Fondazione I.R.C.C.S.
Istituto Neurologico Carlo Besta

Sistema Socio Sanitario
Regione Lombardia

Regolamento Aziendale per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

Regolamento Aziendale per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

Premesse

La protezione delle persone fisiche, con riguardo al trattamento dei dati personali, è un diritto fondamentale dell'individuo, sancito dall'Articolo 8 della Carta dei diritti fondamentali dell'Unione Europea e dall'Articolo 16 del Trattato sul Funzionamento dell'Unione Europea (TFUE).

È indispensabile garantire un livello elevato di protezione dei dati personali coerente con i rischi che le attività di trattamento effettuate comportano, rispetto ai diritti e alle libertà fondamentali dei soggetti interessati.

La normativa vigente sulla quale si fonda il Regolamento sulla protezione dei dati della Fondazione IRCCS Istituto Neurologico "Carlo Besta" (di seguito, per brevità, anche "Istituto" o "Fondazione") riguarda:

- 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 e che abroga la direttiva 95/46/CE" (Regolamento Generale sulla Protezione dei Dati "GDPR");
- Decreto Legislativo n. 196 del 30 giugno 2003 recante il "Codice in materia di protezione dei dati personali" integrato con le modifiche introdotte dal Decreto Legislativo n. 101 del 10 agosto 2018 recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)";
- Decreto-legge n° 139 dell'8 ottobre 2021, convertito con modificazioni dalla L. 03 dicembre 2021 n° 205 - Disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali;
- Linee guida emanate dall'Agenzia per l'Italia Digitale (AgID) ai sensi dell'articolo 14-bis, comma 2, lettera a), del Decreto Legislativo n. 82 del 7 marzo 2005 "Codice dell'amministrazione digitale", per come aggiornato dal Decreto Legislativo n. 217 del 13 dicembre 2017;
- Provvedimenti, linee guida e pareri emanati dall'Autorità Garante per la protezione dei dati personali, tra cui in particolare:
    - Provvedimento del Garante Privacy del 23 novembre 2006 in materia di trattamento dei dati personali dei lavoratori con riferimento alla gestione del rapporto di lavoro;
    - Provvedimento del Garante Privacy del 27 novembre 2008 e successive modificazioni relativamente agli Amministratori di Sistema;
    - Provvedimento del Garante Privacy del 29 aprile 2010 in materia di videosorveglianza;

- Linee guida adottate dal Comitato europeo per la protezione dei dati ("European Data Protection Board", EDPB), nonché dal precedente Gruppo di lavoro "Articolo 29" (WP29), quali, ad esempio:
  - *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, adottate il 18 giugno 2021;
  - Decisione di esecuzione (UE) 2021/914 della Commissione del 4 giugno 2021 relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi a norma del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio;
  - Decisione di esecuzione (UE) 2021/915 della Commissione del 4 giugno 2021 relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio e dell'articolo 29, paragrafo 7, del Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio;
- Procedure, istruzioni operative nonché atti organizzativi, delibere e determine ed ogni altro documento interno all'organizzazione del Titolare del trattamento che risulti funzionale al raggiungimento delle finalità del presente Regolamento.

Art. 1 Oggetto

Il presente Regolamento ha lo scopo di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche e giuridiche, con particolare riferimento alla riservatezza ed all'identità personale degli utenti e di tutti coloro che hanno rapporti con la Fondazione. L'Istituto adotta idonee e preventive misure di sicurezza, volte a ridurre al minimo i rischi di distruzione o di perdita - anche accidentale - dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Art. 2 Definizioni

1) «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;
2) «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 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;

3) «Limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
4) «Profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
5) «Pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
6) «Archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
7) «Titolare del trattamento»: 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;
8) «Responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;
9) «Destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

10) «Terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare del trattamento, il Responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile;
11) «Consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
12) «Violazione dei dati personali»: 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;
13) «Dati genetici»: 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;
14) «Dati biometrici»: 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;
15) «Dati relativi alla salute»: 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;
16) «Autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento UE 2016/679.

Art. 3 Principi applicabili al trattamento dei dati personali

Ogni trattamento dei dati deve essere effettuato con modalità atte ad assicurare il rispetto dei diritti e della dignità dell'interessato.

Nello svolgimento di ogni attività di trattamento dei dati, la Fondazione opera in conformità ai seguenti principi sanciti dalla normativa nazionale e comunitaria:

- Liceità, Correttezza e Trasparenza: l'Istituto si impegna ad eseguire esclusivamente trattamenti leciti ai sensi della normativa nazionale ed europea. Pertanto, ogni autorizzato al trattamento tratta dati personali esclusivamente in forza delle diverse basi giuridiche previste dagli artt. 6 o 9 del GDPR. La Fondazione assicura, inoltre, la trasparenza dei trattamenti eseguiti, con particolare riferimento alle

finalità e modalità del trattamento, attraverso la diffusione di informative facilmente accessibili, comprensibili e redatte con linguaggio chiaro e semplice.

- Limitazione della finalità: l'Istituto predefinisce le finalità di ogni trattamento eseguito e raccoglie dati personali solo se strettamente necessari al perseguimento di tali finalità.
- Minimizzazione dei dati: la Fondazione raccoglie soli i dati funzionali ed essenziali al perseguimento delle finalità per cui il dato è trattato. Il trattamento non è eseguito in tutti i casi in cui le medesime finalità sono realizzabili mediante dati anonimi o altre modalità che rendano non determinabile l'identità dell'interessato. Inoltre, l'Istituto ha definito e formalizzato diversi livelli autorizzativi per ogni struttura. Pertanto, ogni soggetto autorizzato al trattamento dei dati può accedere esclusivamente alle categorie di dati essenziali per lo svolgimento della propria mansione lavorativa.
- Esattezza dei dati: la Fondazione effettua specifiche verifiche atte ad accertare l'esattezza dei dati dalla raccolta del dato fin alla sua cancellazione. A tal fine, durante il periodo di trattamento dei dati, effettua verifiche periodiche atte ad accertare la correttezza dei dati originariamente raccolti.
- Limitazione della conservazione: la Fondazione ha definito i tempi di conservazione di ogni tipologia di dato personale trattato. I tempi di conservazione sono stati definiti in base alla finalità per cui il dato è trattato, nonché in attuazione a quanto previsto negli obblighi contrattuali e normativi.
- Integrità e riservatezza: la Fondazione ha adottato tutte le misure, tecniche e organizzative ritenute idonee a salvaguardare la correttezza del processo di raccolta e gestione dei dati, la loro sicurezza e protezione in caso di intrusioni e alterazioni non autorizzate. Il dettaglio dei presidi adottati è contenuto in apposita sezione dei Registri del trattamento ex art. 30 GDPR.

