So.Re.Sa.
Politica per la gestione della Privacy
(Manuale Privacy)

Autore/i:	Francesco Daniele	EY Advisory S.p.A.
Rivisto Da	Helga Fineo	IBM S.p.A.
Approvato Da:	Nome e Cognome del Responsabile	So.Re.Sa. S.p.A.
Accettato Da:	Nome e Cognome del Responsabile	So.Re.Sa. S.p.A.

Storia del documento

Data	Versione	Descrizione modifiche	Autore
09/10/2020	1.0	Prima emissione	Francesco Daniele

Indice

1 Introduzioni generali al documento....4
1.2 Scopo del Documento....4
1.3 Campo di applicazione....4
1.4 Riferimenti....5
1.5 Definizioni....5
2 Le figure individuate dal GDPR....6
2.2 Titolare del Trattamento....6
2.3 Data Protection Officer....7
2.4 Autorizzato al Trattamento....8
2.5 Soggetti Esterni....8
2.5.1 Responsabili “esterni” del trattamento....8
2.5.2 Contitolari....9
3 Disposizioni Generali in Materia di Dati Personali....10
3.2 Principi Generali del Trattamento....10
3.3 Trattamento di categorie particolari di dati personali....11
4 Modalità di Gestione dei Dati Personali....12
4.2 Registro dei Trattamenti....12
4.3 Data Protection Impact Assessment....13
4.4 Informativa al Trattamento dei Dati Personali....14
4.5 Raccolta, Utilizzo e Conservazione dei Dati....14
5 Diritti dell’Interessato....17
6 Principi di Privacy by Design e Privacy by Default....19
7 Il Data Breach....20
8 Il Sistema Sanzionatorio....21
9 Documentazione in Ambito Privacy....22
9.2 Politiche in Ambito Privacy....22
9.3 Linee Guida in Ambito Privacy....22
9.4 Procedure in Ambito privacy....23

Indice delle Tabelle

Tabella 1 – Definizioni.....8

1 INTRODUZIONI GENERALI AL DOCUMENTO

La normativa Europea in merito alla protezione dei dati personali (Regolamento EU 2016/679 General Data Protection Regulation) è direttamente applicabile a tutti gli stati membri, ed uno dei principi cardine esplicato è la responsabilizzazione di ciascun Titolare del Trattamento, i cui compiti verranno ripresi nei paragrafi successivi.

Al fine di soddisfare adeguatamente i requisiti prescritti, ed evitare il rischio di trattamenti illeciti e le conseguenti sanzioni, ogni trattamento di dati personali effettuato dai Titolari, o dai soggetti designati, deve essere conforme alla normativa sopraindicata.

1.2 SCOPO DEL DOCUMENTO

Il presente documento definisce le regole generali al fine di disciplinare gli adempimenti normativi necessari in riferimento alle attività di trattamento dei dati personali effettuati dall'organizzazione e rimandando alle specifiche procedure, policy e linee guida. I contenuti descritti sono coerenti con le normative di riferimento, in ambito privacy, in particolare al Regolamento Europeo sulla Protezione dei Dati (*GDPR - Regolamento EU 2016/679 "General Data Protection Regulation"*) e al Codice in Materia di Protezione dei Dati Personali (D.Lgs 30 giugno 2003 n.196).

1.3 CAMPO DI APPLICAZIONE

Il presente documento si applica a tutte le strutture aziendali, ai dipendenti e ai collaboratori. Campo d'applicazione della procedura sono tutte quelle attività che rientrano nella definizione di trattamento di dati personali di cui alla normativa applicabile.

In particolare, ai sensi dell'art. 4 del GDPR, con l'espressione "trattamento di dati personali" s'intende "*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*", pertanto rientrano in tale definizione:

- la raccolta dei dati;
- la registrazione dei dati, ovvero il loro inserimento su supporti elettronici o in formato cartaceo;
- il processo di lavorazione che favorisca la fruibilità dei dati;
- la conservazione dei dati;
- l'adattamento o la modifica dei dati registrati in relazione a rettifiche o nuove acquisizioni;
- l'estrazione, ipotesi specifica che rientra nell'ipotesi più generale dell'elaborazione;
- la consultazione o l'uso;
- la comunicazione dei dati ad uno o più soggetti determinati, in qualunque forma;
- il raffronto o l'interconnessione, ovvero la messa in relazione di banche dati diverse e distinte fra loro al fine di compiere ulteriori processi di elaborazione, selezione, estrazione o raffronto;
- la limitazione;
- la cancellazione;
- la distruzione.

