

Regolamento in materia di protezione dei Dati Personali

Sommario

MODALITA' DI GESTIONE DEL DOCUMENTO	2
1. INTRODUZIONE	6
2. CONTESTO NORMATIVO	6
3. PRINCIPI GENERALI	7
4. RUOLI E RESPONSABILITÀ NELLA GESTIONE DEI DATI PERSONALI	8
4.1. Titolare del trattamento	8
4.2. Responsabile / Sub-responsabile del trattamento	8
4.3. Amministratori di sistema	9
4.4. Incaricati del trattamento	9
4.5. I Comitati Regionali	10
4.6. Il Referente privacy	10
4.7. Il Comitato Privacy	11
4.8. Il DPO	11
5. PRIVACY BY DESIGN E PRIVACY BY DEFAULT	11
5.1. Portata del Trattamento	12
5.2. Accesso ai Dati Personali	12
6. MODALITÀ DI GESTIONE DEI DATI PERSONALI	12
6.1. Registro dei Trattamenti (art. 30 GDPR)	12
6.2. Raccolta, utilizzo e conservazione dei Dati Personali	12
6.3. Portabilità, restituzione e cancellazione dei Dati Personali	13
6.4. Misure di sicurezza	14
7. GESTIONE DEI RAPPORTI CON L'AUTORITÀ GARANTE	14
7.1. Riscontro alle richieste del Garante	14
7.2. Ispezioni da parte del Garante	14
8. SANZIONI	15

MODALITA' DI GESTIONE DEL DOCUMENTO

Società emittente	FEDERAZIONE ITALIANA PALLACANESTRO
Titolo	Regolamento in materia di protezione dei Dati Personali
Data decorrenza	DELIBERA PF N.78/A DEL 24/05/2021
Codice del documento	v. 1.0
Tipologia del documento	Policy di <i>compliance</i>

Glossario

Amministratore di sistema	La figura professionale destinata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, in riferimento a sistemi informatici e di elaborazione dati o di sue componenti sia <i>hardware</i> sia <i>software</i> , come definita dai Provvedimenti dell’Autorità Garante per la protezione dei Dati Personali del 27 novembre 2008, del 25 giugno 2009 e ss.mm.ii.
Autorità di controllo o Garante	L’Autorità di cui all’articolo 51 del GDPR (v. <i>infra</i>), ovvero una o più Autorità pubbliche indipendenti incaricate da uno Stato Membro di sorvegliare l’applicazione del Regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento dei Dati Personali. In Italia l’Autorità di controllo indipendente è il Garante per la protezione dei Dati Personali (cd. “Garante Privacy”).
Categorie particolari di dati (Dati sensibili)	I Dati Personali idonei a rivelare l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l’appartenenza sindacale, nonché i dati genetici, dati biometrici trattati per identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all’orientamento sessuale della persona (art. 9 GDPR).
Codice in materia di protezione dei Dati Personali (o “Codice Privacy”)	Il Decreto Legislativo 30 giugno 2003, n. 196, recante disposizioni per l’adeguamento dell’ordinamento nazionale alle disposizioni del Regolamento (UE) n. 2016/679 (<i>General Data Protection Regulation – GDPR</i>), così come emendato dal D.Lgs. 10 agosto 2018, n. 101 e ss.mm.ii.
Dato personale	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 (art. 4, GDPR).

General Data Protection Regulation (o “GDPR”)	Il Regolamento (UE) n. 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, che stabilisce la disciplina europea di regolamentazione in ambito di protezione delle persone fisiche con riguardo al trattamento dei Dati Personali, nonché alla libera circolazione degli stessi.
Incaricati (o “Soggetti designati”)	La persona fisica espressamente designata autorizzata, sotto la responsabilità e nell’ambito dell’assetto organizzativo del Titolare o del Responsabile del trattamento, a compiere specifici compiti e funzioni connessi al trattamento di Dati Personali (art. 29 GDPR, art. 2-quaterdecies Codice Privacy).
Interessato	La persona fisica identificata o identificabile, direttamente o indirettamente, da un dato personale e comunque cui il dato trattato si riferisce (art. 4, n. 1 GDPR).
Responsabile della protezione dei dati (<i>Data Protection Officer</i> , o “DPO”)	Il soggetto designato dal titolare o dal responsabile del trattamento per assolvere funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento (art. 37 GDPR). Il DPO è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati, e della capacità di adempiere ai propri compiti. Tale figura, di alto livello professionale, può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure adempiere ai suoi compiti in base a un contratto di servizi e quindi può essere un libero professionista.
Responsabile del trattamento o Responsabile	La persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che tratta Dati Personali per conto del titolare del trattamento (artt. 4, n. 8 e 28 GDPR).
Titolare del trattamento o Titolare	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 (art. 4, n. 7 GDPR).
Trattamento	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