Il trattamento dei dati personali è effettuato dall'Istituto, in quanto soggetto pubblico, per lo svolgimento dei compiti del Servizio Sanitario Nazionale annoverati tra le finalità di rilevante interesse pubblico e per l'espletamento delle funzioni istituzionali assegnate e previste dalle normative vigenti.

I trattamenti sono finalizzati all'erogazione delle prestazioni sanitarie nonché agli adempimenti amministrativi e contabili, di organizzazione e di controllo, con particolare riguardo alle attività di:

a) erogazione di prestazioni sanitarie, sia istituzionali che in libera professione (comprensive di tutte le attività di supporto), erogate in regime di ricovero, ordinario o diurno, di assistenza specialistica ambulatoriale, di Day Service o altre modalità, volte alla tutela della salute e dell'incolumità fisica degli utenti, di terzi e della collettività;
b) esercizio delle funzioni amministrative di competenza dell'Istituto:
    1. gestione del personale dipendente, comprese le procedure di assunzione;

2. gestione dei soggetti che intrattengono rapporti giuridici con l'Istituto, diversi dal rapporto di lavoro dipendente e che operano a qualsiasi titolo all'interno della Fondazione stessa, ivi compresi gli specializzandi, gli allievi e i docenti di corsi, i consulenti, i tirocinanti, i volontari;
3. gestione dei rapporti con i fornitori per l'approvvigionamento di beni e di servizi nonché con le imprese per l'esecuzione di opere edilizie e di interventi di manutenzione;
4. gestione dei rapporti con i soggetti accreditati o convenzionati;
5. gestione del contenzioso instaurato nei confronti dell'Istituto, dei rapporti con i legali e consulenti di parte;
6. rapporti con l'Autorità Giudiziaria e gli altri soggetti pubblici competenti, per le attività ispettive di vigilanza, di controllo e di accertamento delle infrazioni alle leggi e regolamenti.

Sono altresì effettuati i trattamenti di dati personali previsti da norme legislative e regolamentari concernenti l'adempimento di un obbligo legale al quale è soggetta la Fondazione, nonché, per specifiche finalità diverse da quelle di cui ai precedenti punti, trattamenti ulteriori purché l'interessato esprima il consenso al trattamento.

Art. 4 Titolare del trattamento

Titolare del trattamento dei dati personali è la Fondazione IRCCS Istituto Neurologico "Carlo Besta" nella figura del Direttore Generale, in quanto ente che determina in modo autonomo ed esclusivo le finalità e i mezzi del trattamento: il Titolare è l'ente che decide «perché» e «come» devono essere trattati i dati personali. Ai sensi dell'art. 24 GDPR, il Titolare ha la responsabilità di valutare i rischi inerenti al trattamento, nonché di adottare le misure tecniche ed organizzative adeguate a garantire ed essere in grado di dimostrare che lo stesso venga svolto conformemente al GDPR e ai principi applicabili al trattamento di dati personali stabiliti dall'art. 5 GDPR: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa e di bilancio, previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

Il Titolare adotta misure appropriate per fornire all'interessato:

a) le informazioni indicate dall'art. 13 GDPR, qualora i dati personali siano raccolti presso lo stesso interessato;

b) le informazioni indicate dall'art. 14 GDPR, qualora i dati personali non siano stati ottenuti presso lo stesso interessato.

Nel caso in cui un tipo di trattamento, specie se prevede l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35, GDPR, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento.

Il Titolare, inoltre, provvede a:

a) designare i Responsabili interni del trattamento nelle persone del Direttore Scientifico, Direttore Amministrativo e del Direttore Sanitario, nonché i Responsabili Privacy di Unità (RPU) di cui all'articolo 7, gli autorizzati di cui all'art. 8 che operano nelle singole strutture in cui si articola l'organizzazione aziendale, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza;
b) nominare il Responsabile della protezione dei dati (RPD) – Data Protection Officer (DPO);
c) nominare quali Responsabili esterni del trattamento (ai sensi dell'articolo 28 GDPR) i soggetti pubblici o privati affidatari di attività e servizi per conto della Fondazione, relativamente alle banche dati gestite da soggetti esterni alla Fondazione in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali.

Art. 5 Organizzazione interna del Titolare del trattamento - Responsabili interni del trattamento

Il Responsabile interno del trattamento è il soggetto deputato, tra l'altro, a:

i) monitorare gli aggiornamenti normativi, organizzativi e tecnici, coordinandosi con le strutture competenti;
ii) supportare il Titolare nell'aggiornamento del Registro dei trattamenti;
iii) supportare il Titolare nell'esecuzione di DPIA;
iv) supportare il Titolare nel coordinare e gestire le attività di ricezione e riscontro alle richieste degli Interessati;
v) garantire l'applicazione di procedure, istruzioni e linee guida aziendali sulla base delle istruzioni impartite dal Titolare;
vi) aggiornare costantemente il Titolare di riferimento circa lo stato delle attività.

