POLITICA GENERALE IN MATERIA DI PROTEZIONE DI DATI PERSONALI

FONDAZIONE SDN PER LA RICERCA E L'ALTA FORMAZIONE IN DIAGNOSTICA NUCLEARE

INDICE

1. OBIETTIVI E AMBITO APPLICATIVO

Garantire la sicurezza e la riservatezza dei dati personali, sia comuni che relativi a categorie particolari, è una delle priorità di Fondazione SDN.

Obiettivo della Politica è rappresentare le regole e i principi cui la Fondazione si ispira, in ossequio a quanto stabilito:

- dal Regolamento UE, n. 679/2016, Regolamento Generale sulla Protezione dei dati (di seguito anche "GDPR" o "Regolamento") e, segnatamente dall'art. 24, comma 2, che abroga la precedente Direttiva 95/46/CE e disciplina gli aspetti relativi alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione degli stessi.
- dal Decreto Legislativo n. 196/2003 "Codice in materia di protezione dei dati personali" (di seguito "Codice Privacy"), dagli allegati al Codice così come modificati dalla Legge 25 ottobre 2017, n. 163 Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017;
- dai Provvedimenti, dalle Linee Guida e dai Pareri emessi dall'Autorità Garante per la protezione dei dati personali (di seguito "Garante Privacy"), dal Gruppo di Lavoro ex art. 29 e dal Garante Europeo della Protezione dei Dati (GEPD).

Il documento si applica agli utenti, a tutto il personale della Fondazione, a fornitori, a terzi ed a tutte le persone fisiche i cui dati personali vengono trattati dal Titolare.

2. DEFINIZIONI

Ai fini del Regolamento Generale sulla Protezione dei dati personali, s'intende per:

a) «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata 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;

b) «**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;

c) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

d) «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi

auna persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimentoprofessionale, la situazione economica, la salute, le preferenze personali, gli interessi,l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

e) «**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personalinon possano più essere attribuiti a un interessato specifico senza l'utilizzo diinformazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservateseparatamente e soggette a misure tecniche e organizzative intese a garantire che talidati personali non siano attribuiti a una persona fisica identificata o identificabile;

f) «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criterideterminati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzatoo ripartito in modo funzionale o geografico;

g) «**titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizioo altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi deltrattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinatidal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criterispecifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione degli Stati membri;

h) «**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;

i) «**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altroorganismo 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'ambitodi una specifica indagine conformemente al diritto dell'Unione o degli Statimembri non sono considerate destinatari; il trattamento di tali dati da parte di dette autoritàpubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

j) «**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismoche 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 delresponsabile;

k) «**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprioassenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali chelo riguardano siano oggetto di trattamento;

l) «**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmenteo in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzatao l'accesso ai dati personali trasmessi, conservati o comunque trattati;

m) **«dati genetici»:** i dati personali relativi alle caratteristiche genetiche ereditarie o acquisitedi una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salutedi detta persona fisica, e che risultano in particolare dall'analisi di un campione biologicodella persona fisica in questione;

n) **«dati biometrici»**: i dati personali ottenuti da un trattamento tecnico specifico relativi allecaratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentonoo confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

o) **«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.

3. RUOLI E RESPONSABILITÀ

3.1. STRUTTURA ORGANIZZATIVA

Il trattamento di dati personali dà luogo ad un rapporto giuridico tra un soggetto che acquisisce i dati o svolge altre operazioni sui medesimi, che si propone di definire come "soggetto attivo del trattamento", ed un soggetto al quale i dati personali si riferiscono, definito "soggetto passivo del trattamento". Le norme sulla protezione dei dati personali individuano, pertanto, sul lato dei soggetti attivi del trattamento, alcune figure organizzative obbligatorie:

3.2. TITOLARE DEL TRATTAMENTO

Fondazione SDN, ai fini previsti dal GDPR, è il Titolare del trattamento (di seguito indicato con "Titolare") dei dati personali raccolti o meno in banche dati, automatizzate o cartacee, e direttamente presso gli Interessati. Il Titolare è il centro di imputazione delle decisioni sulle finalità e sui mezzi del trattamento, sia esso persona fisica o giuridica[1], pubblica o privata, riconosciuta o meno.

In quanto ruolo apicale dell'intera catena di trattamento dei dati personali, il Titolare decide sulle finalità, sui mezzi e sul profilo della sicurezza, e, inoltre, può individuare, all'interno della propria struttura, ruoli "subordinati" a cui affidare operazioni di trattamento, istruendoli adeguatamente, e può, altresì, esternalizzare attività di trattamento designando Responsabili del trattamento ed istruendoli adeguatamente. Può, inoltre, autorizzare i Responsabili a designare altri Responsabili (c.d. Sub-Responsabile).

[1]Nel caso di persona giuridiche, pubbliche o private, riconosciute o meno, è la persona giuridica nel suo complesso che va considerata Titolare del trattamento, non il singolo organo decisionale, né la persona fisica o le persone fisiche che la rappresentano. Pertanto, centro di imputazione delle responsabilità e degli oneri probatori risulterà essere la persona giuridica nel suo complesso.

Il Titolare garantisce il rispetto dei 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.

Il Titolare, in relazioni agli obblighi ed agli adempimenti in materia di sicurezza, mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al GDPR (ex art. 32, GDPR). Le misure sono definite fin dalla fase di progettazione (*Privacy by design*, ex art. 25, GDPR) e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 GDPR, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio (*Privacy by default*, ex art. 25, GDPR).

Il Titolare adotta misure appropriate, a garanzia dei diritti e delle libertà degli interessati, per fornire:

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 stati ottenuti presso lo stesso interessato.