	<p>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 (art. 4, n. 2 GDPR).</p>
--	--

1. INTRODUZIONE

Il presente regolamento (di seguito, “**Regolamento**”) definisce le regole generali adottate dalla Federazione Italiana Pallacanestro (di seguito, “**Federazione**”) per la disciplina degli adempimenti connessi al Trattamento dei Dati Personali.

In particolare, la Federazione è stata costituita nel 1921 allo scopo di promuovere, regolare e sviluppare lo sport della pallacanestro in Italia, nel rispetto dei principi costituzionali, della legislazione vigente, dei Regolamenti e disposizioni della Federation Internationale de Basketball (FIBA), cui è affiliata, degli indirizzi e delle direttive del CONI e del Comitato Internazionale Olimpico (CIO). La FIP è riconosciuta dal CONI e dalla FIBA, ed è l'unica rappresentante dello sport della pallacanestro, nelle sue forme agonistiche o amatoriali, svolte al coperto o sui campi all'aperto. La FIP è costituita, quindi, da Società ed Associazioni sportive di qualsiasi forma giuridica che praticano, promuovono od organizzano lo sport della pallacanestro agonistico o amatoriale.

L'attività sportiva si articola attraverso settori professionistici e dilettantistici o, comunque, non professionistici, sulla base dei criteri stabiliti dal Consiglio Federale, in armonia con le leggi dello Stato, con le norme e direttive del CONI e con gli ordinamenti sportivi internazionali purché questi ultimi non siano in contrasto con le deliberazioni e gli indirizzi del CIO e del CONI, garantendo un costante equilibrio di diritti e doveri tra i settori professionistici e non professionistici, nonché tra le diverse categorie nell'ambito del medesimo settore.

La FIP ha autonomia tecnica, organizzativa e di gestione e svolge la sua attività sotto la vigilanza del CONI, a norma della legislazione vigente.

Nell'ambito delle proprie attività, la Federazione svolge operazioni di Trattamento relative a Dati Personali di varia natura, riferiti, a titolo esemplificativo, ai propri dipendenti, collaboratori e tesserati.

In tale contesto, compito del Regolamento è fornire i principi guida volti ad assicurare che il Trattamento dei Dati Personali effettuato dalla Federazione sia conforme alla normativa vigente in materia *data protection*, al fine di tutelare il diritto riconosciuto alle persone fisiche alla protezione dei propri Dati Personali e mitigare i rischi (operativi, reputazionali e di *compliance*) derivanti da una non corretta gestione degli stessi.

Il Regolamento definisce pertanto il “modello organizzativo”, che mostra i ruoli e le responsabilità dei soggetti coinvolti per la gestione dei Dati Personali e la messa a punto delle relative misure di protezione.

2. CONTESTO NORMATIVO

Il Regolamento è redatto ai sensi della normativa in materia di Trattamento dei Dati Personali, sia a livello europeo che nazionale, contenuta nelle seguenti disposizioni e successive modifiche:

- Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 *relativo alla protezione delle persone fisiche con riguardo al trattamento dei Dati Personali, nonché alla libera circolazione di tali dati* (Regolamento Generale sulla Protezione dei Dati, in inglese *General Data Protection Regulation*, di seguito, “**GDPR**”);

- Linee Guida e altra documentazione del Comitato Europeo per la Protezione dei Dati (in inglese, *European Data Protection Board*);
- Decreto Legislativo 30 giugno 2003, n. 196 recante il “Codice in materia di protezione dei Dati Personali”, così come modificato dal D.Lgs. 10 agosto 2018, n. 101 di adeguamento al GDPR e ss.mm.ii. (di seguito, il “**Codice Privacy**”);
- Provvedimenti applicabili dell’Autorità Garante per la protezione dei dati personali, tra cui i Provvedimenti del 27 novembre 2008, del 25 giugno 2009 in materia di amministratori di sistema.