Art. 6 Organizzazione interna del Titolare del trattamento - Responsabili Privacy di Unità

Il Responsabile Privacy di Unità è responsabile del trattamento di tutte le banche dati personali esistenti nell'articolazione organizzativa di competenza e deve essere in grado di offrire garanzie sufficienti in termini di conoscenza, esperienza, capacità ed affidabilità, per mettere in atto, sulla base delle istruzioni fornite dal Titolare, le misure tecniche e organizzative di cui all'art. 6 rivolte a garantire che i trattamenti siano effettuati in conformità al GDPR.

Il Titolare del trattamento designa quali Responsabili Privacy di Unità, per le rispettive aree di competenza, le seguenti figure:

- Direttori di Dipartimento;
- Direttori di Struttura Complessa;
- Responsabili di Strutture Semplici Dipartimentali;
- Responsabili di Strutture Semplici.

Nella lettera di designazione, il Titolare del trattamento conferisce ai suddetti RPU il compito di attuare le politiche e le procedure organizzative della Fondazione in materia di protezione dei dati personali nell'ambito della rispettiva struttura di afferenza, conformemente alle disposizioni normative vigenti.

Ogni Responsabile Privacy di Unità agisce quale *focal point* per tutte le questioni inerenti alla tematica privacy all'interno della propria organizzazione.

I principali compiti del Responsabile Privacy di Unità sono i seguenti:

- nominare per conto del Titolare i soggetti autorizzati al trattamento dei dati personali;
- sensibilizzare i soggetti autorizzati sulla rilevanza del tema privacy nelle attività quotidiane;
- fornire supporto ad ogni soggetto autorizzato al trattamento per l'analisi e la risoluzione di dubbi/difficoltà connesse al trattamento dei dati;
- verificare che le istruzioni impartite dal Titolare – e comunicate attraverso qualsiasi strumento – siano effettivamente conosciute dai soggetti autorizzati;
- verificare che tutte le misure tecniche e organizzative, volte ad evitare rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito definite dal Titolare siano scrupolosamente osservate;
- valutare annualmente l'adeguatezza delle misure di protezione, tecniche e organizzative, adottate;
- provvedere alla compilazione del Registro dei trattamenti ex art. 30 GDPR e al suo aggiornamento periodico, nelle parti di Sua competenza, con le modalità che saranno, di volta in volta, rese note dal Titolare;

- individuare le terze parti che assumo il ruolo di Responsabili del trattamento e vigilare sul rispetto della designazione e delle istruzioni impartite, con il supporto delle strutture competenti.

Ogni Responsabile Privacy di Unità è altresì tenuto a comunicare al DPO e alla S.C. Affari Legali e Generali:

- la necessità di avviare un nuovo processo operativo, di utilizzare un nuovo sistema informativo o di interrompere un processo già in corso;
- ogni eventuale difficoltà riscontrata nell'esercizio della propria funzione;
- le variazioni apportate ai livelli di sicurezza imposti dal Titolare;
- ogni carenza e/o inadeguatezza delle misure di protezione adottate dal Titolare del trattamento nelle aree di propria competenza;
- le richieste di esercizio dei diritti formulate dagli Interessati;
- ogni comportamento od evento che possa determinare una violazione del sistema di gestione privacy adottato dal Titolare o che, più in generale, sia rilevante ai fini della normativa in materia di protezione dei dati personali;
- ogni circostanza idonea a determinare anche solo potenzialmente una violazione dei dati (es. dispersione, distruzione, accesso non autorizzato e comunque trattamenti non consentiti).

L'elenco dei nominativi dei Responsabile Privacy di Unità individuati e nominati è costantemente aggiornato a cura della S.C. Gestione e Sviluppo delle Risorse Umane e conservato presso gli archivi della stessa.

Art. 7 Organizzazione interna del Titolare del trattamento – Autorizzati

Il Titolare del trattamento, per il tramite dei Responsabili Privacy di Unità, individua i soggetti **Autorizzati al trattamento**, ai sensi dell'art. 29, del GDPR "216/679, intesi come persone fisiche autorizzate a compiere operazioni di trattamento.

I soggetti individuati come autorizzati al trattamento sono designati con nota di incarico a firma del RPU, in cui sono ampiamente descritti il ruolo e i compiti loro attribuiti nel trattamento dei dati, nonché le istruzioni cui dovranno attenersi nell'esercizio delle loro funzioni e attribuzioni.

Tali soggetti, nello svolgimento della propria attività, devono rispettare le regole del Sistema Privacy della Fondazione, le indicazioni in materia di protezione dei dati personali contenute nelle procedure di regolamentazione interne, nonché tutte le istruzioni impartite dal Titolare.

In particolare, sono tenuti ad operare con la massima diligenza e attenzione, in modo tale che i dati siano:

- trattati in modo lecito, corretto e non eccedente rispetto alle finalità per le quali sono stati raccolti;
- registrati, utilizzati e raccolti per scopi attinenti alle mansioni assegnate a ciascuna struttura;
- conservati per un periodo non superiore a quello necessario per gli scopi del trattamento;

- non comunicati e/o diffusi all'esterno a soggetti non autorizzati in qualunque forma e per qualunque finalità, se non previa autorizzazione del Titolare del trattamento.

Ogni soggetto autorizzato è poi tenuto a comunicare al DPO e alla S.C. Affari Legali e Generali:

- ogni eventuale difficoltà riscontrata nell'esercizio della propria mansione,
- le richieste di esercizio dei diritti formulate dagli interessati,
- ogni comportamento od evento che possa determinare una violazione del Sistema Privacy o che, più in generale, sia rilevante ai fini della normativa in materia di protezione dei dati personali;
- ogni circostanza idonea a determinare potenzialmente una violazione dei dati (es. dispersione, distruzione, accesso non autorizzato e comunque trattamenti non consentiti).