1.4 RIFERIMENTI

- Regolamento Europeo sulla Protezione dei Dati - (Regolamento EU 2016/679 "General Data Protection Regulation" – GDPR;
- D.Lgs. 30 Giugno 2003 n. 196 recante il "Codice in materia di protezione dei dati personali";
- Politiche, Policy e Linee Guida redatte in ambito Privacy il cui dettaglio è riportato nel paragrafo "Documentazione in ambito Privacy"

1.5 DEFINIZIONI

Di seguito sono riportate le definizioni utilizzate nel documento:

Termine	Descrizione
DPIA	Data Protection Impact Assessment
GDPR	General Data Protection Regulation
Privacy By Design	Tecniche di protezione dei dati personali sia al momento della determinazione dei mezzi di trattamento sia all'atto di trattamento stesso
Privacy By Default	Tecniche atte a garantire che i dati trattati sono necessari al perseguimento delle specifiche finalità per cui sono raccolti e per il periodo strettamente necessario a tale fine
DPO	Data Protection Officer
Data Breach	Violazione dei Dati Personali

Tabella 1 – Definizioni

2 LE FIGURE INDIVIDUATE DAL GDPR

2.2 TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento dei dati personali è, ai sensi dell'art. 4 del GDPR, "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*". Alla luce di tale definizione, il Titolare del trattamento, per ciascuna delle attività di trattamento effettuate nell'ambito della struttura aziendale e mappate nel registro delle attività di trattamento, è l'Azienda Ospedaliera / Azienda Sanitaria Locale (di seguito riportato come Titolare del Trattamento).

Il Titolare, quindi è la struttura nel suo complesso, agisce per mezzo del Consiglio di Amministrazione o del soggetto a cui i relativi poteri in materia di protezione di dati personali sono stati *pro tempore* attribuiti. Tuttavia, non devono essere considerati come Titolari le singole persone fisiche che amministrano la Società o che la rappresentano, quali ad esempio il Direttore Generale, il presidente e/o il legale rappresentante. Al Titolare competono le scelte di fondo in merito alla raccolta e all'utilizzazione dei dati personali, in particolare, la determinazione delle finalità e modalità del trattamento, ivi compreso il profilo della sicurezza.

L'art. 24, GDPR, stabilisce la responsabilità generale del Titolare per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il Titolare deve garantire la conformità e l'attuazione delle attività di trattamento secondo i principi indicati nel Regolamento GDPR. Tali misure di trattamento devono tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche. Inoltre, al fine di allineare con il Regolamento le azioni messe in atto, il Titolare deve adottare politiche interne e attuare misure che soddisfino i principi della protezione dei dati di default (*privacy by default*) e dalla progettazione (*privacy by design*).

Il Regolamento sancisce le regole di delega dal Titolare ad alcuni soggetti sia interni che esterni, appositamente individuati, quali *Owner* del Trattamento, individuati come Amministratori di Sistema, Referente Privacy, DPO e soggetti incaricati del Trattamento etc.

Il Titolare nomina altresì i Responsabili "esterni" del trattamento, ossia i soggetti esterni alla struttura aziendale che, nell'esecuzione di un servizio a favore del Titolare, trattano, per conto di quest'ultima, i dati personali in titolarità della stessa. Il Titolare ha la responsabilità di individuare al riguardo soggetti che presentino garanzie sufficienti per mettere in atto le prescritte misure tecniche e organizzative adeguate.

In relazione alle attività di trattamento effettuate nell'ambito della propria struttura aziendale, il Titolare è inoltre tenuto a valutare, alla luce degli artt. 37 e ss. del Regolamento, la necessità o, quantomeno, l'opportunità di procedere alla nomina di un Responsabile della Protezione dei Dati (DPO). Laddove la nomina fosse ritenuta necessaria o opportuna è compito del Titolare individuare e designare il DPO in funzione delle qualità professionali - e in particolare della conoscenza specialistica della normativa e della

prassi in materia di protezione dei dati – dimostrate dallo stesso. Il DPO può essere individuato nella persona di un soggetto interno alla organizzazione aziendale o di un soggetto esterno sulla base di apposito contratto di servizi. Il Titolare dà atto delle valutazioni in tal senso effettuate in un apposito documento.

2.3 DATA PROTECTION OFFICER

Il DPO risulta essere un supervisore indipendente a garanzia, per i soggetti interessati al Trattamento. Esso è una figura a presidio della legalità, punto di riferimento nella realtà organizzativa e per l'Authority garante della Privacy. L'art. 37, paragrafo 1 del Regolamento GDPR sancisce le modalità di designazione del DPO sia in diversi ambiti:

- in ambito *pubblico*, la nomina del DPO è sempre obbligatoria, fatta eccezione per l'autorità giurisdizionali in esercizio delle loro funzioni;
- in ambito *privato*, la nomina del DPO è obbligatoria quando il Titolare effettua trattamenti regolari e sistematici, su larga scala, o inerenti a dati relativi a condanne penali o reati (come definito dall'art. 10 del Regolamento).

