PRIVACY E SICUREZZA

IL NUOVO GDPR

Definizione degli aspetti organizzativi e funzionali per la gestione della Privacy ai fini dell'adeguamento dell'organizzazione aziendale al Regolamento Europeo 2016/679

INDICE

Premessa

1. - Modello di *governance* e piano di adeguamento: *Data Inventory*

1.1 – Il Registro dei trattamenti (*ex* art. 30 del GDPR)

1.1.1 – Contenuti del Registro

1.1.2 – Categorie di dati personali

1.1.3 – Categorie dei trattamenti

1.1.4 - Tenuta e aggiornamento del Registro

1.2 – Inventario degli *asset* tecnologici

2. – Modello di *governance* e piano di adeguamento: Analisi dei rischi e degli impatti

2.1 – Analisi preliminare del rischio

2.1.1 – Analisi del rischio: rischio inerente e rischio residuo

2.1.2 – Analisi del rischio: profili tecnici

2.2 – Ambito di applicazione della Valutazione di Impatto (DPIA)

2.2.1 – Come effettuare una DPIA: approccio metodologico

3. – Modello di *governance* e piano di adeguamento: Misure organizzative

3.1 – Titolare del trattamento

3.2 – Titolare e Contitolare

3.3 – Il Responsabile del trattamento

3.4 – Il Responsabile della Protezione dei Dati (DPO) *ex* artt. 37-39 del GDPR

3.5 – Incaricati del trattamento

3.6 – Altre figure del modello di *Data Protection Governance* aziendale

3.7 – Informative e consenso

3.7.1 – Informativa *ex* art.13 del GDPR

3.7.2 – Consenso al trattamento dei dati personali

3.8 – I diritti dell'interessato

3.9 – Sistema documentale per la *Data Protection*

3.9.1 – Strutturazione e aggiornamento del sistema documentale *Privacy* – modalità di gestione

3.10 – Attività di monitoraggio

3.11 – *Data Breach* ex art. 33 del GDPR

3.11.1 – Processo di *Data Breach Management*

3.11.2 – Comunicazioni al soggetto interessato

4. – Modello di *governance e* piano di adeguamento: Misure tecniche e applicative

4.1 – Identità e accesso

Allegato

Tabella "Piano di *governance* delle attività finalizzate all'adeguamento dell'organizzazione aziendale al Regolamento Europeo 2016/679 (GDPR) in materia di protezione dei dati personali"

Premessa

Il Regolamento Europeo 2016/679 sulla protezione dei dati personali (di seguito denominato GDPR) è entrato in vigore il 24 maggio 2016 e divenuto direttamente applicabile dal 25 maggio 2018 (termine ultimo di adeguamento), abrogando la Direttiva 95/46/CE.

Il GDPR rivisita completamente la prospettiva della disciplina sulla *privacy*, istituendo un quadro normativo incentrato sui doveri e la responsabilizzazione del Titolare del trattamento (principio di "*accountability*"). La nuova disciplina impone a tale soggetto di garantire il rispetto dei principi in essa contenuti e al contempo di essere in grado di comprovarlo; ciò adottando una serie di strumenti che lo stesso GDPR indica, partendo da un'attenta valutazione di rischi e impatti e con una pianificazione di attività tali da poter incidere significativamente sotto il profilo culturale, organizzativo e tecnologico.

Il concetto di **"responsabilizzazione"** si traduce nel fatto che il Titolare è chiamato a dimostrare che i trattamenti sono coerenti con il disposto del GDPR, a pianificare e mettere in atto misure tecniche e organizzative per poterne comprovare l'adeguatezza e ad attivare un modello di monitoraggio delle misure tecnico-organizzative implementate.

In questa logica vengono introdotti due presupposti chiave dell'impianto del GDPR: la **Privacy by design,** quindi la necessità di disegnare le misure di Sicurezza e Privacy già in fase di progettazione dei sistemi informativi, e la **Privacy by default** vale a dire la capacità di disegnare le misure di Sicurezza e Privacy per *default*, come prerequisito di normale funzionamento dei sistemi informativi aziendali (art. 25).