Fondazione SDN, pertanto, provvede a:

a) decidere, in piena autonomia, in ordine alle finalità e alle modalità dei trattamenti dei dati personali, nonché agli strumenti utilizzati e al profilo della sicurezza;
b) rispettare i doveri di correttezza per l'intera durata del trattamento, conformandosi ai principi di trasparenza e di responsabilizzazione *(«accountability»);*
c) nominare il *Data ProtectionOfficer* (DPO);
d) designare e/o nominare quale Responsabile esterno del trattamento i soggetti affidatari di attività e servizi per conto della Fondazione, relativamente alle banche dati gestite da soggetti esterni 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 aziendali;
e) autorizzare e istruire il personale, ovvero i soggetti autorizzati/referenti interni (c.d. "autorizzati"), compresi i Dirigenti/responsabili delle singole Direzioni, Aree, Settori ed Uffici in cui si articola l'organizzazione, che effettuano operazioni di trattamento all'interno della Fondazione;
f) individuare, e disciplinare con apposito atto formale, le ipotesi in cui, con altro o altri Titolari, determina congiuntamente le finalità e/o i mezzi del trattamento, rendendo manifesta la Contitolarità ex art. 26, GDPR[2];
g) attuare contromisure effettive e tempestive nel caso di violazioni dei dati personali, procedendo, se del caso, alla notificazione all'Autorità di controllo ed alla comunicazione all'interessato;

[2]L'Accordo di Riparto, previsto dall'art. 26, GDPR, nell'ipotesi della Contitolarità, costituisce un obbligo per i Contitolari. Esso deve riflettere, in modo puntuale, i ruoli reciproci, il riparto degli obblighi previsti dal Regolamento Europeo, N. 679/16, il rapporto reciproco nei confronti degli interessati (ad es. in materia di riscontro e di fornitura della informativa). Il contenuto essenziale di tale Accordo deve essere messo a disposizione degli interessati. L'Accordo è inopponibile all'interessato.

h) coopera con l'Autorità di controllo.

Fondazione SDN, inoltre, favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del GDPR e per dimostrarne il concreto rispetto da parte del Titolare.

3.3. RESPONSABILE DEL TRATTAMENTO

Nei casi in cui un soggetto terzo effettua trattamenti di dati personali per conto diFondazione SDN, non può essere considerato come autonomo Titolare o Contitolare, questi è obbligatoriamente designato come Responsabile (esterno) del trattamento dati esterno (di seguito indicato con "Responsabile") ai sensi dell'art. 28 del Regolamento UE, N. 679/2016. L'elemento dirimente del ruolo del Responsabile consiste nella strumentalità rispetto alla finalità decisa dal Titolare. Se il Responsabile fuoriesce dall'alveo della strumentalità e usa i dati per finalità e mezzi propri, si colloca *ipso facto* in una posizione assimilata a quella del Titolare.

Il Responsabile, quindi, può essere una persona fisica o giuridica, pubblica o privata, riconosciuta o no. Deve presentare garanzie sufficienti al fine di attuare misure tecniche ed organizzative adeguate.

La designazione avviene per contratto o altro atto giuridico, scritto, vincolante per il Responsabile, stipulato anche in forma elettronica, che contiene una serie di clausole minime inderogabili, ex art. 28, par. 3, Reg. Ue, N. 679/2016. La caratteristica principale dell'atto di designazione è la vincolatività: quale che sia lo strumento di designazione (contratto o altro atto giuridico), è essenziale che esso sia vincolante per il Responsabile.

Il Responsabile ha il dovere di agire secondo le istruzioni di trattamento fornite dal Titolare e di impartirle, in senso conforme, ai suoi dipendenti e collaboratori che accedano a dati personali forniti dal Titolare. Deve, inoltre, assistere il Titolare, se richiesto, nel garantire il rispetto degli obblighi derivanti dallo svolgimento di una Valutazione d'Impatto sulla Protezione dei dati (DPIA, ex art. 35, Reg. Ue, N. 679/2016).

Il Responsabile deve collaborare con l'Autorità di controllo e con gli organismi indipendenti di certificazione. Presta supporto al DPO del Titolare, fornendolo dei mezzi, delle informazioni e degli accessi necessari a realizzare la sua attività, senza interferire con istruzioni nello svolgimento dei suoi compiti.

Per il risarcimento del danno cagionato dal trattamento, il Responsabile risponde in solido col Titolare, ma entro i limiti in cui siano configurabili violazioni o inadempimenti a lui imputabili. Nell'ipotesi in cui uno dei due paghi l'intero, ha regresso, conformemente alla parte di responsabilità dell'altro.

Il Responsabile, inoltre, può designare espressamente, con autorizzazione particolare o generale da parte del Titolare del trattamento, un altro Responsabile (c.d. Sub – Responsabile). Le istruzioni del primo Responsabile al secondo, così come quelle interne del Responsabile ai suoi dipendenti, dovranno essere conformi alle istruzioni del Titolare. Il rapporto, pertanto, rifletterà esclusivi connotati di strumentalità alle finalità del Titolare.

3.4. SOGGETTI AUTORIZZATI AL TRATTAMENTO

Fondazione SDN prevede, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento dei dati personali, siano attribuiti a persone fisiche, espressamente designate, che operano sotto la propria autorità.

La Fondazioneindividua le modalità più opportune per autorizzare al trattamento dei dati personali i soggetti che operano sotto la propria autorità diretta. Ciò avviene per il tramite di lettere di autorizzazione differenziate per ruolo e mansione svolti.

Designa come "Soggetto autorizzato del trattamento" tutto il proprio personale; contestualmente all'assunzione, l'ufficio Risorse Umane fornisce l'informativa Dipendenti e Collaboratori, e la lettera di nomina a "Soggetto autorizzato del trattamento".