L'articolo 39 del Regolamento sancisce i compiti assegnati al Responsabile della Protezione dei Dati, tra cui:

- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
- cooperare con l'autorità di controllo;
- fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

2.4 AUTORIZZATO AL TRATTAMENTO

Ai fini del trattamento dei Dati Personali è possibile definire, all'interno della struttura aziendale, i soggetti interni da autorizzare a compiere operazioni di trattamento di dati personali contenuti in banche dati elettroniche o cartacee. Tali soggetti rivestono il ruolo di "Incaricati al Trattamento" per conto del Titolare del Trattamento. Quest'ultimo provvede alla definizione di un opportuno obbligo legale di riservatezza da sottoporre ai soggetti Autorizzati al Trattamento al fine di proteggere le informazioni trattate.
L'attuale orientamento dell'Autorità Garante conferma la compatibilità di tale figura con quanto definito dal GDPR, nonostante la normativa europea non preveda formalmente tale figura/ruolo, parlando semplicemente di soggetti autorizzati al trattamento.
L' Autorizzato al Trattamento effettua operativamente le attività di trattamento dei dati personali attinenti alla propria attività lavorativa. Pertanto, ogni dipendente o collaboratore del Titolare che, per le mansioni assegnate, debba trattare dati personali, è autorizzato nell'ambito dei compiti che gli sono affidati ad accedere alle banche dati necessarie per lo svolgimento di tali mansioni.
L' Autorizzato al Trattamento è indentificato nell'ambito della propria area di competenza e deve attenersi strettamente alle istruzioni impartite dal Titolare in relazione alle specifiche finalità e modalità di utilizzo dei dati personali a cui lo stesso abbia accesso.

2.5 SOGGETTI ESTERNI

2.5.1 RESPONSABILI "ESTERNI" DEL TRATTAMENTO

Il Titolare per effetto della conclusione ed esecuzione di specifici contratti, può demandare alcuni servizi che prevedono il trattamento di dati personali in sua titolarità a soggetti esterni alla propria struttura. In tali casi, i soggetti esterni sono nominati Responsabili "esterni" del trattamento, intesi, ai sensi dell'art. 4 del GDPR, come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".
Il Responsabile "esterno" del trattamento deve essere nominato, con apposito contratto o atto giuridico.
Secondo la normativa vigente, il Responsabile "esterno" è tenuto a presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.
Il Responsabile "esterno", inoltre, non può ricorrere ad un altro Responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare. In caso di autorizzazione, il Responsabile esterno è tenuto a nominare il subfornitore Responsabile del trattamento e ad imporre allo stesso, tramite contratto o atto giuridico, i medesimi doveri in materia di protezione dei dati personali che il Titolare gli ha prescritto.
I trattamenti da parte di un Responsabile "esterno" del trattamento sono disciplinati da un contratto o da altro atto giuridico a norme del diritto dell'Unione o degli Stati membri; tale contratto tra il Titolare ed il Responsabile "esterno" del trattamento, oltre a vincolare a vicenda le due figure, deve prevedere la materia disciplinata, la durata del trattamento, la natura e le finalità del trattamento nonché il tipo di dati personali e le categorie di interessati a cui gli stessi dati si riferiscono.

2.5.2 CONTITOLARI

Ai sensi dell'art. 26 del Regolamento, allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. In tali circostanze, il Regolamento richiede che tali soggetti determinino in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi in materia di protezione dei dati personali derivanti dalla normativa applicabile, con particolare riguardo all'esercizio dei diritti dell'Interessato e le rispettive funzioni di comunicazione delle informative di cui agli artt. 13 e 14 del Regolamento, salvo che le rispettive responsabilità siano già determinate per legge.
L'accordo di riparto costituisce un obbligo per i contitolari definendo i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.
La contitolarità va ravvisata nella decisione condivisa delle finalità e dei conseguenti mezzi di trattamento tra titolati distinti.

3 DISPOSIZIONI GENERALI IN MATERIA DI DATI PERSONALI

In merito al trattamento dei dati personali, vengono messe in atto una serie disposizioni generali appositamente regolamentati dal GDPR, meglio descritti di seguito.

3.2 PRINCIPI GENERALI DEL TRATTAMENTO

Il trattamento dei dati personali deve essere effettuato nel rispetto delle norme di legge, delle disposizioni di cui alla presente Politica, nonché delle istruzioni di volta in volta impartite dal Titolare o, se del caso, dal DPO.

Le funzioni coinvolte nelle attività di raccolta, conservazione ed utilizzo di dati personali operano nel rispetto del sistema normativo interno e del sistema di poteri e responsabilità, nonché in piena conformità con tutte le leggi ed i regolamenti vigenti, ispirandosi ai seguenti principi fondamentali:

- In conformità al disposto dell'art. 5, Regolamento, i dati personali oggetto di trattamento sono:
  - trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato (principio di "liceità", "correttezza" e "trasparenza");
  - raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità (principio di "limitazione della finalità");
  - adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (principio di "minimizzazione dei dati");
  - esatti e, se necessario, aggiornati; devono pertanto essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (principio di "esattezza");
  - conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (principio di "limitazione della conservazione");
  - trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale (principio di "integrità e riservatezza");
- il Titolare è competente per il rispetto dei principi sopra elencati e deve essere in grado di dimostrarlo (principio di "responsabilizzazione" o "accountability");
- ogni trattamento dei dati personali deve svolgersi nel rispetto dei diritti e delle libertà fondamentali e della dignità dell'Interessato, con particolare riferimento alla riservatezza, all'identità personale ed al diritto alla protezione dei dati personali, in coerenza con i principi normativi previsti per il loro esercizio;
- laddove necessario collabora con l'Autorità garante per la protezione dei dati personali, anche con riferimento specifico ad eventuali casi di notifica per violazioni ovvero in relazione alla valutazione preliminare per il trattamento di taluni dati, allo scopo di garantire il pieno rispetto dei diritti dell'Interessato e di fornire tutte le informazioni necessarie all'Autorità Garante;