Inoltre, all'art. 5, vengono ribaditi i principi di **liceità del trattamento** che può essere possibile solo se l'Interessato ha espresso un esplicito consenso (che il Titolare deve dimostrare di aver acquisito, art.7), di **adeguatezza, pertinenza e non eccedenza dei dati** rispetto alle finalità per cui vengono trattati.

Sempre ai sensi dell'art. 5 del GDPR **liceità, correttezza e trasparenza** sono i principi a cui deve ispirarsi ogni operazione di trattamento di dati personali effettuata da Titolari e Responsabili del trattamento, i quali sono chiamati a rispondere della loro eventuale violazione.

I dati personali devono essere:

- raccolti per finalità determinate, esplicite e legittime (**limitazione delle finalità**);
- adeguati, pertinenti e limitati a quanto necessario per le finalità dichiarate e il loro trattamento deve essere sempre coerente con le medesime finalità (**minimizzazione dei dati**);
- esatti e, quando necessario, aggiornati, anche per mezzo dell'adozione di misure idonee a cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (**esattezza**);
- conservati in una forma che consenta l'identificazione degli individui per un periodo di tempo non eccedente il conseguimento delle finalità per le quali sono trattati. Possono essere conservati per periodi più lunghi se sono trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta

salva l'attuazione di misure tecniche e organizzative adeguate per tutelare i diritti e le libertà degli individui (**limitazione della conservazione**);

- trattati in maniera da garantire, con misure tecniche e organizzative apposite, la loro sicurezza e un adeguato livello di protezione nei confronti di trattamenti non autorizzati o illeciti, di eventuali perdite o di distruzione di informazioni e/o possibili danni accidentali (**integrità e riservatezza**).

Il rispetto dei suddetti principi impone al Titolare del trattamento, tra l'altro, l'adozione di comportamenti corretti e rispettosi delle norme e l'utilizzo di modalità di comunicazione chiare per tutta la durata delle operazioni di trattamento, fin dal momento della raccolta dei dati.
Le informazioni e le comunicazioni, fornite con un linguaggio semplice e chiaro, devono essere messe a disposizione di tutti i soggetti coinvolti nei processi di trattamento, inclusi coloro che svolgono operazioni di trattamento di dati personali per conto del Titolare del trattamento (quali ad esempio dipendenti, collaboratori o terze parti). La diffusione della cultura della protezione dei dati personali aumenta il livello di consapevolezza dell'organizzazione che opera e permette a tutti gli attori coinvolti nel processo di agire in modo informato, migliorando i comportamenti e, quindi, riducendo i rischi.
Il comma 2 dell'articolo 5 del GDPR stabilisce che "Il Titolare del trattamento è competente" per il rispetto dei principi applicabili al trattamento dei dati personali e, soprattutto, che lo stesso deve essere in grado di comprovarlo. Si tratta di un richiamo fondamentale in quanto l'assolvimento degli obblighi in capo a coloro che effettuano il trattamento di dati personali è in qualche modo basato sul principio di responsabilizzazione. In tal senso, tutti coloro che effettuano trattamenti di dati personali sono tenuti a dimostrare, fornendo l'evidenza delle scelte effettuate e delle azioni intraprese, di aver svolto i propri compiti in modo lecito, corretto e trasparente nel rispetto di tutti i principi richiamati nell'articolo 5 della norma.
Successivamente alla enunciazione dei principi chiave, una attenzione particolare viene dedicata ai Diritti dell'interessato disciplinati in un apposito Capo del GDPR (Capo III):

- ***Informativa sul trattamento*** (art.12) laddove si evidenzia che deve essere fatta in forma concisa, trasparente, intellegibile e facilmente comprensibile e laddove si pone attenzione alla necessità di fornire precise indicazioni (art.13) sulla finalità del trattamento, gli eventuali destinatari/utilizzatori dei dati, il periodo di conservazione dei dati, le modalità per richiedere rettifica o cancellazione degli stessi;
- ***Accesso*** ai dati da parte dell'interessato (art.15) che prevede al comma 3 la possibilità dell'interessato di ricevere copia dei dati trattati;
- ***Rettifica e cancellazione dei dati*****:** diritto di rettifica (art.16), di cancellazione c.d. diritto all'oblio (art.17) e di limitazione del trattamento (art.18) con obbligo di notifica all'interessato in caso di rettifica, cancellazione o limitazione (art.19);
- ***Portabilità dei dati*****:** l'interessato ha il diritto di ricevere in formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano e ha il diritto di trasmettere questi dati ad altro Titolare (art.20);