Può designare come soggetti autorizzati anche persone fisiche esterne alla Fondazione che, per esigenze legate alle attività contrattualizzate, partecipano ai trattamenti di dati personali di cuiFondazione SDN è Titolare.

Ogni soggetto autorizzato deve attenersi alle istruzioni ricevute dal Titolare del trattamento. La Fondazioneprovvede all'adeguata formazione professionale nella materia della *data protection*.

3.5. RESPONSABILE DELLA PROTEZIONE DATI *(DATA PROTECTIONOFFICER)*

Il Titolare del trattamento ha designato il Responsabile della protezione dei dati/*Data ProtectionOfficer* (in seguito indicato con "DPO"). Il DPO, la cui nomina risulta obbligatoria perFondazione SDN, ex art. 37, par. 1, lett. c)[3], Reg. UE, N. 679/2016, svolge un ruolo di vigilanza dei processi interni alla struttura del Titolare e dei Responsabili, di consulenza, di contatto rispetto agli interessati ed alle Autorità di controllo; viene, inoltre, investito di ogni questione interna in materia di protezione dei dati personali.

Il Responsabile Protezione Dati – DPO, scelto in base alla sua professionalità giuridico-informatica ed alla competenza in materia di protezione dei dati personali, è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare ed al Responsabile del trattamento 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 e/o al delegato 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

[3] Ai sensi dell'art. 37, paragrafo 1, lett. C, GDPR, è obbligatorio nominare il DPO quando «*le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10*». Inoltre, in base al provvedimento del Garante per la Protezione dei Dati Personali del 26.03.2018, *«sono tenuti obbligatoriamente alla nomina del DPO, a titolo esemplificativo e non esaustivo, tra l'altro, istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di recupero crediti; società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione».*

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 e del Responsabile del trattamento;
c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile 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 a ogni altra questione. A tali fini il nominativo del DPO è comunicato dal Titolare al Garante;
f) altri compiti e funzioni a condizione che il Titolare del trattamento si assicuri 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 del trattamento assicura che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

a) il DPO è invitato a partecipare alle riunioni di coordinamento dei Dirigenti/Responsabili che abbiano per oggetto questioni inerenti la protezione dei dati personali;
b) 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;
c) 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;
d) il DPO deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

Fondazione SDNha deciso di nominare un DPO esterno in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39 del Reg. Ue, n. 679/2016 (GDPR). Il livello di conoscenza specialistica richiesto è stato ritenuto proporzionato alla sensibilità, complessità e quantità dei dati sottoposti a trattamento.

È stata, inoltre, ritenuta utile la conoscenza dello specifico settore di attività e della struttura organizzativa del Titolare del trattamento,nonché una buona familiarità con i sistemi informativi e le esigenze di sicurezza e protezione dati manifestate dal titolare.

Il DPO svolge un ruolo chiave nel promuovere la cultura della protezione dei dati all'interno dell'organizzazione del Titolare, e contribuisce a dare attuazione a elementi essenziali del regolamento quali i principi fondamentali del trattamento, i diritti degli interessati, la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita, i registri delle attività di trattamento, la sicurezza dei trattamenti e la notifica e comunicazione delle violazioni di dati personali.

Fondazione SDN, ha escluso l'esistenza di qualsiasi conflitto di interessi[4], valutando il complesso dei compiti assegnati al DPO–sia aventi rilevanza interna (consulenza, pareri, sorveglianza sul rispetto delle disposizioni) che esterna (cooperazione con l'autorità di controllo e contatto con gli interessati in relazione all'esercizio dei propri diritti) In merito, l'art. 38, par. 3, Reg. Ue, n. 679/2016, fissa alcune garanzie essenziali per consentire al DPO di operare con un grado sufficiente di autonomia all'interno dell'organizzazione, prevedendo che il Responsabile della Protezione dei Dati *"non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti"*.Il considerando 97, GDPR, aggiunge, poi, che i DPO *"dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente"*. Il Titolare, pertanto, garantisce che il DPO, nell'esecuzione dei compiti attribuitigli ai sensi dell'articolo 39, GDPR, non riceva istruzioni sull'approccio da seguire nel caso specifico, né riceva istruzioni sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.

4. PRINCIPI IN MATERIA DI PROTEZIONE DEI DATA PERSONALI

Al fine di agevolare il rispetto delle norme in materia di protezione di dati personali, Fondazione SDN osserva i seguenti principi:

- **liceità, correttezza e trasparenza**: i dati personali sono raccolti e trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;

[4]In base all'articolo 38, paragrafo 6, al RPD è consentito di "*svolgere altri compiti e funzioni*", ma a condizione che il titolare del trattamento o il responsabile del trattamento si assicuri 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. Anche se un RPD può svolgere altre funzioni, l'affidamento di tali ulteriori compiti e funzioni è possibile solo a condizione che essi non diano adito a conflitti di interessi. Ciò significa, in modo particolare, che un RPD non può rivestire, all'interno dell'organizzazione del titolare del trattamento o del responsabile del trattamento, un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali. Si tratta di un elemento da tenere in considerazione caso per caso guardando alla specifica struttura organizzativa del singolo titolare del trattamento o responsabile del trattamento.
A grandi linee, possono sussistere situazioni di conflitto all'interno dell'organizzazione del titolare del trattamento o del responsabile del trattamento riguardo a ruoli manageriali di vertice (amministratore delegato, responsabile operativo, responsabile finanziario, responsabile sanitario, direzione marketing, direzione risorse umane, responsabile IT), ma anche rispetto a posizioni gerarchicamente inferiori se queste ultime comportano la determinazione di finalità o mezzi del trattamento. Inoltre, può insorgere un conflitto di interessi se, per esempio, a un RPD esterno si chiede di rappresentare il titolare o il responsabile in un giudizio che tocchi problematiche di protezione dei dati. *Cfr. Guidelines on Data ProtectionOfficers (WP243 – rev. 01)*