Art. 8 Responsabili esterni del trattamento

Il Titolare può avvalersi, per il trattamento di dati, anche particolari, di soggetti pubblici o privati che, in qualità di **Responsabili esterni** del trattamento (ai sensi dell'art. 28 del GDPR), forniscano le garanzie di cui al par. 1 art. 28 GDPR, stipulando atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento. Gli atti che disciplinano il rapporto tra il Titolare ed i Responsabili esterni del trattamento devono in particolare contenere quanto previsto dall'art. 28, par. 3, GDPR; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.

Nell'individuare i soggetti da nominare sono applicati i seguenti criteri fondamentali:

- che sia un'entità distinta e separata rispetto al Titolare del trattamento;
- che tratti dati personali per conto ed in nome del Titolare del trattamento e su sua documentata istruzione (fermo restando che le istruzioni del Titolare del trattamento possono lasciare un certo grado di discrezionalità consentendo al Responsabile del trattamento di scegliere la soluzione tecnica e organizzativa più adatta al caso concreto).

Tutti i fornitori nominati Responsabili del trattamento sono inseriti nel Registro dei Responsabile, tenuto in forma digitale dalla Fondazione, in cui sono annotati anche il giorno di sottoscrizione della nomina ed eventuali verifiche svolte sul Responsabile.

Art. 9 Responsabile della protezione dati – Data Protection Officer (DPO)

Il Responsabile della protezione dei dati – Data Protection Officer (in seguito indicato con "DPO") è individuato in un soggetto esterno / società scelta tramite procedura ad evidenza pubblica.

Il DPO è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR e dalle altre normative relative alla protezione dei dati. In tal senso il DPO può indicare al Titolare del trattamento i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;
b) sorvegliare l'osservanza del GDPR e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare del trattamento;
c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare del trattamento;
d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il DPO in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al GDPR;
e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 GDPR, ed effettuare, se del caso, consultazioni relativamente ad ogni altra questione. A tali fini il nominativo del DPO è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante;
f) altri compiti e funzioni a condizione che tali compiti e funzioni non diano adito a un conflitto di interessi. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del DPO.

Il Titolare assicura che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

A tal fine:

- il DPO è invitato a partecipare alle riunioni di coordinamento dei Dirigenti/Responsabili P.O. che abbiano per oggetto questioni inerenti alla protezione dei dati personali;
- il DPO deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;

- il parere del DPO sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal DPO, è necessario motivare specificamente tale decisione;
- il DPO deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

Nello svolgimento dei compiti affidatigli il DPO deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. In tal senso il DPO:

- procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;
- definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare.

Il DPO dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio della Fondazione.

La figura di DPO è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili (in relazione alle dimensioni organizzative della Fondazione):

- il Responsabile per la prevenzione della corruzione e per la trasparenza;
- i Responsabili interni e i sub responsabili del trattamento;
- qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

Il Titolare fornisce al DPO le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare, è assicurato al DPO:

- supporto attivo per lo svolgimento dei compiti da parte dei Dirigenti/Responsabili P.O. e degli altri organi di natura amministrativa e politica, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa, di bilancio e di Piano della performance;
- tempo sufficiente per l'espletamento dei compiti affidati al DPO;
- comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno della Fondazione;
- accesso garantito ai settori funzionali della Fondazione così da fornirgli supporto, informazioni e input essenziali.

Il DPO opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione

attinente alla normativa in materia di protezione dei dati. Il DPO non può essere rimosso o penalizzato dal Titolare e dai Responsabili Interni del trattamento per l'adempimento dei propri compiti.

Ferma restando l'indipendenza nello svolgimento di detti compiti, il DPO riferisce direttamente al Titolare - o suo delegato - o ai Responsabili interni del trattamento. Nel caso in cui siano rilevate dal DPO o sottoposte alla sua attenzione decisioni incompatibili con il GDPR e con le indicazioni fornite dallo stesso DPO, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed ai Responsabili interni del trattamento.

Art. 10 Sicurezza del trattamento

Il Titolare e i Responsabili esterni del trattamento mettono in atto misure tecniche ed organizzative adeguate a garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento possono ricomprendere, se del caso: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Costituiscono misure tecniche ed organizzative che possono essere adottate:

- sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);
- misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

Art. 11 Informazioni per la raccolta dei dati

La Fondazione, quale Titolare del trattamento, adotta misure appropriate per fornire all'interessato tutte le informazioni e comunicazioni riguardanti il trattamento dei dati quali l'identità ed i dati di contatto del titolare del trattamento, i dati di contatto del responsabile della protezione dei dati, le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento, i legittimi interessi perseguiti dal titolare del trattamento o dai terzi, gli eventuali destinatari dei dati personali.

Nel momento in cui i dati personali sono ottenuti, il Titolare fornisce all'interessato ulteriori informazioni per garantire un trattamento corretto e trasparente quali:

a) l'identità ed i dati di contatto del titolare del trattamento;
b) i dati di contatto del responsabile della protezione dei dati;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
e) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale;
f) il periodo di conservazione dei dati personali, oppure se non è possibile, i criteri utilizzati per determinare tale periodo;
g) l'esistenza del diritto dell'interessato di chiedere al titolare l'accesso ai dati personali e la rettifica o la cancellazione degli stessi, ove possibile, o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
h) l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
i) il diritto di proporre reclamo ad un'autorità di controllo;
j) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
k) esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora l'Istituto intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente.

Qualora i dati non siano stati ottenuti presso l'interessato, la Fondazione fornisce all'interessato anche le informazioni relative alla fonte dalla quale ha tratto i suoi dati.

Art. 12 Registro delle attività di trattamento

Il Registro dei trattamenti della Fondazione è un documento telematico, formato da molteplici sezioni di lavoro, ciascuna dedicata ad uno specifico trattamento come di seguito meglio specificato.

La Fondazione si è dotata di un proprio Registro dei trattamenti, non solo al fine di adempiere all'obbligo normativo previsto dall'art. 30 GDPR, ma anche e soprattutto al fine di dotarsi di uno strumento attraverso cui svolgere un'analisi accurata dei dati trattati, una mappatura approfondita dei trattamenti ed una ricognizione puntuale delle finalità perseguite.