- ogni attività di trattamento dei dati personali deve essere avviata in maniera trasparente rendendo all'Interessato idonea informativa in merito alle finalità, tempistiche, comunicazione e diffusione del Trattamento stesso e acquisendone, in tutti i casi previsti dalla legge, il consenso in maniera formale, scritta e libera.

Si precisa inoltre che:

- il trattamento deve essere effettuato dagli Incaricati del Trattamento per gli scopi determinati nelle rispettive job descriptions (ossia in relazione alle rispettive mansioni di lavoro);
- i dati personali raccolti e/o trattati in violazione dei principi enunciati nei precedenti punti non possono essere ulteriormente oggetto di trattamento;
- i dati personali oggetto del trattamento devono essere conservati per un periodo non eccedente a quello necessario per le finalità per cui gli stessi sono stati raccolti e trattati;
- in nessun caso i dati personali possono essere utilizzati per scopi illeciti o incompatibili con i fini per i quali sono stati raccolti e registrati.

Al fine di definire meglio i principi e le regole generali di comportamento che devono ispirare tutte le attività condotte è stata predisposta una specifica politica per la "Classificazione dei trattamenti e delle informazioni".

3.3 TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI

L'articolo 9 del Regolamento definisce dati personali appartenenti a categorie particolari quei dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
Il trattamento di tali dati personali deve essere effettuato tenendo conto di ulteriori cautele e, in particolare, esclusivamente, per quanto in questa sede rileva, (i) con il consenso esplicito dell'Interessato; (ii) se necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare del trattamento o dell'Interessato in materia di diritto del lavoro, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri; (iii) se il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; (iv) se il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria.
In ogni caso, gli Incaricati del Trattamento devono assicurarsi che i dati personali di natura sensibile siano oggetto unicamente di trattamenti strettamente necessari per il perseguimento delle finalità per le quali sono raccolti. Sono inoltre implementati mezzi idonei a prevenire la conoscenza da parte di soggetti non autorizzati.

4 MODALITÀ DI GESTIONE DEI DATI PERSONALI

In merito alla protezione dei dati personali, in linea con quanto definito dal Regolamento GDPR e dalle normative Nazionali in riferimento alla protezione dei dati, sono attuati una serie di macro-processi descritti di seguito.

4.2 REGISTRO DEI TRATTAMENTI

Il GDPR impone ai Titolari e ai Responsabili del Trattamento, con limitate eccezioni, di tenere un Registro delle attività di trattamento svolte sotto la propria responsabilità (il "Registro").
Ai sensi dell'articolo 30 del Regolamento, il quale recita *"Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità"*, il Registro deve contenere, almeno, le seguenti informazioni:

- il nome ed i dati di contatto del Titolare del trattamento e, ove applicabile, del Contitolare del Trattamento, nonché del DPO e del rappresentante del Titolare;
- le finalità del trattamento;
- una descrizione delle categorie di Interessati e delle categorie di dati personali trattati;
- le categorie di terzi/destinatari a cui i dati personali sono stati o saranno comunicati;
- eventuali trasferimenti di dati personali verso un paese terzo o organizzazioni internazionali;
- i termini ultimi previsti per la cancellazione delle diverse categorie di dati personali;
- una descrizione generale delle misure di sicurezza tecniche ed organizzative adottate.

Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

- il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e del responsabile della protezione dei dati;
- i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale;
- le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- una descrizione generale delle misure di sicurezza tecniche e organizzative

I registri sono tenuti in forma scritta, anche in formato elettronico e su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.
In conformità a quanto previsto dal Regolamento, è stato predisposto un registro delle attività di trattamento effettuate in qualità di Titolare.
Il Registro è stato redatto nella forma di fogli excel nei quali ad ogni "riga" corrisponde una attività di trattamento e a ogni colonna corrisponde una delle informazioni richieste a norma del Regolamento.