- **limitazione della finalità**: i dati personali sono raccolti e trattati per finalità determinate, esplicite e legittime;
- **minimizzazione**: i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- **esattezza**: i dati personali sono mantenuti esatti ed aggiornati e sono adottate misure ragionevoli per cancellare o rettificare, tempestivamente, i dati inesatti o superati;
- **limitazione della conservazione** (c.d. *data retention*): i dati personali sono conservati per un arco temporale non superiore al conseguimento delle finalità per cui sono stati raccolti;
- **integrità e riservatezza**: i dati personali sono trattati in modo da garantirne un'adeguata sicurezza, attraverso l'adozione di misure tecniche ed organizzative adeguate;
- ***accountability*o responsabilizzazione**: si sostanzia nell'adozione di comportamenti proattivi e tali da dimostrare la concreta implementazione di misure tecniche ed organizzative adeguate per garantire un livello di sicurezza proporzionato al rischio;
- ***privacy by design e privacy by default***: tutti gli aspetti in materia di protezione dei dati personali vengono considerati fin dalle fasi di progettazione, implementazione e configurazione di tutte le tecnologie utilizzate per le operazioni di trattamento.

Al riguardo la Fondazione:

i. prima di intraprendere qualsiasi attività di trattamento di dati personali, valuta l'esistenza di un fondamento giuridico di liceità, verificando se ricorra uno dei presupposti di cui all' art. 6, Reg. UE. La Fondazione, dunque, tratta i dati personali comuni solo se: l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità (art. 6, par. 1, lett. a); il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso (art. 6, par. 1, lett. b); il trattamento è necessario per adempiere un obbligo legale al quale è soggetto (art. 6, par.1, lett. c); il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o diun'altra persona fisica (art. 6, par.1, lett. d);il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito (art. 6, par.1, lett. e);

ii. in relazione al trattamento di categorie particolari di dati[5], valuta l'esistenza di una delle condizioni di cui all'art. 9, par. 2, GDPR e, segnatamente tratta i dati quando *"il trattamento è necessario per finalità di medicina preventiva o di medicina dellavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza oterapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sullabase del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità"*[6].

[5] Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare data genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

[6] A seguito dell'emanazione del provvedimento n. 55 del 7 marzo 2019, *(Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario – doc. web n. 909194),* il Garante per la protezione dei dati personali ha chiarito alcuni aspetti riguardanti il trattamento dei dati relativi alla salute, con specifico riferimento ai trattamenti effettuati per finalità di cura, di cui all'art. 9, par. 2, lett. h) e par. 3 del Reg. UE 679/2016.Il Garante, in relazione ai trattamenti effettuati per "*finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali, sulla base del diritto dell'Unione/Stati membri o conformemente al contratto con un professionista della sanità, effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza"*, ha chiarito che **non**

iii. adotta processi, strumenti e controlli idonei, che consentano il pieno rispetto dei principi già menzionati;
iv. tratta solo i dati che sono essenziali per svolgere le attività, infatti, i sistemi ed i processi sono progettati per limitare la raccolta dei dati personali a ciò che è strettamente necessariogli scopi specifici del trattamento;
v. garantisce adeguati flussi informativi da e verso gli organi sociali, le strutture di controllo e operative;
vi. assicura lo svolgimento delle attività di formazione del personale in materia di protezione dei dati personali, al fine di garantire il rispetto della normativa applicabile da parte di chiunque realizzi attività di trattamento dei dati personali all'interno dell'organizzazione sotto l'autorità del titolare.

5. I DIRITTI DEGLI INTERESSATI

Il Regolamento Europeo riconosce ai soggetti cui si riferiscono i dati trattati (utenti, lavoratori, consulenti, fornitori, ecc.) taluni di diritti volti a garantire un controllo adeguato e diretto.

A tal fine,Fondazione SDN si impegna a garantire l'efficace esecuzione dei processi necessari all'esercizio dei diritti degli interessati, con particolare riferimento a:

- **Diritto di essere informato**
  In conformità ai principi di trasparenza, correttezza, limitazione delle finalità e *data retention*, la Fondazioneprevede che, ai soggetti interessati, all'atto della raccolta dei dati personali, vengano fornite chiare informazioni circa: l'identità e 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; la base giuridicadel trattamento;qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessiperseguiti;gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a unpaese terzo o a un'organizzazione internazionale e l'esistenza di garanzie adeguate.
  La Fondazione ha predisposto, in base alla categoria di soggetti interessati e alla tipologia di trattamento effettuato, specifiche informative ex artt. 13 e 14, Reg. UE.
  Tutti i dipendenti sono tenuti ad utilizzare solo ed esclusivamente le informative predisposte dal Titolare.

