una comunicazione federale ovvero errato invio ad un destinatario differente rispetto a quello inserito nella predisposizione della mail*);
6. Alterazione non autorizzata o impropria dei dati personali (*es. mancata protezione dei personal computer aziendale);*
7. Impossibilità di trattare i dati personali per cause accidentali o per interruzione dei sistemi della Federazione (*es. distruzione accidentale di un documento ovvero interruzione dei sistemi federali per calamità naturali, virus o attacco cyber*);

8. Situazioni anomale segnalate o riscontrate nei sistemi informatici della Federazione (*es. rilevazione da parte dei sistemi informatici federali di infezione da virus, malware, ransomware*);

9. Divulgazione non autorizzata dei dati personali (*es. comunicazione o diffusione non sicura o illecita, anche attraverso i media, di dati personali, di cui la Federazione ne è Titolare o Responsabile, o comportamenti sleali o fraudolenti di dipendenti o altri Utenti*).

### 6.2 Gestione del data breach

In caso di segnalazione, Il Referente Privacy effettua tempestivamente una prima analisi per identificare con ragionevole certezza la presenza di un data breach e valutarne l'impatto sui diritti e alle libertà degli interessati con il supporto del DPO, avvalendosi ove necessario delle Funzioni interessate, e dei Responsabili del trattamento.

Tale impatto rileva in termini di danno alle persone fisiche:

- fisico (es. rischio di frode o usurpazione d'identità che comportano in caso di persona vulnerabile un danno fisico);
- materiale (es. perdite finanziarie);
- immateriale (es. pregiudizio alla reputazione).

Al fine di stimare **l'entità dell'impatto** si considerano complessivamente i seguenti aspetti:

- il tipo di violazione;
- la natura del dato personale violato;
- il volume dei dati personali violati in termini di tempo e contenuto;
- la facilità di identificazione delle persone fisiche interessate;
- la gravità delle conseguenze;
- le caratteristiche particolari degli interessati coinvolti;
- il numero delle persone fisiche coinvolte.

Il Referente Privacy, con il supporto del DPO e del fornitore esterno interessato, individua la strategia di gestione dell'evento, anche al fine di minimizzare l'eventuale danno.

Qualora l'evento fosse ancora in corso, è opportuno definire:

a) le modalità di contenimento attraverso misure tecniche ed organizzative di protezione (ad esempio, denuncia di smarrimento, blocco da remoto dei dispositivi, recupero dei dati tramite back up, isolamento delle utenze, reset delle password);

b) le modalità di monitoraggio della situazione (ad esempio, analisi e monitoraggio dei log, del traffico di rete e funzionamento del firewall);

c) eventuale piano delle comunicazioni interne ed esterne (ad esempio, predisposizione di una comunicazione interna dell'accaduto oppure di una comunicazione da rendere pubblica attraverso media, Forze dell'Ordine, sito istituzionale);

d) a seguito della ricostruzione dell'accaduto, le azioni correttive per contenere i danni, rispristinare l'accesso ai dati e assicurare la resilienza dei sistemi (ad esempio, denuncia di smarrimento, blocco da remoto dei dispositivi, recupero dei dati tramite back up, isolamento delle utenze, reset delle password).

Qualora l'evento fosse già avvenuto, è opportuno definire i punti c) e d) del punto elenco di cui sopra.

I Responsabili delle strutture federali sono tenuti all'implementazione delle misure correttive individuate e il Referente Privacy deve monitorare la completa e corretta attuazione delle misure.

Il Referente Privacy è tenuto altresì a formalizzare l'esito della valutazione del data breach con il supporto del DPO da sottoporre al Titolare del trattamento.

Tutti i soggetti coinvolti devono garantire la riservatezza delle informazioni comunicate o rilevate durante la gestione del data breach.

### 6.3 Notifica al Garante per la protezione dei dati personali

Nel caso in cui il data breach abbia effetti avversi significativi sui diritti e le libertà degli Interessati, si procede obbligatoriamente alla notifica nei confronti del Garante per la protezione dei dati personali ovvero anche alla comunicazione agli Interessati coinvolti dalla violazione.

La notifica viene inoltrata dal Titolare del trattamento, con il supporto del DPO e del Referente Privacy, tramite l'apposita procedura telematica disponibile nel sito istituzionale dell'Autorità Garante, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui la Federazione ne è venuta a conoscenza, ossia nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali. Oltre tale termine, la notifica deve essere corredata delle ragioni del ritardo.

Qualora non sia possibile fornire tutte le informazioni contestualmente alla notifica, queste ultime potranno essere fornite in fasi successive senza ulteriore ingiustificato ritardo, avendo cura di dare evidenza delle motivazioni per cui tali informazioni non siano disponibili all'interno della notifica.

Nel caso in cui sia il Garante per la protezione dei dati personali ad ordinare con provvedimento l'applicazione di ulteriori misure correttive rispetto alla violazione notificata, sarà cura del DPO supervisionare sulla completa e corretta implementazione delle suddette misure.