Al fine di definire le regole di riferimento finalizzate ad assicurare il rispetto di leggi, regolamenti o normative di riferimento è stata predisposta una specifica Linea Guida in merito alla *"Gestione del Registro dei Trattamenti".*

4.3 DATA PROTECTION IMPACT ASSESSMENT

Il Regolamento ha introdotto l'obbligo per il Titolare del trattamento di eseguire, al ricorrere di determinate condizioni, una valutazione d'impatto sulla protezione dei dati (*DPIA - Data Protection Impact Assessment*).
Ai sensi dell'art. 35 del Regolamento, è previsto in capo al Titolare l'onere di procedere ad una valutazione d'impatto sulla protezione dei dati personali *"quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche".*
Nello specifico, lo svolgimento della DPIA è in particolare richiesto nei seguenti casi:

- valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basato su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- trattamento su larga scala di Dati sensibili o Dati giudiziari;
- sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

La valutazione d'impatto sulla protezione dei dati personali risponde al principio di accountability, in quanto permette al Titolare di valutare e dimostrare di aver adottato le misure idonee a garantire il rispetto delle prescrizioni dettate dal Regolamento relativamente alla gestione dei rischi per i diritti e le libertà delle persone fisiche interessate. In particolare, la DPIA ha lo scopo di valutare, in ottica prudenziale, la probabilità e la gravità dei rischi connessi a un'attività di trattamento per i diritti e le libertà degli interessati, con lo scopo di individuare le misure di sicurezza, sia tecniche sia organizzative, necessarie a garantire un livello di sicurezza adeguato al rischio identificato, assicurando al contempo la protezione dei dati personali trattati.
Per tali ragioni, la valutazione deve essere effettuata prima di procedere al trattamento.
Il Regolamento riconosce tuttavia la possibilità per il Titolare di svolgere una singola valutazione al fine di esaminare un insieme di trattamenti simili che presentato rischi elevati analoghi.
L'adempimento dell'obbligo di DPIA è in carico al Titolare, nello specifico, la valutazione circa la necessità o quantomeno l'opportunità di provvedere o meno allo svolgimento di una DPIA deve essere condotta, ogniqualvolta sia implementato un nuovo servizio, sia impiegata una nuova tecnologia nell'ambito di attività di trattamento già effettuate, ovvero siano effettuate nuove attività di trattamento.
Laddove risultasse necessario o quantomeno opportuno procedere con la DPIA, tale valutazione deve contenere:

- una descrizione sistematica dei trattamenti previsti e delle rispettive finalità, nonché, ove applicabile, l'eventuale interesse legittimo del Titolare;
- una valutazione sulla necessità e proporzionalità dei trattamenti in relazione alle finalità;

- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare tali rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento.

Qualora dall'esito del processo di DPIA risultasse che il trattamento, nonostante le contromisure di sicurezza identificate, presenti un rischio alto e/o comunque rilevante per i diritti e le libertà delle persone fisiche, il Titolare del Trattamento è tenuto a consultare l'Autorità di controllo che provvederà a fornire un proprio parere in merito.
Inoltre, si precisa che la violazione delle norme in materia di DPIA comporta rilevanti conseguenze. In particolare, l'inosservanza delle disposizioni in merito alla può comportare sanzioni amministrative pecuniarie.
Al fine di definire le regole di riferimento finalizzate ad assicurare il rispetto di leggi, regolamenti o normative di riferimento è stata predisposta una specifica Linea Guida in merito alla *"Conduzione delle attività di Data Protection Impact Assessment".*

4.4 INFORMATIVA AL TRATTAMENTO DEI DATI PERSONALI

Il Titolare, prima di procedere a qualsiasi attività di trattamento, è tenuto obbligatoriamente a fornire apposita informativa agli Interessati in merito ai loro diritti e alle caratteristiche del trattamento in particolare per ciò che concerne le finalità e le modalità del trattamento dei dati stessi, in accordo a quanto previsto dalle disposizioni di legge in materia.
L'obbligo di fornire l'informativa all'Interessato risponde alla necessità di riconoscere a quest'ultimo il diritto di avere conoscenza dell'ambito di circolazione dei propri dati, al fine di poter procedere ad un consapevole esercizio dei poteri allo stesso riconosciuti (i.e. esprimere o negare il consenso, opporsi al trattamento, esercitare i propri diritti).

4.5 RACCOLTA, UTILIZZO E CONSERVAZIONE DEI DATI

Il Titolare, prima di procedere alla raccolta dei dati presso l'interessato di dati che lo riguardano, fornisce all'interessato le seguenti informazioni:

- l'identità e i dati di contatto del titolare del trattamento e del suo rappresentante;
- 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;
- qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

- l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione

Il titolare, in ottemperanza ai principi del Regolamento GDPR, stabilisce i termini per la conservazione dei dati personali al fine di assicurare che gli stessi non siano mantenuti per un periodo superiore a quello necessario per il conseguimento delle finalità per le quali il dato è trattato o ai tempi previsti per l'esecuzione di obblighi di legge.