---

risulta più necessario richiedere il consenso del paziente. Consenso da cui può prescindersi quando il trattamento dei dati personali risulti necessario alla prestazione sanitaria richiesta.Al contrario, per gli *"eventuali trattamenti attinenti, solo in senso lato, alla cura, ma non strettamente necessari"*, è necessario ricorrere a un diverso fondamento di liceità del trattamento, che potrebbe essere anche individuato nel consenso del paziente o in un altro presupposto di liceità (artt. 6 e 9, par. 2, del Regolamento).
Richiedono, invece, il consenso esplicito dell'interessato (art. 9, par. 2, lett. a) i seguenti trattamenti:

- Trattamenti connessi all'utilizzo di App mediche;
- Trattamenti preordinati alla fidelizzazione della clientela;
- Trattamenti effettuati in campo sanitario da persone giuridiche private per finalità promozionali o commerciali;
- Trattamenti effettuati da professionisti sanitari per finalità commerciali o elettorali;
- Trattamenti effettuati attraverso il Fascicolo sanitario elettronico;
- Trattamenti effettuati attraverso il Dossier sanitario elettronico;
- Trattamenti effettuati mediante sistemi di refertazione on line.

Tutte le informative sono messe a disposizione degli interessati e risultano disponibili al pubblico presso il sito*web*di Fondazione SDN.

- **Diritto di accesso ai dati**
  La Fondazionegarantisce all'interessato il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, se è in corso tale trattamento, l'accesso ai dati e alle informazioni. L'interessato, inoltre, ha,in ogni caso,il diritto di ricevere una copia dei dati personali oggetto di trattamento.

- **Diritto di rettifica**
  L'interessato ha diritto di otteneredalla Fondazione, l'integrazione, l'aggiornamento nonché la rettifica dei Suoi dati personali senza ingiustificato ritardo. Tale diritto consiste nella possibilità di ottenere la correzione di inesattezze o l'integrazione di informazioni non complete. Il titolare s'impegna, altresì, a rendere nota la rettifica/integrazione a ciascuno dei soggetti cui ha comunicato o trasferito i dati.

- **Diritto alla cancellazione**
  Il diritto alla cancellazione consente all'interessato di ottenere, senza ingiustificato ritardo, la rimozione dei dati personali che lo riguardano, nei casi in cui ricorra una delle ipotesi previste dall'art. 17 del Reg. UE (dati personali non più necessari rispetto alle finalità per cui sono stati raccolti o trattati, revoca del consenso ed insussistenza di altro fondamento giuridico per il trattamento, dati personali trattati illecitamente, esercizio del diritto di opposizione, ecc.).

- **Diritto di limitazione del trattamento**
  Ciascun interessato ha diritto di otteneredal Titolare, la limitazione del trattamento dei dati personali, nei casi espressamente previsti dal Regolamento, ovvero quando: contesta l'esattezza dei dati, il trattamento è illecito e chiede che ne sia meramente limitato l'utilizzo, i dati sono necessari per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria o si è opposto al trattamento per motivi legittimi.
  Se il trattamento è limitato, i dati personali saranno trattati solo con il consenso esplicito dell'interessato. Fondazione SDN lo informa prima che la limitazione venga revocata.

- **Diritto alla portabilità dei dati**
  Al fine di promuovere il controllo degli interessati sui propri dati personali, la Fondazionene facilita la circolazione, la copia o la trasmissione da un ambiente informatico all'altro. All'interessato viene, dunque, garantito il diritto di ricevere, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano, nonché il diritto di trasmetterli a un altro titolare del trattamento senza impedimenti da parte della Fondazione.

- **Diritto di opposizione**
  L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento di dati personali che lo riguardano. Verrà, comunque, effettuato da Fondazione SDN un bilanciamento tra i suoi interessi ed i motivi legittimi

cogenti per procedere al trattamento (tra cui, ad esempio, accertamento, esercizio e difesa di un diritto in sede giudiziaria, ecc.).

- **Diritto di non essere sottoposto a decisioni automatizzate**
  La Fondazioneassicura agli interessati il diritto di non essere sottoposti a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che li riguardano o che incida in modo analogo significativamente sulla persona, quali il rifiuto automatico di una domanda di credito *online* o pratiche di assunzione elettronica senza interventi umani.

Fondazione SDN, in qualità di Titolare del trattamento, al fine di agevolare l'esercizio dei diritti, mette a disposizione degli interessati uno specifico modulo.

S'impegna, inoltre, a dar seguito alle richieste dell'interessato, in relazione all'esercizio dei suindicati diritti, entro il termine di 1 mese, prorogabile motivatamente, e con preavviso tempestivo, a due mesi. Nei casi in cui non sia possibile ottemperare alla richiesta dell'interessato, la Fondazione lo informa senza ritardo, entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo ad un'autorità di controllo e di proporre ricorso giurisdizionale.

6. I REGISTRI

6.1. IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Per dimostrare la conformità al Regolamento Europeo sulla protezione dei dati, la Fondazione conserva, in formato elettronico, i registri di tutte le attività di trattamento, in un formato chiaro e di facile lettura e prontamente disponibile su richiesta dell'Autorità di Controllo.

Il Registro delle attività di trattamento diFondazione SDN contiene, ai sensi dell'art. 30 del GDPR, le seguenti informazioni:

a) il nome e i dati di contatto della Fondazione, del DPO e, ove applicabile, del contitolare del trattamento e del rappresentante;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresii destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazioneinternazionale, compresa l'identificazione del paese terzo o dell'organizzazioneinternazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazionedelle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzativedi cui all'articolo 32, paragrafo 1.

Nelle ipotesi in cui la Fondazioneagisca in qualità di Responsabile del trattamento, documenta tutte le attività di trattamento svolte per conto di un titolare all'interno di un apposito Registro, il quale contiene le seguenti informazioni:

a) il nome e i dati di contatto della Fondazione, di ognititolare del trattamento per conto del quale agisce, del DPO e, ove applicabile, del proprio rappresentante o di quello del titolare del trattamento;
b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazioneinternazionale, compresa l'identificazione del paese terzo o dell'organizzazioneinternazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazionedelle garanzie adeguate;
d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzativedi cui all'articolo 32, paragrafo 1.