Ciascuna scheda di censimento è costituita da molteplici sezioni, ognuna dotata di una propria denominazione, tra cui:

- Denominazione del trattamento;
- Ruoli, ovvero i) Titolare, ii) Contitolare, iii) Responsabile di Unità, iv) Soggetti autorizzati;
- Categorie di interessati, ovvero le persone fisiche cui sono riconducibili i dati trattati;
- Categorie di dati personali, ovvero le tipologie di dati personali che costituiscono oggetto del trattamento;
- Finalità del trattamento, ovvero lo scopo perseguito dal Titolare attraverso il trattamento dei dati personali;
- Base giuridica del trattamento, ovvero il fondamento di legittimità del trattamento tra quelli di cui agli artt. 6 e 9 GDPR;
- Ambito di diffusione, ovvero luogo e modalità dell'eventuale comunicazione dei dati ad un numero di soggetti indeterminato;
- Ambito di comunicazione, ovvero destinatari dell'eventuale comunicazione dei dati;
- Termini di conservazione, ovvero i periodi di tempo massimo per cui i dati possono essere trattati dalla Fondazione;
- Misure tecniche ed organizzative, ovvero gli strumenti approntati dal Titolare per garantire un livello di sicurezza adeguato al rischio proprio di ogni trattamento effettuato.

Nel caso in cui si determini la necessità di procedere all'aggiornamento di una o più parti del Registro, ciascun Responsabile d'Unità, con il supporto del DPO ove necessario, provvede alla creazione di un nuovo trattamento.

Il Responsabile aggiorna il Registro:

(i) ogni volta che vengono modificate le aree di trattamento già registrate o vengono introdotte nuove aree di trattamento;

(ii) in ogni caso, almeno una volta all'anno.

Art. 13 Valutazioni d'impatto sulla protezione dei dati (DPIA)

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 GDPR, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

Ai fini della decisione di effettuare o meno la DPIA si tiene conto del Provvedimento del Garante Privacy 11 ottobre 2018 n° 467 relativo all'elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, pp. 4-6, del Regolamento (UE) n. 2016/679.

La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, GDPR, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

a) trattamenti valutativi o di *scoring*, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;
c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, GDPR;
e) trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;
f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il

Titolare del trattamento, come i dipendenti della Fondazione, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;

h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto. Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno alla Fondazione. Il Titolare deve consultarsi con il DPO anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il DPO monitora lo svolgimento della DPIA. Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria. Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della DPIA.

Il DPO può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale. Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:

a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);

b) valutazione della necessità e proporzionalità dei trattamenti, sulla base: delle finalità specifiche, esplicite e legittime; della liceità del trattamento; dei dati adeguati, pertinenti e limitati a quanto necessario; del periodo limitato di conservazione; delle informazioni fornite agli interessati; del diritto di accesso e portabilità dei dati; del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento; dei rapporti con i responsabili del trattamento; delle garanzie per i trasferimenti internazionali di dati; consultazione preventiva del Garante privacy;

c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;
d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Il Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

Art. 14 Violazione dei dati personali

In particolare, gli eventi di *Data Breach* possono essere suddivisi in tre macrocategorie:

- Violazione di confidenzialità *(confidentiality breach)*: divulgazione o accesso non autorizzato o accidentale ai dati personali;
- Violazione di disponibilità *(availability breach)*: perdita accidentale o non autorizzata dell'accesso ai dati o distruzione di dati personali;
- Violazione di integrità *(integrity breach)*: alterazione non autorizzata o accidentale dei dati personali.

A titolo esemplificativo, e non esaustivo, vengono riportate di seguito alcune tipologie di violazione dei dati personali:

- distruzione di dati informatici o documenti cartacei, intesa come indisponibilità irreversibile di dati con accertata impossibilità di ripristino degli stessi, conseguente a eliminazione logica (es. errata cancellazione dei dati nel corso di un intervento manuale o automatizzato o fisica, rottura di dispositivi

di memorizzazione informatica, incendio/allagamento di locali dove sono archiviati i contratti e altri documenti degli utenti);

- perdita di dati, conseguente a smarrimento/furto di supporti informatici (es. laptop, tablet, HD, memory card) o di documentazione contrattuale o altri documenti cartacei (in originale o in copia);
- accesso non autorizzato o intrusione a sistemi informativi, inteso come lo sfruttamento di vulnerabilità dei sistemi interni e delle reti di comunicazione oppure attraverso la compromissione o rilevazione abusiva di credenziali di autenticazione (es. user-id e password) per l'accesso ai sistemi;
- modifica non autorizzata di dati, derivante, ad esempio, da un'erronea esecuzione di interventi sui sistemi informatici o da interventi umani;
- rivelazione di dati e documenti a soggetti terzi non legittimati, anche non identificati, conseguenti ad esempio alla fornitura di informazioni, anche verbali, a persone diverse dal soggetto legittimato (in assenza di delega formale di quest'ultimo), all'invio di fatture o altri documenti di valore contrattuale o esecutivo, all'errata gestione di supporti informatici.

Ai sensi degli artt. 33 e 34 GDPR, in caso di *data breach*, il Titolare del trattamento deve notificare il *data breach*, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne sia venuto a conoscenza, all'Autorità di controllo, a meno che sia improbabile che il *data breach* presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora la notifica all'Autorità di controllo non avvenga effettuata entro 72 ore, è corredata dei motivi del ritardo.

Inoltre, l'art. 34 GDPR (*Comunicazione di una violazione dei dati personali all'interessato*) al par. 1 dispone che quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

Nel caso in cui la violazione si verifichi nell'ambito di un trattamento dei dati che un Responsabile svolge per conto di un Titolare, il Responsabile è tenuto ai sensi dell'art. 33, par. 2 GDPR a informare il Titolare senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

La comunicazione, in ogni caso, indica i dati, le categorie e il numero degli interessati, la violazione circostanziata, le conseguenze attuali e potenziali, le misure prese in risposta.