3. PRINCIPI GENERALI

I referenti federali coinvolti nelle attività di raccolta, conservazione ed utilizzo di Dati Personali operano nel rispetto del sistema normativo interno e del sistema di poteri e responsabilità, 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, equo e trasparente nei confronti dell’Interessato (“liceità, equità 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) laddove necessario, la Federazione, attraverso le figure chiave previste dal GDPR, collabora con l’Autorità di controllo, anche con riferimento specifico ad eventuali casi di notifica per violazioni ovvero in relazione alla valutazione preliminare per il Trattamento di taluni dati, 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, scritta e libera.

4. RUOLI E RESPONSABILITÀ NELLA GESTIONE DEI DATI PERSONALI

Le complessità connesse al Trattamento dei Dati Personali richiedono l'individuazione di diverse figure, con specifici compiti e responsabilità nell'ambito della gestione degli stessi.

Alcune di tali figure sono espressamente previste dal GDPR, tra cui, ad esempio, il Titolare del trattamento, il Responsabile/Sub-responsabile del trattamento e il DPO.

Altre figure, invece, sono attualmente previste dal Codice Privacy e dai provvedimenti dell'Autorità di controllo, quali gli Incaricati del trattamento e l'Amministratore di sistema.

4.1. Titolare del trattamento

Per Titolare del trattamento si intende la persona fisica o giuridica che, singolarmente o insieme ad altri, determina le finalità ed i mezzi del Trattamento dei Dati Personali.

Il Titolare è pertanto responsabile per la definizione delle finalità e delle modalità dei trattamenti effettuati, per l'adozione delle misure organizzative e tecniche adeguate a garantire il rispetto della normativa applicabile, avendo cura di riesaminare ed aggiornare tali misure quando necessario, e per la garanzia agli Interessati dell'esercizio dei diritti che il GDPR riconosce loro.

Ad esempio, la Federazione riveste tale ruolo nell'ambito del Trattamento dei Dati Personali relativi ai propri dipendenti, collaboratori e tesserati.

4.2. Responsabile / Sub-responsabile del trattamento

Il Responsabile del trattamento, così come individuato ai sensi dell'art. 28 GDPR, è una persona fisica o giuridica che effettua operazioni di Trattamento per conto del Titolare.

Nei casi in cui la Federazione debba avvalersi di soggetti che agiscono in qualità di Responsabile del trattamento (per esempio società ad associazioni sportive affiliate), i Trattamenti effettuati, gli obblighi e le responsabilità sono disciplinati in un atto giuridico che vincoli il Responsabile del trattamento e disciplini ogni aspetto rilevante del Trattamento (durata, natura e finalità, tipo di Dati Personali, categorie di Interessati, obblighi e diritti del Titolare).

In ottemperanza al disposto dell'art. 28 GDPR, il Titolare del trattamento ricorre unicamente a Responsabili che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, così garantendo la possibilità di mettere in atto misure di sicurezza adeguate alle esigenze di protezione espresse dal GDPR.

Ai sensi dell'art. 28, par. 4 GDPR, previa autorizzazione scritta (generale o specifica) del Titolare, il Responsabile può designare Sub-responsabili del trattamento soggetti terzi, persone fisiche o giuridiche, che effettuino Trattamenti di Dati Personali nell'ambito delle attività per cui essa è nominata Responsabile.

4.3. Amministratori di sistema

Gli Amministratori di sistema sono soggetti incaricati della gestione e della manutenzione dei sistemi di elaborazione dei Dati Personali.

Con tale termine si distinguono varie figure, quali gli amministratori di *database*, gli amministratori di rete e di apparati di sicurezza e gli amministratori di sistemi *software* complessi.