6.2. ALTRI REGISTRI

Oltre ai già menzionati Registri, la Fondazioneha, altresì, adottato:

- **Registro degli Asset**
  Contiene l'elenco degli strumenti, informatizzati o cartacei, del trattamento, con indicazione della relativa tipologia, localizzazione, nonché dei dati personali ivi contenuti,dei soggetti preposti al loro utilizzo ed i relativi permessi. Ulteriori informazioni di dettaglio presenti nel registro sono: la data di acquisto e smaltimento dell'asset, l'indirizzo IP, i tempi di ripristino dell'asset, il formato dei dati, le verifiche sul funzionamento sicuro dell'asset, le modalità di smaltimento dell'asset.

- **Registro delle violazioni *(data breach)***
  Indipendentemente dal fatto che una violazione debba o meno essere notificata all'autorità di controllo, Fondazione SDN, in qualità di Titolare del trattamento, conserva la documentazione di tutte le violazioni, come previstodall'articolo 33, paragrafo 5, del GDPR, al fine di consentire all'Autorità di controllo di effettuare le verifiche necessarie. Il registro documenta i dettagli relativi alla violazione, comprese le cause, i fatti, i dati personali interessati, gli effetti e le conseguenze della violazione e i provvedimenti adottati per porvi rimedio.

- **Registro delle istanze**
  La Fondazioneagevola l'esercizio dei diritti dell'interessato, ai sensi degli articoli da 15 a 22 del Regolamento e, per dimostrare ciò, documenta tutte le istanze ricevute all'interno di un registro. Il registro delle istanze contiene: il nominativo del soggetto interessato che ha avanzato una richiesta; la data di ricezione ed evasione dell'istanza; la persona autorizzata allo svolgimento delle attività esecutive ai fini dell`esercizio del diritto dell`interessato; la tipologia di istanza (accesso, rettifica, cancellazione, portabilità, limitazione, opposizione e revoca del consenso); i trattamenti di dati in relazione ai quali viene esercitato il diritto; le modalità di evasione dell'istanza.

- **Registro delle informative**
  Fondazione SDN, al fine di dimostrare che ciascun interessato è stato informato circa il trattamento dei dati personali che lo riguardano, ha predisposto il registro delle informative, contenente: il soggetto interessato a cui è stata resa l'informativa, la data, i trattamenti coinvolti ed i relativi allegati.

- **Registro dei consensi**
  L'articolo 7, paragrafo 1, del GDPR, prevede l'obbligo esplicito del titolare del trattamento di dimostrare il consenso dell'interessato. Conformemente a tale articolo, l'onere della prova èa carico del titolare del trattamento, pertanto, la Fondazione, per i trattamenti basati sul consenso dell'interessato, ha predisposto un apposito registro per dimostrare che l'interessato ha acconsentito al trattamento, dopo aver letto la relativa informativa. L'obbligo di dimostrare l'esistenza del consenso sussiste fintantoché dura l'attività di trattamento dei dati in questione. Al termine della stessa, la prova del consenso viene conservata non più di quanto strettamente necessario per adempiere ad obblighi giuridici o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Tutti i registri sono tenuti in formato elettronico.

7. LA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

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, la Fondazione, prima di effettuare il trattamento, attua una valutazione d'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 GDPR, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento.

Una valutazione d'impatto sulla protezione dei dati è, quindi, un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli. Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione di Fondazione SDN, in quanto sostengono il Titolare del trattamento non soltanto nel rispettare i requisiti del Reg. UE, N. 679/2016, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento. In altre parole, una valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità

L'obbligo per la Fondazionedi realizzare una valutazione d'impatto sulla protezione dei dati va inteso nel contesto dell'obbligo generale, cuiFondazione SDNè soggetto, di gestire adeguatamente i rischi presentati dal trattamento di dati personali. Un "rischio" è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. La "gestione dei rischi", invece, può essere definita come l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi. L'articolo 35 fa riferimento al possibile rischio elevato *"per i diritti e le libertà delle persone fisiche"*. Come indicato nella dichiarazione del WP-29 sulla protezione dei dati sul ruolo di un approccio basato sul rischio nei quadri giuridici in materia di

protezione dei dati, il riferimento a "diritti e libertà" degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la libertà di parola, la libertà di pensiero, la libertà di circolazione, il divieto di discriminazione, il diritto alla libertà di coscienza e di religione.

In linea con l'approccio basato sul rischio adottato dal Regolamento Generale sulla Protezione dei Dati, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento. Al contrario, è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento *"può presentare un rischio elevato per i diritti e le libertà delle persone fisiche"* (articolo 35, paragrafo 1, Reg. UE, 679/2016).

Una valutazione d'impatto sulla protezione dei dati può riguardare una singola operazione di trattamento dei dati. Tuttavia, l'articolo 35, paragrafo 1, indica che *"una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi"*. Il considerando 92 aggiunge che *"vi sono circostanze in cui può essere ragionevole ed economico effettuare una valutazione d'impatto sulla protezione dei dati che verta su un oggetto più ampio di un unico progetto, per esempio quando autorità pubbliche o enti pubblici intendono istituire un'applicazione o una piattaforma di trattamento comuni o quando diversi titolari del trattamento progettano di introdurre un'applicazione o un ambiente di trattamento comuni in un settore o segmento industriale o per una attività trasversale ampiamente utilizzata"*.