Il Referente Privacy invia la comunicazione della violazione agli Interessati sottoscritta dal Titolare del trattamento senza ingiustificato ritardo, qualora sia disposto dal Garante per la protezione dei dati personali o qualora il data breach presenti un rischio elevato per gli Interessati.

### 6.4 Modalità di archiviazione

Sulla base delle richieste pervenute, il Referente Privacy compila il Registro Interno delle Violazioni, monitorandolo annualmente. Per la tenuta del registro vengono adottate idonee misure atte a presidiare la sua integrità quali:

- salvataggio in una cartella con accesso limitato alle sole persone autorizzate;
- protezione delle celle per evitare che i dati siano modificati da persone non autorizzate.

Il Referente Privacy archivia tutta la documentazione cartacea ed elettronica relativa al data breach. Le cartelle elettroniche sono soggette a back up, mentre i faldoni cartacei sono archiviati in armadi chiusi a chiave presso la Federazione.

## 7. GESTIONE DEI RAPPORTI CON L'AUTORITÀ GARANTE

La gestione dei rapporti con il Garante è affidata al DPO. Si rimanda al capitolo precedente, per quanto attiene la consultazione preventiva in caso di Trattamenti a rischio elevato e la notifica in caso di Data Breach.

### 7.1 Riscontro alle richieste del Garante

Il Garante può richiedere informazioni relativamente a segnalazioni o ricorsi degli Interessati o, nell'ambito di indagini conoscitive, richiedere contributi informativi specifici; inoltre può, anche in occasione delle verifiche ispettive, raccogliere documentazione relativamente alle misure tecniche e organizzative implementate a protezione dei Dati Personali trattati, documentazione contrattuale, modelli e documenti privacy, estendendo l'analisi a qualsiasi altro processo, misura o Trattamento effettuato da parte della Federazione.

È compito del DPO dare formalmente riscontro alle richieste del Garante.

Gli Incaricati e gli Amministratori di sistema dovranno prestare la massima collaborazione al DPO e fornire tutte le informazioni e documenti attinenti alle operazioni di Trattamento di Dati Personali oggetto di chiarimento.

### 7.2 Ispezioni da parte del Garante

Il Garante può effettuare ispezioni presso la Federazione, finalizzate a verificare l'effettiva implementazione da parte di questa delle tutele previste dalla normativa.

Il DPO ha il compito di interfacciarsi con i soggetti esterni in caso di ispezioni e dovrà gestire e coordinare la cooperazione tra le Autorità di controllo e il Titolare.

Gli Incaricati dovranno prestare la massima collaborazione ai funzionari dell'autorità di vigilanza che effettuino le suddette ispezioni e fornire tutte le informazioni attinenti alle operazioni di Trattamento di Dati Personali svolte che siano richieste dagli stessi.

## 8. SANZIONI

La violazione della normativa in materia di protezione dei Dati Personali può esporre il Titolare e/o il Responsabile a diverse tipologie di responsabilità e conseguenti sanzioni (di carattere amministrativo e/o penale), in base alle norme concretamente violate, oltre che al risarcimento del danno verso l'Interessato che abbia subito un danno materiale o immateriale causato da una violazione della normativa, nonché ad impatti reputazionali negativi.

Il GDPR ha innalzato significativamente l'importo delle sanzioni amministrative, portandole fino a euro 20 milioni o al 4% del fatturato annuo dell'esercizio precedente se superiore. Nei singoli casi, l'Autorità Garante può decidere se applicare le sanzioni amministrative pecuniarie in aggiunta alle misure di carattere prescrittivo o interdittivo, o al posto di tali misure.

In ogni caso, le sanzioni amministrative pecuniarie devono essere in concreto effettive, proporzionate e dissuasive e pertanto, nella determinazione dell'ammontare della sanzione, il Garante tiene conto di una serie di fattori, tra i quali la natura, la gravità e la durata della violazione, eventuali precedenti violazioni pertinenti, le misure adottate dal Titolare o dal Responsabile per attenuare il danno subito dagli Interessati. Inoltre, chiunque al fine di trarre per sé o per altri profitto, violi la normativa privacy e arrechi nocumento all'Interessato, può incorrere in sanzioni penali, con la reclusione fino a tre anni.[1]

Fermo quanto sopra in relazione alla responsabilità degli Incaricati, l'inosservanza degli obblighi previsti dal presente documento costituisce comportamento rilevante ai fini disciplinari e può determinare l'applicazione delle sanzioni previste dalla contrattazione collettiva di lavoro applicabile e dalla normativa vigente.

L'accertamento di determinate violazioni può anche comportare l'emissione, da parte delle autorità competenti, di ordini finalizzati alla cancellazione dei Dati Personali raccolti o all'interruzione di determinate operazioni di Trattamento che si assumono illecite. Inoltre, gli Interessati possono promuovere azioni di risarcimento per i danni subiti a causa dello svolgimento di operazioni di illecito Trattamento, riguardanti i loro Dati Personali.

[1] Fino a sei anni in caso di comunicazione e diffusione illecita di Dati Personali riferibili a un rilevante numero di persone.