Il Garante ha richiamato l'attenzione di enti, amministrazioni, società private sulla figura professionale dell'Amministratore di sistema e ha prescritto l'adozione di specifiche misure tecniche ed organizzative che agevolino la verifica sulla sua attività da parte di chi ha la titolarità delle banche dati e dei sistemi informatici (Provvedimento del Garante recante *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema* del 27 novembre 2008, così come modificato dal Provvedimento del 25 giugno 2009).

Gli Amministratori di sistema nominati dalla Federazione sono pertanto responsabilizzati mediante l'accettazione degli incarichi elencati nell'atto di nomina, nonché attraverso le istruzioni impartite, più in generale, agli Incaricati.

Gli Amministratori di sistema, nelle loro consuete attività, effettuano concretamente specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

In tale contesto, attività tecniche quali il salvataggio dei Dati (c.d. funzioni di *backup* e *recovery*), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione *hardware* comportano, infatti, un'effettiva capacità di azione su informazioni e Dati che va considerata a tutti gli effetti come un Trattamento di Dati Personali.

Per tali ragioni, l'attribuzione delle funzioni di Amministratore di sistema deve avvenire, come previsto dai Provvedimenti citati, previa valutazione delle caratteristiche tecniche di esperienza e capacità e del soggetto designato.

Nei richiamati Provvedimenti, il Garante ha mirato a creare una condizione di consapevolezza in ordine alla rilevanza del ruolo di queste figure professionali, fornendo una serie di prescrizioni destinate alla totalità dei Titolari e dei Responsabili.

La Federazione è quindi tenuta ad assolvere tali adempimenti mediante l'attuazione di adeguate misure riguardanti l'operato degli Amministratori di sistema, tramite, per esempio, designazioni degli Amministratori di sistema con lettera di nomina individuale, che elenchi in via analitica gli ambiti di operatività consentiti e che sia coerente al profilo di autorizzazione assegnato.

4.4. Incaricati del trattamento

L'art. 29 del GDPR prevede che chiunque agisca sotto l'autorità del Titolare, che abbia accesso a Dati Personali, non può trattare tali Dati se non è istruito in tal senso dal Titolare.

Ai sensi del Codice Privacy, il Titolare può quindi prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al Trattamento di Dati Personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la sua autorità.

La Federazione, in qualità di Titolare del trattamento, designa quale Incaricato del trattamento ogni dipendente e/o collaboratore che effettua operazioni di Trattamento sui Dati Personali di cui la Federazione è Titolare.

La designazione viene effettuata mediante delle istruzioni fornite agli Incaricati, consegnate al momento dell'assunzione del collaboratore e, ove necessario, oggetto di aggiornamenti e integrazioni. Istruzioni *ad hoc* sono inoltre fornite a coloro che rivestono specifici incarichi federali.

Ogni Incaricato è tenuto ad osservare scrupolosamente le istruzioni e le misure di sicurezza fornite dalla Federazione, oltre a quanto previsto del presente Regolamento e dalla normativa interna di dettaglio.

Gli Incaricati del trattamento sono destinatari di interventi formativi in materia di protezione dei Dati Personali e misure di sicurezza, finalizzati ad acquisire familiarità con i profili della disciplina sulla protezione dei Dati Personali più rilevanti in rapporto alle relative attività, i compiti e le responsabilità che ne derivano e conoscere le misure disponibili per prevenire eventi dannosi.

4.5. I Comitati Regionali

La Federazione è strutturata in Comitati Regionali, cui sono delegati i compiti in materia di amministrazione federale locale e di organizzazione di eventi per la specifica area di riferimento.

Nell'ambito delle operazioni di trattamento di dati personali a livello locale, i membri del personale e i collaboratori interni dei Comitati Regionali agiscono in qualità di Incaricati del trattamento e sono a tal fine debitamente istruiti.

La Federazione è Titolare del trattamento effettuato dai Comitati attraverso Internet, e ne cura il rispetto in materia di protezione dei dati, predisponendo tutta la documentazione necessaria (a titolo esemplificativo, le informative privacy e cookie).

4.6. Il Referente privacy

La Federazione ritiene utile individuare, altresì, dei c.d. "Referenti Privacy" nelle persone dei Presidenti dei Comitati territoriali ossia di soggetti che supportino la gestione operativa delle tematiche privacy agendo quale punto di contatto per il Comitato Privacy.