Fondazione SDN, quindi, effettua Valutazioni d'impatto conformi a:

- Regolamento UE 679/2016 *(Artt. 35 e 36 - Considerando 84, 89, 90, 91, 92, 93, 94, 95, 96)*;
- WP29-248 del 4 ottobre 2017 *(Linee Guida concernenti la valutazione d'impatto sulla protezione dei dati, nonché i criteri per stabilire se un trattamento possa presentare un rischio elevato ai sensi del GDPR)*;
- ISO/IEC 29134:2017 *(International Standard of Information Technology - Security Techniques - Guidelines for Privacy Impact Assessment);*
- ICO 20140235 *(Conducting Privacy Impact Assessment - Code of practice);*
- UNI CEI EN ISO/IEC 27001:2017 *(European Standard of Information Technology - Information Security Management System - Requirements).*

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 e 10 del 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 la Fondazioneritenga, motivatamente, che non può presentare un rischio elevato; la Fondazione 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 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, inoltre, monitora lo svolgimento della DPIA e redige suo parere motivato.

La pubblicazione di una valutazione d'impatto sulla protezione dei dati non è un requisito giuridico sancito dal Reg. UE, n. 679/2016, tuttavia, la Fondazioneprende in considerazione la pubblicazione di almeno alcune parti della DPIA, ad esempio di una sintesi o della conclusione della valutazione d'impatto sulla protezione dei dati.

8. TRASFERIMENTO E CONDIVISIONE DEI DATI – TRASFERIMENTI EXTRA UE

8.1. COMUNICAZIONE E DIFFUSIONE DEI DATI

Una specifica attenzione viene dedicata daFondazione SDN alle ipotesi di comunicazione o diffusione dei dati. In altri termini, ogni qual volta si prospetti l'eventualità di divulgare (in qualsiasi forma o modo) dati personali, vengono effettuate le seguenti verifiche, specie se a riguardo di categorie particolari di dati personali:

i. verifica della legittimità della divulgazione alla luce della informativa fornita all'interessato;
ii. verifica della legittimità della base giuridica di tale trattamento;

iii. verifica della presenza di strumenti giuridicamente vincolanti che consentano la comunicazione o la diffusione;
iv. verifica della presenza di misure di sicurezza, tecniche ed organizzative, che rendano sicuro il trattamento, minimizzando i rischi;
v. verifica di eventuali normative e regolamenti che consentano/rendano obbligatoria la divulgazione.

8.2. CONDIVIDERE E COMUNICARE I DATI PERSONALI

I dati personali possono essere condivisi con altre società, autorità pubbliche, agenzie governative o soggetti terzi (pubblici e/o privati) nel rispetto delle leggi vigenti e del Regolamento UE, N. 2016/679.
In caso di condivisione con soggetti terzi di dati personali di cuiFondazione SDN è Titolare, si deve ottenere la garanzia che il soggetto terzo abbia la capacità e l'intenzione di proteggere tali dati in conformità agli standard e ai principi espressi dalla presente *Policy*, dovendo presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti previsti dal Regolamento UE, N. 2016/679.
Un contratto che regoli il trasferimento, quindi, il trattamento dei dati è richiesto ogniqualvolta un soggetto terzo abbia accesso ai dati personali di cuila Fondazioneè Titolare, sia nelle ipotesi in cui debba elaborarli per conto del Titolare (in qualità di Responsabile o Sub-Responsabile *ex* art. 28, Regolamento UE, N. 679/2016), sia nelle ipotesi i cui debbano essere trattati con condivisione di finalità e/o mezzi (nelle ipotesi di Contitolarità *ex* art. 26, Reg. UE, N. 679/2016). Tutti i contratti devono comprendere i principi generali e le condizioni per il trattamento dei dati personali, così come specificati all'interno delle disposizioni normative in materia di protezione dei dati personali.

8.3. CONDIVIDERE I DATI CON SOGGETTI TERZI

Fondazione SDN deve assicurare che, in caso di condivisione di dati personali con un altro soggetto, le responsabilità di entrambe le parti riguardo la protezione delle informazioni siano formalmente documentate in un accordo o contratto scritto.
Tale contratto deve garantire che, laddove il soggetto terzo utilizzi i dati personali per le proprie finalità:

i. siano esplicitamente riportate le finalità per le quali le informazioni possono essere utilizzate dalla terza parte, con eventuali limitazioni o restrizioni sull'ulteriore utilizzo per altri scopi;
ii. il soggetto terzo fornisca una prova del proprio impegno nei confronti delTitolareper garantire il trattamento dei dati personali in modo da non contravvenire alla legislazione vigente.

Ogni nuovo trattamento che comporta la condivisione di dati personali con terze parti deve essere conforme con quanto indicato nell'informativa fornita all'interessato.

La Fondazionedeve assicurarsi inoltre di avere:

i. una base giuridica per la condivisione dei dati;
ii. di aver fornito un'adeguata comunicazione all'interessato della condivisione dei dati;
iii. di aver tenuto in considerazione il principio di limitazione delle finalità del trattamento;

iv. di aver ottenuto il consenso dell'interessato, dove previsto.

8.4. TRASFERIRE I DATI PERSONALI ALL'ESTERO (EXTRA UE)

In alcuni casi i dati personali possono essere condivisi con soggetti terzi che operano all'estero nel rispetto delle prescrizioni previste dal Regolamento UE 2016/679. Un trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, infatti, può avvenire soltanto qualora il livello di protezione dei dati garantito dal Reg. UE, N. 679/2016, non sia pregiudicato.

Qualsiasi trasferimento di dati personali verso un paese terzo o una organizzazione internazionale deve essere identificato; Fondazione SDN, pertanto, li annota nel Registro dei trattamenti *ex* art. 30, Reg. UE, N. 679/2016.

Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione dell'UE ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione, garantiscono un livello di protezione adeguato. In tali ipotesi, infatti, il trasferimento non necessita di autorizzazioni specifiche.