In particolare, considerando:

- l'art. 39 del Regolamento, il quale illustra *"l'obbligo di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica".*

- L'art. 65 del Regolamento prevede che *"Tuttavia, dovrebbe essere lecita l'ulteriore conservazione dei dati personali qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria"*

- L'art. 5, paragrafo 1, lettera e) stabilisce che i dati personali sono *"conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»)".*

- L'art. 13, paragrafo 2 stabilisce che *"nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente: a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo".*

Pertanto, deve essere garantita l'adozione di misure tecnico - organizzative necessarie affinché i dati personali siano conservati per un periodo di tempo adeguato alle finalità e alle richieste dell'Interessato. A tal file, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il diritto di proporre reclamo a un'autorità di controllo;
- 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;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

5 DIRITTI DELL'INTERESSATO

Il titolare del trattamento garantisce l'esercizio dei diritti dell'interessato come previsto dal Regolamento, attraverso un processo di gestione delle richieste effettuate dagli interessati con riferimento ai seguenti diritti:

- **ricevere un'informativa** contenente tutti gli elementi indicati negli articoli 13 e 14, GDPR sia nel caso in cui i dati siano forniti direttamente dall'Interessato stesso al Titolare che nel caso in cui questi siano ottenuti da terzi (artt. 13 e 14, GDPR);
- **revocare**, in qualsiasi momento, il **consenso**, senza alcun condizionamento e con la stessa facilità con cui è stato prestato (art. 7, GDPR);
- **accesso**, consistente nella facoltà di ottenere dal Titolare la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso a tali dati – compresa una copia degli stessi – ed alle informazioni elencate all'articolo 15, GDPR (art. 15, GDPR);
- **rettifica**, consistente nella possibilità di ottenere dal Titolare la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo e/o l'integrazione dei dati personali incompleti (art. 16, GDPR);
- **cancellazione** (c.d. **diritto all'oblio**), consistente nella facoltà di ottenere dal Titolare la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo nel rispetto delle condizioni del GDPR (art. 17, GDPR);
- **limitazione del trattamento**, consistente nella possibilità di ottenere dal Titolare la limitazione (temporanea) del trattamento al ricorrere di una delle ipotesi elencate dall'articolo 18, GDPR e salve le deroghe ivi previste (art. 18, GDPR);
- ottenere la **comunicazione** da parte del Titolare a ciascuno dei destinatari cui sono trasmessi i dati personali dell'interessato, di eventuali rettifiche, cancellazioni o limitazioni del trattamento, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato per il titolare. Inoltre, l'interessato ha diritto di ottenere la comunicazione di tali destinatari (art. 19, GDPR)
- **portabilità dei dati**, consistente nella facoltà – nei soli casi in cui il trattamento si basa sul consenso o su un contratto ed è effettuato con mezzi automatizzati – di ricevere dal Titolare del trattamento, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano forniti dall'Interessato stesso. Inoltre, qualora tecnicamente possibile, il diritto alla portabilità dei dati consente di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro (art. 20, GDPR);
- **opposizione**, consistente nel diritto di opporsi, alle condizioni e nel rispetto dei limiti previsti dal GDPR, al trattamento dei dati personali che lo riguardano qualora il trattamento degli stessi fosse: (i) necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri; (ii) fondato sull'interesse legittimo del titolare; (iii) finalizzato ad attività di marketing diretto svolte sulla base del legittimo interesse del Titolare; (iv) finalizzato alla ricerca scientifica o storica o con fini statistici (art. 21, GDPR);
- non essere sottoposto a una decisione basata unicamente sul **trattamento automatizzato**, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona, salvo la decisione (i) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'Interessato e il Titolare; (ii) sia autorizzata dal diritto dell'Unione

Europea e/o dalla legge nazionale cui è sottoposto il Titolare; ovvero (iii) si basi sul consenso esplicito dell'Interessato (art. 22, GDPR).

In ogni caso, l'articolo 12, GDPR, prevede che tutte le informazioni ed i riscontri debbano essere forniti all'interessato con le seguenti modalità:

- in una forma concisa, trasparente, intelligibile e con un linguaggio semplice e chiaro;
- per iscritto, o con mezzi elettronici se la richiesta è stata effettuata con mezzi elettronici. Una risposta orale è consentita solo su domanda espressa dall'interessato;
- senza ingiustificato ritardo e, al più tardi, entro un mese dal ricevimento della richiesta, salva la possibilità di prorogare tale termine di due mesi nei particolari casi previsti e fermo restando l'obbligo di informare comunque l'interessato del ritardo e dei motivi entro un mese dal ricevimento della richiesta. In ogni caso, se non è possibile soddisfare la richiesta entro un mese dal suo ricevimento, è necessario informare l'interessato (i) che non sarà possibile soddisfare la sua richiesta entro tale termine, (ii) sui motivi della proroga e (iii) sulla possibilità di proporre reclamo ad un'autorità di controllo e ricorso giurisdizionale;
- gratuitamente. Può essere addebitato un contributo ragionevole, o negata la soddisfazione della richiesta, solo nel caso di richieste manifestamente infondate o eccessive, anche per la loro ripetitività;
- dopo aver verificato l'identità dell'interessato, eventualmente anche domandando informazioni aggiuntive a quelle già raccolte.