Tra le principali attività affidate al Referente nell'ambito della Federazione, vi è:

- l'obbligo di rispettare i principi generali in materia di Trattamento dei Dati Personali delineati nel paragrafo 3 che precede;
- supportare il Comitato Privacy nell'esecuzione delle attività a lui affidate e allinearli sulle tematiche in materia privacy ed informarlo di eventuali Data Breach.

4.7. Il Comitato Privacy

La Federazione ritiene utile e positivo in termini di “*accountability*” stabilire un *Comitato Privacy* formato da risorse interne con differenti profili, opportunamente nominato dal Titolare del Trattamento che si occupi di:

- supportare la gestione operativa delle tematiche privacy agendo quale punto di contatto per il DPO, i Comitati Territoriali, i tesserati, i dipendenti, i collaboratori, i fornitori, i consulenti e per il Titolare;
- costituire un riferimento interno alla Federazione per le tematiche di Privacy;
- valutare e applicare i principi di *privacy-by-design* sui singoli Trattamenti;
- essere il primo punto di contatto per la segnalazione di eventuali data breach o per la gestione di eventuali richieste degli interessati.

4.8. Il DPO

Il Titolare ha individuato un DPO, altamente qualificato e specializzato in materia di *data protection*, che svolge i compiti di cui all’art. 39, GDPR, in particolare:

- informa e fornisce consulenza alla Federazione, agli Incaricati e agli Amministratori di sistema in merito agli obblighi derivanti dal GDPR nonché da altre disposizioni relative alla protezione dei dati;
- sorveglia l’osservanza del GDPR e delle altre disposizioni relative alla protezione dei dati;
- fornisce, se richiesto, un parere in merito alla valutazione d’impatto sulla protezione dei dati e ne sorveglia lo svolgimento;
- coopera, ove necessario, con il Garante;
- funge da punto di contatto per l’Autorità di controllo e con gli Interessati per questioni connesse al Trattamento, ed effettua, se del caso, consultazioni relativamente a qualunque altra questione;
- offre supporto per l’aggiornamento del registro dei trattamenti e verifica, ove richiesto, la correttezza e la coerenza dei profili privacy della documentazione predisposta dalla Federazione.

5. 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 il 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.

Al fine di ottemperare ai principi sopra esposti, la Federazione definisce di seguito le direttive che i soggetti coinvolti nelle attività di Trattamento (ossia, Incaricati e Amministratori di sistema) devono

seguire nello sviluppo di iniziative, prodotti e/o servizi che implicano qualsivoglia Trattamento dei Dati Personali di dipendenti, collaboratori, tesserati o altri soggetti terzi di cui la Federazione sia Titolare.

5.1. Portata del Trattamento

Gli Amministratori di sistema e gli Incaricati dovranno attenersi ai principi sanciti dal GDPR e, in particolare, al principio di minimizzazione dei dati, in forza del quale non dovranno essere richiesti all' Interessato o, più in generale, non dovranno essere trattati ovvero raccolti Dati Personali ultronei rispetto a quelli strettamente necessari al perseguimento delle finalità di Trattamento.

5.2. Accesso ai Dati Personali

Nell'espletamento delle attività poste in essere dalla Federazione, gli Incaricati dovranno 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 dovrà essere reso disponibile esclusivamente a quei soggetti che sono tenuti al Trattamento di quei Dati Personali per il raggiungimento delle finalità perseguite dalla Federazione.

6. MODALITÀ DI GESTIONE DEI DATI PERSONALI

6.1. Registro dei Trattamenti (art. 30 GDPR)

La Federazione istituisce e conserva un apposito Registro dei Trattamenti, che deve indicare, *inter alia*:

- nome e dati di contatto del Titolare;
- finalità del Trattamento;
- categorie di Interessati e di Dati trattati;
- categorie di terzi destinatari a cui i Dati possono essere eventualmente comunicati;
- eventuali trasferimenti di Dati verso paesi terzi ed indicazione delle adeguate garanzie;
- termini ultimi per la cancellazione (rispetto alle finalità del Trattamento);
- descrizione generale delle misure di sicurezza tecniche e organizzative;
- condizioni di liceità del Trattamento.