In mancanza di una decisione di adeguatezza adottata dalla Commissione UE, il Titolare trasferisce dati personali verso un paese terzo o una organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.
Possono costituire garanzie adeguate, senza necessitare di autorizzazioni specifiche da parte di un'Autorità di controllo:

i. uno strumento giuridicamente vincolante ed avente efficacia esecutiva tra autorità pubbliche o organismi pubblici;
ii. le norme vincolanti d'impresa (BCR);
iii. le clausole tipo di protezione dei dati adottate dalla Commissione;
iv. un codice di condotta approvato, unitamente all'impegno vincolante ed esecutivo da parte del Titolare ad applicare, nel paese terzo, le garanzie adeguate, anche per quanto riguarda i diritti degli interessati;
v. un meccanismo di certificazione approvato, unitamente all'impegno vincolante ed esecutivo da parte del Titolare ad applicare, nel paese terzo, le garanzie adeguate, anche per quanto riguarda i diritti degli interessati.

Possono costituire garanzie adeguate, fatta salva l'autorizzazione specifica da parte di un'Autorità di controllo:

i. le clausole contrattuali tra il Titolare ed il Titolare, il Responsabile o il Destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale;
ii. le disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi ed azionabili per gli interessati.

Qualora si renda necessario il trasferimento dei dati personali al di fuori dell'Unione Europea, pertanto, la Fondazionedeve garantire la protezione dei diritti e delle libertà degli interessati:

i. includendo nei contratti con le terze parti condizioni specifiche per assicurare la protezione dei dati personali;

ii. verificando la conformità rispetto ad un codice di condotta o ad un meccanismo di certificazione del soggetto terzo;

iii. mettendo in atto norme vincolanti d'impresa (BCR) nel caso in cui il trasferimento avvenga verso un'altra entità (es. del Gruppo o una controllata) che si trova al di fuori dell'Unione Europea.

9. AUDIT E MONITORAGGIO

Fondazione SDN svolgeregolarmente *audit* e attività di monitoraggio della conformità, al fine di garantire che le misure e i controlli in atto per proteggere gli interessati e i loro dati siano adeguati, efficaci e conformi in ogni momento.

Il DPO ha il compito di coadiuvare il titolare del trattamento nel valutare, collaudare, rivedere e migliorare i processi, le misure e i controlli in atto e segnalare eventuali piani di azione per il potenziamento delle attività.

Vengono frequentemente esaminatii metodi di minimizzazione dei dati, insiemealle nuove tecnologie impiegate.

Tutte le revisioni, gli *audit* e i processi di monitoraggio in corso sono registrati dalla Fondazionecon l'obiettivo di:

- Assicurare che siano in atto politiche e procedure appropriate;
- Verificare che tali politiche e procedure siano seguite da tutti gli attori coinvolti;
- Verificare l'adeguatezza e l'efficacia delle misure e dei controlli in atto;
- Rilevare violazioni o potenziali violazioni della conformità;
- Identificare i rischi e valutare le azioni di mitigazione per minimizzarli;
- Raccomandare soluzioni e piani d'azione ai vertici per migliorare la protezione degli interessati e salvaguardare i loro dati personali;
- Monitorare la conformità al Regolamento e alle altre norme sulla protezione dei dati e dimostrare di aver adottato le *best practice*.

10. FORMAZIONE

Attraverso un forte impegno e solidi controlli, la Fondazionegarantisce che tutto il personale comprenda le norme in materia di protezione dei dati e i suoi principi e, a tal uopo, fornisce formazione, supporto e valutazioni costanti per assicurare e dimostrare le proprie conoscenze, competenze e adeguatezza in merito alle specifiche funzioni. Lepolitiche di formazione e sviluppo della Fondazioneincludono: sessioni di formazione e informazione sul GDPR, test di valutazione, sessioni di supporto, accesso alle politiche e alle procedure.

11. SANZIONI

Fondazione SDN comprende i propri obblighi e responsabilità ai sensi delle norme sulla protezione dei dati edè consapevoledella gravità di eventuali violazioni ai sensi del Regolamento.

Pertanto, la Fondazione riconosce che:

a) la violazione delle disposizioni relative agli obblighidella Fondazione, in qualità di titolare e responsabile del trattamento, a normadegli articoli 8, 11, da 25 a 39, 42 e 43, è soggetta a sanzioniamministrative pecuniarie fino a 10 000 000 EUR, o al 2 % delfatturato mondiale totale annuo dell'esercizio precedente, se superiore;
b) le violazioni ai principi del trattamento, alle condizioni per il consenso, ai diritti degli interessati, ai trasferimenti di dati personali in un paese terzo o un'organizzazione internazionale o nei casi di inosservanza di un ordine dall'Autorità di Controllo, sono soggette a sanzioni amministrative pecuniarie fino a € 20.000.000 o al 4% delfatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Tutti coloro che operano presso l'organizzazione, o trattano i dati per conto diFondazione SDN, sono stati informati della gravità delle sanzioni e della loro natura proporzionata alle violazioni.

12. REVISIONE E AGGIORNAMENTO

La presente politica sulla Protezione dei Dati sarà aggiornata ogniqualvolta intervengano variazioni significative all'interno dell'organizzazione ovvero nelle ipotesi di aggiornamenti delle prescrizioni richieste dalla normativa vigente, dalle *best practice* o a seguito dei risultati delle attività di *audit.*

Sarà cura del Responsabile per la Protezione dei Dati procedere al suo riesame, alla verifica delle politiche di sicurezza complessive ed alla messa a disposizione di tutti i soggettiche trattano i dati personali di cui Fondazione SDN è Titolare del trattamento.