- **Diritto di opposizione:** diritto dell'interessato di opporsi al trattamento dei dati che lo riguardano in qualsiasi momento (art. 21) e diritto di non essere sottoposto a un processo decisionale automatizzato, compresa la profilazione (art.22).

Il modello di *governance* e di gestione delle azioni da realizzare a livello aziendale - ai fini del conseguimento della *compliance* dell'organizzazione al GDPR stesso - contempla le seguenti quattro aree di intervento in termini di attività:

1. ***DATA INVENTORY***
2. **ANALISI DEI RISCHI E DEGLI IMPATTI**
3. **MISURE ORGANIZZATIVE**
4. **MISURE TECNICHE ED APPLICATIVE**

Al riguardo, si evidenzia che le diverse misure/azioni previste dalle richiamate aree di intervento sono state identificate con uno specifico "codice misura" e conseguentemente ricondotte nella tabella "Piano di *governance* delle attività finalizzate all'adeguamento dell'organizzazione aziendale al Regolamento Europeo 2016/679 (GDPR) in materia di protezione dei dati personali", allegata al presente documento.

Preliminarmente alla trattazione del modello di *governance* delle azioni da attuare in materia di protezione dei dati personali, nell'ambito della presente premessa appare, altresì, utile fornire breve cenno in ordine alla rappresentazione del contesto organizzativo aziendale.
L'Azienda ospedaliera "Ospedali Riuniti Marche Nord" si articola in due Presidi Ospedalieri:
- Presidio Ospedaliero "San Salvatore": stabilimenti ospedalieri in Pesaro - P.le Cinelli, 4 e Via Lombroso,1;
- Presidio Ospedaliero "Santa Croce": stabilimento ospedaliero in Fano - Via Vittorio Veneto, 2.
La sede legale dell'Azienda è in Pesaro, P.le Cinelli 4.
Il Legale rappresentante dell'Azienda è il Direttore Generale *pro tempore*.
L'Azienda ospedaliera "Marche Nord" è parte della rete dei servizi sanitari e ospedalieri della Regione Marche e costituisce centro di riferimento per la diagnosi e la cura dei pazienti che necessitano di trattamenti di alta specializzazione.
L'Azienda ospedaliera si è dotata dell'Atto Aziendale (ai sensi dell'art. 5 della l.r.13/2003 e ss.mm.ii. ed in coerenza alle linee di indirizzo di cui alla Deliberazione di Giunta Regione Marche n. 406/2010) e i riferimenti normativi su organizzazione ed attività, gli atti generali (anche di natura regolamentare) che dispongono sull'organizzazione, sulle funzioni, sui procedimenti nonché i documenti di programmazione strategico-gestionale (ivi compreso il Piano Triennale di Prevenzione della Corruzione e della Trasparenza) sono tutti pubblicati sul sito *web* aziendale nell'ambito della Sezione "Amministrazione Trasparente".

L’organizzazione dipartimentale è il modello ordinario di gestione operativa di tutte le attività dell’Azienda Ospedaliera. Il Dipartimento è struttura di coordinamento aziendale, sovraordinata alle Unità operative per gli aspetti gestionali o funzionali, costituita da strutture omogenee interdipendenti, affini o complementari, che perseguono comuni finalità pur mantenendo propria autonomia e responsabilità in ordine agli aspetti clinico - assistenziali, ovvero, tecnico - amministrativi.
L’assetto organizzativo dei Dipartimenti "Sanitari", del Dipartimento "Amministrativo”, nonché di Staff alla Direzione Aziendale è quello risultante dall’Atto Aziendale cui si fa espresso rinvio, pubblicato nel sito *web* aziendale - Sezione “Amministrazione Trasparente”.