In considerazione di quanto sopra, il Titolare ha adottato misure tecniche ed organizzative, al fine di ottemperare all'obbligo di dare seguito alle richieste degli Interessati relativamente all'esercizio dei diritti loro riconosciuti dal GDPR.
Al fine di definire meglio i principi e le regole generali di comportamento che devono ispirare tutte le attività condotte è stata predisposta una specifica politica per la *"Gestione dei diritti dell'interessato"* e la relativa *"Procedura per la gestione dei diritti dell'interessato"*.

6 PRINCIPI DI PRIVACY BY DESIGN E PRIVACY BY DEFAULT

L'articolo 25 del Regolamento GDPR, pone l'obbligo al Titolare del Trattamento di mettere in atto le seguenti misure tecniche ed organizzative adeguate a:

- proteggere i dati personali sia al momento della determinazione dei mezzi di trattamento sia all'atto di trattamento stesso i.e. principio di "Privacy by Design";
- garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari al perseguimento delle specifiche finalità per cui sono raccolti e per il periodo strettamente necessario a tale fine i.e. principio di "Privacy by Default";

I principi trasversali di Privacy by Design and by Default hanno l'obiettivo di definire le logiche di protezione dei dati personali, attraverso l'individuazione dei potenziali rischi di non conformità in materia di privacy e delle conseguenti misure tecniche-organizzative per la riduzione degli stessi sin dalla fase di progettazione e lungo tutto il ciclo di vita del trattamento dei dati.

Privacy by Design

La Privacy by Design trova fondamento nell'obbligo, in capo al Titolare del Trattamento, di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti previsti dal Regolamento a tutela dei diritti degli interessati al trattamento. Il titolare dovrà tenere conto del contesto complessivo ove il trasferimento si colloca e dei rischi per i diritti e le libertà dei soggetti interessati al trattamento.

Privacy by Default

La Privacy by Default trova fondamento nell'obbligo, in capo al Titolare/ Delegato al Trattamento, di adottare misure tecniche-organizzative adeguate a garantire l'applicazione dei principi di protezione dei dati come impostazione di default. Tale attività ha l'obiettivo di definire le azioni da intraprendere al fine di assicurare che vengano trattati solo i dati personali necessari al perseguimento delle specifiche finalità del trattamento.

7 IL DATA BREACH

Il GDPR definisce Data Breach "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".

Eventi di Data Breach possono riguardare sia la diffusione di dati relativi a un singolo individuo, che casi più critici di furto o perdita di intere basi dati, quali, a titolo esemplificativo, l'anagrafica dei clienti del Titolare, o le informazioni relative ai dipendenti.

Il Regolamento prevede che, nel caso in cui una organizzazione rilevi una violazione dei Dati personali trattati (c.d. *Data Breach*), la stessa:

- sia tenuta a informare l'Autorità di controllo (i.e., Garante Privacy, come sopra definita, nel caso dell'Italia) entro e non oltre le 72 ore successive all'avvenuta conoscenza della violazione – a meno che sia del tutto improbabile che la violazione dei Dati personali presenti un rischio per i diritti e le libertà degli Interessati

- nel caso in cui tale violazione sia suscettibile di comportare un rischio elevato per i diritti e le libertà degli interessati, debba informare senza ritardo anche gli Interessati stessi.

Al fine di adempiere alle indicazioni del Regolamento, è altresì importante che tutti coloro che nell'ambito della propria attività quotidiana trattano Dati personali partecipino attivamente a tale processo, segnalando tempestivamente ogni caso di violazione di cui siano venuti a conoscenza e ogni evento che potrebbe potenzialmente condurre ad una violazione.

Al fine di definire le regole di riferimento finalizzate ad assicurare il rispetto di leggi, regolamenti o normative di riferimento è stata predisposta una specifica Linea Guida per la *"Gestione delle Violazioni della Sicurezza dei Dati Personali (data breach)"* e la relativa "*Procedura per la gestione del data breach"*

8 IL SISTEMA SANZIONATORIO

La riforma globale del contesto normativo sulla protezione dei dati personali introdotta dal Regolamento prevede, tra i propri pilastri fondamentali, un rafforzamento dei poteri destinati a far rispettare le disposizioni previste in materia.

Il Titolare del Trattamento ha pertanto maggiori responsabilità rispetto al passato nel garantire l'efficace tutela dei Dati personali delle persone fisiche. Allo stesso tempo, le Autorità di controllo, e tra queste, per quanto maggiormente rilevante ai fini della Procedura, l'Autorità Garante come sopra definita, sono dotate dei poteri necessari per garantire che i principi del Regolamento e i diritti delle persone interessate siano rispettati conformemente al dettato e alla ratio del Regolamento.

Nello specifico, il Regolamento inasprisce significativamente le sanzioni a carico di chi dovesse violare il dettato normativo e i diritti e le libertà degli Interessati come previsti e garantiti dal Regolamento stesso, portandole, a seconda della gravità della violazione posta in essere, sino ad un massimo di € 10.000.000 o fino al 2% del fatturato mondiale annuo del gruppo riferito all'anno precedente, se superiore, ovvero sino a un massimo di € 20.000.000 o al 4% del fatturato mondiale annuo del Gruppo dell'anno precedente, ove superiore.