Ulteriori riferimenti normativi ed interpretativi sono contenuti:

- nelle Linee Guida dell'Agenzia dell'Unione Europea per la sicurezza delle reti e dell'informazione (ENISA) e ulteriori parametri tratti dall'art. 3, par. 2 reg. (UE) n. 611/2013;

- nelle Linee Guida del Gruppo di Lavoro WP29 sulla notifica delle violazioni dei dati personali – WP250 rev.01;
- nelle comunicazioni della Commissione al Parlamento europeo e al Consiglio (tra cui COM (2018), 24.1.2018, Maggiore protezione, nuove opportunità).

Art. 15 I diritti dell'interessato

La Fondazione, al fine di tutelare pienamente gli Interessati nell'ambito dei trattamenti eseguiti, ha istituto appositi canali per la ricezione delle istanze relative all'esercizio dei diritti riconosciuti all'Interessato dal Regolamento UE.

Ad ogni Interessato è riconosciuta la possibilità di esercitare – nei limiti definiti dal Regolamento – i seguenti diritti:

- Diritto di Accesso (art. 15 GDPR): esercitando il proprio diritto di accesso, l'Interessato può i) avere conferma dell'esistenza di propri dati personali presso il Titolare, ii) accedere ai dati da questo trattati. A seguito della richiesta, il Titolare è tenuto a fornire gratuitamente una copia dei dati, in forma cartacea o elettronica, potendo addebitare il costo di eventuali ulteriori copie in capo all'Interessato. Nelle ipotesi in cui il trattamento comporti una notevole quantità di informazioni, si potrà chiedere all'Interessato di specificare le informazioni a cui la richiesta si riferisce.
- Diritto di rettifica (art. 16 GDPR): ogni Interessato ha il diritto di ottenere la correzione di eventuali inesattezze nonché l'integrazione di informazioni non complete. L'inesattezza potrà in ogni caso essere inerente esclusivamente a dati di valore oggettivo. Di conseguenza, l'Interessato potrà chiedere la rettifica esclusivamente di dati fattuali e non invece di valutazioni soggettive e personali. Se non richiede uno sforzo sproporzionato, il Titolare comunica le richieste ricevute e le rettifiche/integrazioni effettuate ai soggetti cui i dati sono stati eventualmente comunicati.
- Diritto di cancellazione (diritto all'oblio) (art. 17 GDPR): nel caso di espressa richiesta dell'Interessato, il Titolare ha l'obbligo di cancellare i dati dell'Interessato, su qualsiasi supporto archiviati. Inoltre, se tali dati sono stati diffusi (es. pubblicazione su un sito web), il Titolare deve informare della richiesta di cancellazione gli altri Titolari che trattano i dati personali oggetto della richiesta di cancellazione, invitandoli a rimuovere ogni copia degli stessi. In ogni caso, si precisa che la richiesta di cancellazione deve essere accolta solo al ricorrere di una delle ipotesi previste dal Regolamento Europeo: 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 società dell'informazione di cui all'articolo 8, paragrafo 1.

In ogni caso, la richiesta sarà respinta in tutte le ipotesi in cui ricorra una delle fattispecie derogatorie previste dagli artt. 2-undecies e 2-duodecies del Codice Privacy.

In forza dello specifico interesse connesso ai dati oggetto della richiesta, il Titolare del trattamento potrà optare per la loro cancellazione o anonimizzazione.

- Diritto di limitazione del trattamento (art. 18 GDPR): l'Interessato può chiedere al Titolare di limitare il trattamento dei propri dati solo con riferimento ad alcune specifiche finalità ma solo al ricorrere di una delle quattro ipotesi tassativamente elencate all'art. 18 del GDPR, ovvero in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), nel caso in cui l'interessato chieda la rettifica dei dati (in attesa di tale rettifica da parte del titolare) o si opponga al loro trattamento ai sensi dell'art. 21 del GDPR (in attesa della valutazione da parte del titolare), nelle ipotesi in cui i dati non siano più necessari al Titolare per il perseguimento delle proprie finalità ma divengano necessari per l'esercizio o la difesa di un diritto dell'interessato in sede giudiziaria.

  Le tempistiche di limitazione sono strettamente connesse alla ragione posta a fondamento della richiesta. Infatti, nel caso in cui la limitazione sia richiesta per consentire la verifica della correttezza dei dati, per l'esercizio del diritto di opposizione o per l'esercizio di un diritto giudiziario dell'interessato i dati potranno essere nuovamente resi disponibili in seguito all'accertamento; nel caso di trattamento illegittimo e conseguente richiesta di limitazione dell'Interessato, la limitazione potrà proseguire fino alla cancellazione dei dati o, all'eventuale, richiesta di portabilità dell'Interessato.

  La richiesta è in ogni caso derogata in tutte le ipotesi derogatori di cui agli artt. 2-undecies e 2-duodecies del Codice Privacy.

- Diritto alla portabilità dei dati (art. 20 GDPR): il diritto alla portabilità dei dati consente all'Interessato a) di ottenere, su richiesta, la restituzione dei propri dati personali da parte del Titolare del trattamento e b) la loro trasmissione ad un nuovo Titolare. La richiesta di portabilità può essere accolta solo al ricorrere di determinati presupposti: 1) sono portabili solo i dati trattati con il consenso dell'Interessato o sulla base di un contratto stipulato con l'interessato e 2) solo i dati che siano stati "forniti" dall'Interessato al Titolare, inoltre 3) il diritto alla portabilità può essere soddisfatto solo se non lesivo di diritti e libertà altrui.