Si precisa, infine, che il presente documento è, comunque, suscettibile di modifiche/integrazioni che dovessero rendersi necessarie a seguito degli esiti di analisi/valutazioni da parte dei diversi Responsabili/Ruoli operanti nell’ambito delle articolazioni organizzative aziendali e/o in ragione di intervenute disposizioni attuative in materia di protezione dei dati personali.

1 – Modello di *governance* e piano di adeguamento: *Data Inventory*

L'obiettivo della prima area di attività è finalizzato alla conoscenza dei dati trattati.

Il GDPR prevede a tal fine la creazione di un **"registro dei trattamenti"** (art.30) che può essere redatto in forma cartacea o anche in formato elettronico/digitale. In tal senso l'Azienda si è orientata sull'acquisizione di apposito *software* che consenta di gestire anche, appunto, il predetto Registro; tale procedura è ad oggi in fase di espletamento.

1.1 - Il Registro dei trattamenti (*ex* art. 30 del GDPR)

La tenuta di un registro delle attività di trattamento rappresenta non solo uno dei primi adempimenti obbligatori previsti dal Regolamento UE 2016/679, ma soprattutto uno strumento operativo e funzionale alla gestione organica e sistematica dei dati trattati. Obbliga, infatti, ad avere un censimento sempre aggiornato dei dati trattati, un elenco ordinato degli archivi (o delle base dati) che contengono i dati, una classificazione delle categorie degli interessati coinvolti nonché una completa mappatura di tutti gli elementi rilevanti di un trattamento di dati personali per assicurare non solo un impianto di *Data Protection* in linea con i diversi requisiti normativi, ma anche un controllo reale, puntuale ed effettivo delle attività svolte.

Oltre alla sua natura di strumento operativo di lavoro *ex ante*, la costituzione e l'aggiornamento del registro delle attività rappresenta anche un importante documento probatorio *ex post* da esibire in caso di verifica da parte dell'Autorità di Controllo al fine di dimostrare - nell'ottica del principio di *accountability* - la *compliance* al GDPR. Al riguardo, si rileva che la mancata tenuta del registro delle attività di trattamento può essere soggetta alla sanzione amministrativa pecuniaria fino a 10 milioni di euro.

In tale sede giova richiamare testualmente la raccomandazione espressa – sul punto - dall'Autorità Garante italiana per la protezione dei dati personali nell'ambito della "Guida all'applicazione del Regolamento Europeo in materia di protezione dei dati personali", pubblicata sul sito web istituzionale dell'Autorità medesima:

"La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali. Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche - ove già non condotta. I contenuti del registro sono fissati, come detto, nell'art. 30; tuttavia, niente vieta a un Titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti.".

Con Comunicato dell'08.10.2018, il Garante stesso ha, inoltre, pubblicato sul proprio sito *web* un modello di registro che i titolari ed i responsabili possono utilizzare ed integrare nei modi più opportuni.

Tanto premesso, la costruzione sistematica del registro richiede un impegno significativo, soprattutto in ambito sanitario ove vengono trattati e prodotti dati in grande quantità e con un

livello di alta "sensibilità". Proprio in ragione della complessità e specificità del contesto organizzativo di riferimento, l'Azienda ha orientato, come detto, la propria scelta sull'acquisizione di apposito *software* che consenta di alimentare e aggiornare direttamente il formato elettronico tale registro.

1.1.1 – Contenuti del Registro

Al paragrafo 1 e 2 dell'art. 30, rispettivamente, il GDPR dettaglia - come di seguito riportato - i contenuti minimi del Registro del Titolare del trattamento e del Registro del Responsabile del trattamento.

Il Registro del Titolare deve contenere:

a) il nome e i dati di contatto del Titolare del trattamento e, ove applicabile, del conTitolare del rappresentante del Titolare del trattamento e del responsabile della protezione dei dati;

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, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle 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 organizzative di cui all'articolo 32, paragrafo 1.