Il Regolamento prevede inoltre che gli Stati membri dovrebbero poter stabilire disposizioni relative a sanzioni penali in caso di violazioni del Regolamento, comprese violazioni di norme nazionali adottate in virtù ed entro i limiti del Regolamento. Tali sanzioni penali possono altresì autorizzare la sottrazione dei profitti ottenuti attraverso violazioni del Regolamento. A riguardo si rileva che, a livello nazionale, specifiche sanzioni di carattere penale in caso di violazioni del Regolamento sono espressamente previste nello schema di decreto legislativo di coordinamento della normativa nazionale alle novità legislative introdotte a livello europeo e attualmente al vaglio delle commissioni parlamentari.

Alla luce di quanto sopra, tutte le funzioni aziendali sono tenute a cooperare con il Titolare affinché sia garantito il rispetto delle disposizioni del Regolamento e dei diritti e libertà riconosciuti all'Interessato alla luce dell'innovato contesto normativo. A tal fine, a ciascuna funzione aziendale, ed in particolare, a ciascun Responsabile di funzione o Autorizzato al Trattamento è richiesto di rispettare pedissequamente e di porre in essere quanto previsto all'interno della presente politica e in tutte le procedure ad essa correlata.

9 DOCUMENTAZIONE IN AMBITO PRIVACY

Al fine di attuare ed integrare i concetti descritti nel presente manuale si rimanda a tutta la documentazione Aziendale nell'ambito della quale vengono regolamentati nel dettaglio i comportamenti secondo le norme di riferimento. A tale scopo, nei paragrafi successivi, saranno riportate le Procedure, le Politiche e le Linee Guida da seguire che hanno impatto in ambito Privacy per garantire una compliance al GDPR.

9.2 POLITICHE IN AMBITO PRIVACY

Per definire meglio i principi e le regole generali di comportamento che devono ispirare tutte le attività condotte, al fine di garantire i principi espressi nel presente documento, si rimanda ai concetti esplicati nelle Policy in ambito privacy elencate di seguito:

- Politica per la gestione dei diritti dell'interessato
- Politica per la classificazione dei trattamenti e delle informazioni
- Politica per la gestione delle utenze preposte al trattamento dei dati personali
- Politica per la gestione degli amministratori di sistema
- Politica per la cancellazione sicura e lo smaltimento dei supporti elettronici
- Politica per la gestione e la conservazione dei log
- Politica per la definizione dei requisiti di sicurezza per le terze parti
- Politica per il corretto utilizzo delle risorse informative aziendali
- Politica per gli Amministratori di Sistema

9.3 LINEE GUIDA IN AMBITO PRIVACY

Per definire le regole di riferimento finalizzate ad assicurare il rispetto di leggi, regolamenti o normative di riferimento, si rimanda ai concetti espressi nelle Linee Guida, in ambito privacy, elencate di seguito:

- Linee Guida per la gestione del registro dei trattamenti;
- Linee Guida per la conduzione delle attività di Data Protection Impact Assessment;
- Linee Guida per le verifiche di conformità e adeguatezza
- Linee Guida per la tutela della privacy e la gestione della sicurezza nei servizi applicativi informatizzati
- Linee Guida classificazione informazioni e trattamenti
- Linee Guida per la Gestione delle Violazioni della Sicurezza dei Dati Personali (data breach)

- Linee guida per la conduzione delle verifiche di conformità e adeguatezza delle misure preposte alla tutela dei dati personali
- Linea guida per l'analisi periodica dell'integrità dei dati personali
- Linea guida per la gestione degli incidenti di sicurezza
- Linea guida continuità operativa dei sistemi e delle informazioni
- Linee guida per il censimento e la gestione dell'inventario degli asset
- Linee guida sull'uso della crittografia, pseudonimizzazione e/o anonimizzazione dei dati personali
- Linee guida per il censimento e la gestione dell'inventario degli asset

9.4 PROCEDURE IN AMBITO PRIVACY

I documenti Procedurali definiscono le modalità di svolgimento delle attività che compongono i processi, in conformità alle normative di riferimento applicabili, individuando compiti, responsabilità e modalità di gestione. Di seguito sono elencate le Procedure, in ambito Privacy, di riferimento:

- Procedura per la gestione dei diritti dell'Interessato
- Procedura per la gestione del data breach
- Procedura per la gestione delle utenze del personale interno ed esterno
- Procedura per gestione delle utenze amministrative
- Procedura di gestione degli aggiornamenti di sicurezza (patch management)
- Procedura per la gestione delle configurazioni di sicurezza dei sistemi (change e configuration management)
- Procedura per l'esecuzione dei test di sicurezza funzionali al rilascio in esercizio dei sistemi/applicativi
- Procedura di back up e restore dei sistemi
- Procedura per l'accesso fisico ai Data Center
- Procedura per l'accesso fisico ai locali ove sono trattati i dati personali ed agli archivi contenenti dati personali