- Diritto di opposizione (art. 21 GDPR): l'Interessato può chiedere l'interruzione, in modo permanente, del trattamento dei suoi dati personali. La richiesta di opposizione sarà accolta esclusivamente al ricorrere delle ipotesi previste dall'art. 21 par. 1 Regolamento Europeo. Quando accolta, la richiesta di opposizione obbliga il Titolare ad interrompere il trattamento in modo definitivo e permanente.
- Diritto di reclamo (art. 77 GDPR): l'Interessato ha sempre il diritto di proporre reclamo al Garante della privacy qualora ritenga che i diritti di cui gode a norma della disciplina vigente sono stati violati a seguito di un trattamento.

Nelle informative rese agli Interessati al momento della raccolta dei dati, la Fondazione comunica la possibilità di esercitare i diritti di cui al GDPR, ovvero di chiedere: l'accesso ai dati personali, l'indicazione delle modalità, finalità e logiche del trattamento, la richiesta di limitazione, opposizione o portabilità dei dati, la rettifica e la cancellazione, nei limiti e nelle modalità indicate dal Regolamento, nonché, laddove il trattamento dei dati si basi sul consenso, il diritto di revocarlo in qualsiasi momento.

Da ultimo, le informative contengono esplicito riferimento alla possibilità per gli Interessati di proporre reclamo all'autorità di controllo ai sensi dell'art. 77 del Regolamento.

Ai sensi dell'art. 12, par. 3 del GDPR, l'Istituto fornisce riscontro all'interessato senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto delle complessità e del numero delle richieste. Il Titolare è tenuto, però, ad informare l'interessato di tale proroga e dei motivi del ritardo, entro un mese dal ricevimento della richiesta.

Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.

Art. 16 Trasferimento dei dati extra-UE

Per trasferimento di dati personali deve intendersi ogni ipotesi in cui i dati personali siano accessibili in uno stato Extra UE, non solo mediante un vero e proprio trasferimento, ma anche tramite il semplice accesso da remoto.

A tal proposito, l'*European Data Protection Board* stabilisce, all'interno delle *recommendations* approvate il 10 novembre 2020, che l'accesso di un soggetto da un Paese terzo a dati personali che sono collocati in Europa è altresì considerato trasferimento.

Ai sensi del Capo V GDPR (articolo 44 e ss.) i dati personali degli interessati possono essere trasferiti verso un Paese terzo o un'organizzazione internazionale dal Titolare del trattamento che sia stabilito nel territorio dell'Unione.

Tuttavia, tale trasferimento transfrontaliero può essere effettuato solo se sussiste almeno una delle seguenti condizioni:

i. la presenza di una decisione di adeguatezza (articolo 45 GDPR),
ii. garanzie adeguate fornite dal Titolare con annessi diritti azionabili e mezzi di ricorso effettivi a vantaggio degli interessati (articolo 46 GDPR),
iii. norme vincolanti d'impresa (articolo 47 GDPR),
iv. specifiche situazioni sancite dall'articolo 49 GDPR.

Nello specifico, laddove non vi sia una decisione di adeguatezza della Commissione Europea, prima di procedere con il trasferimento di dati personali in un Paese Terzo, mediante utilizzo di diverse condizioni di trasferimento, quali le Clausole Contrattuali Standard o le Norme Vincolanti d'Impresa, l'esportatore congiuntamente con l'importatore deve verificare che il Paese terzo assicuri un livello di protezione dei dati personali sostanzialmente equivalente a quello garantito dalla legislazione europea.

Le *recommendations* dell'EDPB, sopra citate, delineano un percorso valutativo che occorre seguire prima di procedere al trasferimento affinché possano valutarsi le garanzie sottese.

Le *recommendations* sono state, infatti, approvate allo scopo di fornire supporto agli esportatori e importatori di dati personali dopo che la Corte di Giustizia dell'Unione Europea, nella sentenza Schrems II del 16 luglio 2020, ha invalidato il c.d. *Privacy Shield*, che legittimava il trasferimento di dati dall'Unione Europea verso gli Stati Uniti, affermando che l'esportatore e l'importatore di dati personali devono verificare che nell'ambito del trasferimento sia assicurato un livello di garanzia sostanzialmente equivalente a quello previsto dalla normativa europea.

Con le proprie *recommendations*, dunque, l'EDPB fornisce una *roadmap* per determinare le garanzie ed elenca, altresì, delle misure supplementari da adottarsi nei casi in cui, all'esito del procedimento valutativo, emerga che le garanzie assicurate dal Paese terzo non sono equivalenti a quelle dettate dalla disciplina del GDPR.

Successivamente alle *recommendations* del 2020, sono state approvate dalla Commissione Europea le nuove Clausole Contrattuali Standard (Decisione di esecuzione della Commissione Europea 2021/915) che prevedono al proprio interno delle clausole in base alle quali, al fine di garantire la sicurezza nei trattamenti, sono previsti specifici obblighi in capo all'importatore e all'esportatore, nonché precise indicazioni ed adempimenti in caso di richieste e/o accessi delle autorità pubbliche locali.

Nello svolgimento della propria attività, la Fondazione non trasferisce dati personali al di fuori dell'Unione Europea.

Nel caso in cui dovesse emergere la necessità di procedere con il trasferimento, questo sarebbe ammesso solo se anticipato dalla verifica che sussista una delle condizioni di cui al Capo V del GDPR o una delle deroghe di cui all'art. 49 del GDPR di seguito riepilogate:

1. l'interessato ha acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato;
2. il trasferimento è necessario all'esecuzione di un contratto stipulato tra il Titolare del trattamento e l'interessato ovvero all'esecuzione di misure precontrattuali su richiesta dell'interessato;
3. il trasferimento è necessario per la conclusione o l'esecuzione di un contratto stipulato tra il Titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato;
4. il trasferimento è necessario per importanti motivi di interesse pubblico;
5. il trasferimento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
6. il trasferimento è necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
7. il trasferimento sia effettuato a partita da un registro che, a norma del diritto dell'Unione o degli Stati Membri, mira a fornire informazioni al pubblico e può essere consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati Membri.