Il Registro del Responsabile deve contenere:

a) 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, ove applicabile, del responsabile della protezione dei dati;

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'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Come risulta evidente i due registri non hanno identico contenuto: solo il Titolare del Trattamento deve dettagliare anche le finalità, le categorie di interessati, di dati personali

trattati, di soggetti cui i dati possono essere comunicati e i tempi di data *retention*. Sono tutti gli elementi "distintivi" di un trattamento dati che non possono essere decisi da un Responsabile del trattamento, pena l'assunzione di fatto dello *status* di Titolare, con tutte le responsabilità tipiche che ne derivano (art. 28, paragrafo 10, del GDPR).
Le informazioni che, invece, possono essere speculari in entrambi i registri, laddove il trattamento viene svolto dal Responsabile per conto del Titolare, sono - oltre a quelle generali sui soggetti coinvolti nelle attività di trattamento - le misure di sicurezza tecniche ed organizzative messe in atto per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al GDPR e gli eventuali trasferimenti verso paesi terzi con il dettaglio delle garanzie adeguate in conformità a quanto disciplinato negli artt. 46 e seguenti del GDPR.
Il Registro delle attività di trattamento può contenere una serie di informazioni ulteriori rispetto a quelle minime previste nei paragrafi 1 e 2 dell'art. 30, quali ad esempio: la base giuridica su cui si fonda il trattamento, le modalità di raccolta del consenso, l'elenco dei database e degli applicativi utilizzati, la filiera di tutti soggetti coinvolti nel trattamento (responsabili, sub-responsabili), ecc. in quanto fondamentali per contribuire alla formazione di un sistema documentale *privacy* quanto più possibile organico e completo.

1.1.2 – Categorie di dati personali

Per dato personale, ai sensi dell'art. 4 del GDPR, si intende "qualsiasi informazione riguardante una persona fisica identificata o identificabile: 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".
In relazione alla tipologia di informazioni da essi veicolate, alcuni dati personali sono inseriti dal Regolamento UE 2016/679 in apposite categorie. All'eventuale violazione di questi dati "particolari" è associato un rischio maggiore per i diritti e le libertà fondamentali degli individui a cui le informazioni si riferiscono; il trattamento dei dati personali appartenenti a queste "categorie particolari" necessita perciò di maggiori cautele e garanzie.
Si tratta, ai sensi degli artt. 9 e 10 del GDPR, di tutti i dati atti a rivelare l'origine razziale o etnica, le opinioni politiche, l'appartenenza sindacale e le convinzioni religiose o filosofiche di un individuo, insieme alle informazioni genetiche, ai dati biometrici, alle notizie in merito alla salute, alla vita o all'orientamento sessuale della persona e alle informazioni relative ai reati o alle condanne penali.
Di seguito si riportano le definizioni contenute nella normativa.
Dati genetici: sono i dati relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, che forniscono informazioni univoche sulla sua fisiologia o sulla sua salute, e sono desumibili in particolare dall'analisi di un suo campione biologico.

Dati biometrici: sono i dati ottenuti da un trattamento tecnico specifico che forniscono informazioni relative alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, consentendone o confermandone l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Dati relativi alla salute: sono i dati attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

Dati relativi a condanne penali o reati: sono i dati relativi alle condanne penali, ai reati o a connesse misure di sicurezza.

Il trattamento delle categorie particolari di dati personali di cui al citato art. 9 è sempre vietato a meno che:

- l'individuo abbia prestato il proprio consenso esplicito al trattamento di tali dati per finalità specifiche;
- il trattamento sia necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare del trattamento o dell'individuo in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
- il trattamento sia necessario per tutelare un interesse vitale di un individuo o di un'altra persona fisica qualora l'individuo si i trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- Il trattamento sia effettuato da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con dette entità, avvenga in relazione a fini che sono loro propri e che i dati personali non siano comunicati all'esterno senza il consenso dell'individuo;
- il trattamento riguardi dati personali resi manifestamente pubblici dall'interessato;
- il trattamento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
- il trattamento sia necessario per motivi di interesse pubblico;
- il trattamento sia necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della Sanità, fatti salvi i casi in cui i dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza;
- il trattamento sia necessario per motivi di interesse pubblico nel settore della Sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero

o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici;

- il trattamento sia necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, sia proporzionato alla finalità perseguita, rispetti l'essenza del diritto alla protezione dei dati e preveda misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'individuo.