6.2. Raccolta, utilizzo e conservazione dei Dati Personali

I Dati Personali trattati dalla Federazione possono essere conservati in archivi informatici o cartacei, comunque strutturati in modo da poter reperire le informazioni riferibili all' Interessato, nel rispetto delle regole e dei principi previsti dalla normativa applicabile.

Gli archivi contenenti gli atti e i documenti nei quali sono raccolti Dati Personali vengono sottoposti a controllo e custodia per tutto il tempo necessario al loro Trattamento, anche in relazione alla natura dei Dati Personali e alle possibili finalità di Trattamento.

Alla scadenza dei periodi di conservazione, i Dati Personali sono cancellati automaticamente ovvero resi anonimi in modo permanente e non reversibile, dal momento in cui la conservazione non risulti ulteriormente giustificata.

Il GDPR non ha previsto criteri univoci per la determinazione dei tempi di conservazione dei Dati, limitandosi a specificare che questi devono essere trattati per il tempo strettamente necessario al perseguimento delle finalità per cui sono stati raccolti.

Alcuni termini di conservazione sono determinati direttamente dalla normativa nazionale o da un contratto, mentre altri sono determinati dal Titolare del trattamento in base ad autonome scelte organizzative.

6.3. Portabilità, restituzione e cancellazione dei Dati Personali

L'Interessato può richiedere la portabilità dei propri Dati Personali ovvero la cancellazione e/o restituzione degli stessi mediante l'invio di una richiesta all'indirizzo e-mail indicato nell'informativa al Trattamento dei Dati Personali consegnatagli, a cui dovrà essere allegata la copia del documento di identità dell'istante-Interessato oltre che, nel caso in cui l'istanza sia effettuata per suo conto da un terzo a ciò delegato, la copia della procura e del documento di identità di quest'ultimo.

Qualora l'Interessato contatti la Federazione direttamente per via telefonica, l'operatore deve invitarlo ad utilizzare i canali di comunicazione indicati nell'informativa e ad effettuare la richiesta con le modalità appena descritte.

Le valutazioni delle richieste sono effettuate dall'Incaricato preposto alla gestione delle istanze degli Interessati, che ha il compito di verificare che le richieste siano legittime, evadibili e non lesive dei diritti e delle libertà di altri Interessati.

Ricevuta una istanza di trasferimento/cancellazione/restituzione da parte di un Interessato, detto Incaricato accerta, in particolar modo:

- l'identità dell'Interessato;
- la completezza delle informazioni inviate;
- la presenza della copia del documento di identità dell'Interessato e, se del caso, di quello del terzo a ciò delegato, nonché della copia della procura con cui questo compito è stato conferito.

All'esito di una valutazione preliminare, l'Incaricato richiederà, se del caso, le eventuali informazioni mancanti ovvero provvederà ad evadere la richiesta. In particolare:

- nel caso di richiesta di trasferimento, estrarrà i Dati Personali oggetto della richiesta dal sistema individuato per tale finalità e provvederà ad inviare tale *file* al Titolare tramite i canali e le modalità convenzionalmente individuate dalle parti, nonché ad inviare una notifica all'Interessato di avvenuto invio del set di dati al Titolare ricevente;
- nel caso di richiesta di restituzione, estrarrà i Dati Personali oggetto della richiesta dal sistema individuato per tale finalità e provvederà ad inviare tale *file* all'Interessato;

- nel caso di richiesta di cancellazione, estrarrà i Dati Personali oggetto della richiesta dal sistema individuato per tale finalità e provvederà a rimuoverli (se digitali) o distruggerli (se cartacei).

6.4. Misure di sicurezza

La Federazione ha definito ed implementato adeguate misure di sicurezza 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.

Tra l'altro, come anticipato, la Federazione si assicura che chiunque agisca sotto la sua autorità e abbia accesso a Dati li tratti previa istruzioni in tal senso.

7. GESTIONE DEI RAPPORTI CON L'AUTORITÀ GARANTE

La gestione dei rapporti con il Garante è affidata al DPO.

Si rimanda alle relative procedure, 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.