Nei casi in cui il trasferimento di dati verso Paesi extra-UE avvenga nell'ambito del rapporto tra un Responsabile esterno debitamente nominato ex art. 28 GDPR ed un suo fornitore, il Titolare deve espressamente e previamente autorizzare il trasferimento.

A tal fine, il Responsabile è tenuto a rivolgere al Titolare la richiesta di autorizzazione al trasferimento dei dati in Paesi Extra-UE fornendo la documentazione attestante la legittimità del trasferimento nel rispetto del Regolamento.

Art. 17 Controllo

Un primo livello di controllo è in carico al Responsabile Privacy di Unità, il quale dovrà verificare che le istruzioni fornite agli autorizzati con specifiche lettere di incarico siano effettivamente rispettate e applicate.

Un secondo livello di controllo è invece in carico al Responsabile interno del trattamento, il quale, ha la facoltà di effettuare specifici *assessment* e verifiche a campione, finalizzate a monitorare la corretta applicazione delle regole, delle procedure e delle istruzioni fornite, nonché effettua verifiche su tutto il sistema privacy del Titolare.

Il terzo livello di controllo è, da ultimo, in capo al DPO.

Art. 18 Sanzioni Amministrative e risarcimento del danno

In caso di violazione della disciplina prevista dal Regolamento UE, ai sensi dell'articolo 83 GDPR e dell'art. 166 del D. Lgs. 196/2003, l'Autorità di controllo provvede ad infliggere sanzioni amministrative pecuniarie.

In particolare, in base alla tipologia di violazione le sanzioni possono ammontare fino a 10 milioni di euro, o fino al 2% del fatturato mondiale annuo della società se superiore, ovvero fino a 20 milioni di euro, o fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente se superiore.

Ancora, il Titolare del trattamento ovvero il Responsabile del trattamento devono, ai sensi dell'articolo 82 del GDPR, risarcire il danno all'interessato che abbia subito un danno materiale o immateriale causato dalla violazione e che ne faccia richiesta.

Inoltre, le Autorità di controllo possono limitare, sospendere ovvero anche bloccare un trattamento di dati.

Il GDPR non prevede direttamente delle sanzioni penali in materia di protezione dei dati personali; tuttavia, nel Considerando 149 stabilisce che gli Stati membri dovrebbero poter stabilire disposizioni relative a sanzioni penali per violazioni del Regolamento.

Sono state inserite, pertanto, delle sanzioni penali nel Codice Privacy mediante il D. Lgs. n. 101 del 2018, di seguito riepilogate.

Norma incriminatrice	Descrizione	Sanzione
Art. 167 Trattamento illecito di dati	Sanziona chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, **arreca nocumento all'interessato**in violazione di specifiche disposizioni di legge. È punito chi al fine di trarre per sé o per altri profitto o di arrecare danno all'interessato procedendo al trasferimento dei dati personaliverso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti, arreca nocumento all'interessato	Reclusione da sei mesi aun anno e sei mesi Reclusione da uno a treanni
Art. 167 *bis* Comunicazionee diffusione illecita di dati personali oggetto di trattamento su larga scala	**Sanziona la comunicazione e diffusione**, al finedi trarre profitto per sé o altri ovvero al fine di arrecare danno, di un **archivio automatizzato** ouna parte sostanziale dello stesso contenente dati personali oggetto di trattamento su larga scala anche quando lo si fa senza consenso quando questo è richiesto per le operazioni di comunicazione e di diffusione.	Reclusione da uno a sei anni
Art. 167 *ter* Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala	Sanziona la condotta per cui, al fine di trarne profitto per sé o altri, ovvero di arrecare danno, si acquisiscano con **mezzi fraudolenti** un **archivio automatizzato** o una parte sostanziale dello stesso contenente dati personali oggetto di trattamento su larga scala	Reclusione da uno aquattro anni
Art. 168	Sanziona chiunque, in un procedimento o nel corso	Reclusione da sei

Falsità nelle dichiarazioni al Garante einterruzione dell'esecuzione dei compitio dell'esercizio dei poteri del Garante	di accertamenti dinanzi al Garante, dichiario attesti falsamente notizie o circostanze o produce atti o documenti falsi Sanziona altresì colui che **cagioni intenzionalmente un'interruzione** o turbi la regolarità di un procedimento dinanzi al Garanteo degli accertamenti da questi svolti.	mesi atre anni Reclusione fino a unanno
Art. 170 Inosservanza di provvedimenti del Garante	Sanziona l'inosservanza di provvedimenti del Garante	Reclusione da 3 mesi a 2 anni
Art. 171 Violazione delle disposizioni in materia di Controlli a distanza e indagini sulle opinioni deilavoratori	Sanziona l'utilizzo da parte dei datori di lavoro degli impianti audiovisivi e degli altri strumenti dai quali derivi anche la possibilità di controllo adistanza dell'attività dei lavoratori (possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale epossono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali o, in mancanza di accordo,previa autorizzazione dell'Ispettorato). Sanziona altresì la violazione del divieto al datoredi lavoro, ai fini dell'assunzione e nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore.	Arresto da 15 giorni a un anno

Nel caso in cui i soggetti autorizzati violino, eludano o applichino parzialmente o non correttamente le norme del Sistema Privacy della Fondazione saranno sanzionati ai sensi della disciplina relativa ai contratti di lavoro, con particolare riferimento agli illeciti disciplinari, e la sanzione sarà modulata rispetto al livello di responsabilità ed autonomia del dipendente, all'intenzionalità del comportamento e alla gravità del medesimo rispetto agli effetti a cui il Titolare può ragionevolmente ritenersi esposto.

Art. 19 Rinvio

Per tutto quanto non espressamente disciplinato nel presente Regolamento, si applicano le disposizioni del GDPR e tutte le sue norme attuative vigenti, nonché le Procedure, i Regolamenti, le Istruzioni Operative delle Fondazione vigenti in materia.