Il trattamento di dati personali relativi a condanne penali e reati o a connesse misure di sicurezza di cui al citato articolo 10 è sempre vietato a meno che esso avvenga sotto il controllo dell'autorità pubblica, oppure per autorizzazione del diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

MISURE/AZIONI DA ATTUARE

(codice misura A)

Ai fini della strutturazione del Registro del Titolare si procederà alla ricognizione dei dati di cui all'art. 30, paragrafo 1, lettere b), c), d), e), f), g), da formalizzare in apposito documento predisposto a cura del Responsabile della Protezione dei Dati (DPO)/Gruppo multidisciplinare di supporto al DPO e quindi sottoposto all'analisi della Direzione Medica dei Presidi per i dati di natura sanitaria e del Servizio Informatico/Responsabile per la Transizione Digitale (RTD). Tale documento così redatto verrà esaminato congiuntamente alla Direzione Generale ai fini della relativa validazione e lo stesso sarà quindi ricondotto nel Registro dei trattamenti, a seguito della relativa acquisizione.

1.1.3 – Categorie dei trattamenti

Ai fini della strutturazione del Registro in termini di contenuti, oltre alle azioni già rilevate nel precedente paragrafo, sarà parimenti condotta la ricognizione/aggiornamento delle categorie dei trattamenti effettuati dai Responsabili per conto del Titolare del trattamento - secondo quanto previsto dall'art. 30, paragrafo 2, lettera b) - procedendo altresì alla rilevazione delle specifiche informazioni di cui alle lettere c) e d) del medesimo paragrafo.

A tal proposito le informazioni necessarie possono essere reperite da:

- mappatura dei processi/percorsi in cui sono riportate le attività di trattamento (ad es. procedure interne);
- ricognizione delle schede dei trattamenti precompilate;
- recupero delle informazioni contenute nei diversi documenti aziendali, opportunamente riviste e/o validate dalla Direzione Medica dei Presidi, per le UU.OO. sanitarie, e dai Responsabili di struttura per le UU.OO. di Staff e di area amministrativa e tecnica.

Con riferimento, più in generale, alle attività di ricognizione delle informazioni connesse ai trattamenti, potrà farsi riferimento a *checklist* privacy standard e *best practice* eventualmente esistenti nel settore di riferimento.

MISURE/AZIONI DA ATTUARE

(codice misura B)

Ai fini della strutturazione del Registro del Responsabile si procederà alla ricognizione dei dati di cui all'art. 30, paragrafo 2, lettere b), c), d), da formalizzare in apposito documento predisposto a cura del DPO/Gruppo multidisciplinare di supporto al DPO, in stretto raccordo e con il supporto della Direzione Medica dei Presidi per i dati di natura sanitaria, con il coinvolgimento delle Unità di Staff e del Dipartimento Tecnico Amministrativo, del Servizio Informatico/RTD, e comunque con il coinvolgimento di tutti i "Referenti" (come individuati al corrispondente capitolo Misure Organizzative) al fine di ottimizzare le informazioni da raccogliere. Tale documento così redatto verrà esaminato congiuntamente al Direttore Sanitario e Amministrativo per gli ambiti di rispettiva competenza.

1.1.4 – Tenuta e aggiornamento del Registro

A seguito dell'acquisizione del Registro dei trattamenti in formato elettronico nonché della relativa implementazione - come espresso nei paragrafi che precedono - la tenuta del Registro medesimo è in capo al Titolare e ai Responsabili.

Relativamente alla sezione del Registro del Titolare, quest'ultimo, secondo quanto previsto dal WP243, paragrafo 4.5, può affidare al Responsabile della Protezione dei Dati (DPO) il compito di tenere il registro delle attività di trattamento.

Pertanto a livello aziendale, il Registro dei trattamenti del Titolare è tenuto ed aggiornato a cura del DPO; mentre il Registro dei trattamenti dei Responsabili è tenuto ed aggiornato a cura dei Responsabili/Direttori di Unità Operativa come designati al corrispondente paragrafo di cui alle Misure Organizzative.

Si evidenzia che il Registro deve essere aggiornato con regolarità onde assicurare una rappresentazione realistica dei trattamenti effettuati e di tutti gli aspetti correlati oggetto di attenzione da parte del GDPR (finalità, eventuali trasferimenti verso paesi terzi ecc.).

In particolar modo, sarà necessario provvedere ad un aggiornamento del Registro in presenza di ogni cambiamento organizzativo, operativo e tecnologico rilevante e tale da impattare sulla gestione dei dati personali.

MISURE/AZIONI DA ATTUARE

(codice misura C)

Definizione ed attivazione di flussi informativi periodici e/o specifici verso il soggetto o l'unità organizzativa preposta all'aggiornamento del Registro.

1.2 - Inventario degli *asset* tecnologici

Una buona gestione dell'inventario è un presupposto per l'efficacia e l'efficienza di molti processi di gestione.

Nel caso dell'adeguamento al GDPR, costituisce il collegamento fra il Registro dei trattamenti - che è il punto di partenza per individuare gli ambiti applicativi ed i flussi interessati - ed il sistema informativo aziendale in quanto insieme di *asset* tecnologici.

Il primo e più importante aspetto riguarda la capacità di associare i trattamenti agli *asset* che li supportano: sistemi e applicativi principalmente, ma anche componenti infrastrutturali.

Il Servizio Informatico/RTD deve assicurare la mappatura ed il costante aggiornamento dell'inventario degli *asset* e dei flussi corrispondenti.

Da un punto di vista operativo, tale inventario sarà a supporto degli interventi di adeguamento: laddove, ad esempio un provvedimento del Garante, un'evoluzione del rischio o una modifica ad un trattamento richiedano di intervenire sui sistemi a supporto di uno o più trattamenti, l'inventario permetterà di fornire la completezza del perimetro su cui le modifiche saranno effettuate.

Infine, in caso di *data breach*, nella direzione opposta, a fronte della compromissione di uno o più sistemi, sarà possibile individuare con la tempestività richiesta i trattamenti potenzialmente impattati. Detto aspetto è, quindi, presupposto necessario:

- per una gestione della sicurezza in generale e della conformità all'art. 32 del GDPR;
- per individuare, ad esempio, i sistemi interessati da una vulnerabilità relativa ad una specifica versione di sistema operativo;
- per valutare correttamente le segnalazioni di un sistema di *intrusion detection* o di monitoraggio eventi in generale.

In questa prospettiva è particolarmente importante un inventario degli applicativi, dei *database* e dei *middleware*, nonché dei sistemi a supporto, che comprenda le versioni dei *software* e lo stato di aggiornamento (anche di strumenti di sicurezza come gli antivirus). Queste informazioni si devono integrare con una mappa dei flussi applicativi; ciò in quanto l'Azienda, operando in ambito sanitario, tratta e produce dati in grande quantità e con un livello di alta "sensibilità". Pertanto, la corretta e sicura gestione dei dati dei pazienti - in particolare quelli idonei a rilevare lo stato di salute - deve essere finalizzata ad assicurarne al contempo la confidenzialità, l'inviolabilità e la protezione al fine di prevenire danni materiali e morali all'individuo, come ad es. ipotesi di discriminazioni.

MISURE/AZIONI DA ATTUARE

(codice misura D)

Mappatura e costante aggiornamento dell'inventario degli *asset* tecnologici e dei flussi corrispondenti a cura del Servizio informatico/RTD in raccordo con Fisica Medica e Tecnologie Biomediche/*Information Communication Technology*.

2 - Modello di *governance* e piano di adeguamento: Analisi dei rischi e degli impatti

La seconda area di attività riguarda la valutazione dei rischi connessi ai trattamenti e i relativi impatti sulla protezione dei dati.
In sede di prima applicazione si intende attivare la costruzione di una mappa dei rischi che consenta di stimare, per ogni tipologia di trattamento, un indice di rischio generico.
Conseguentemente, una volta determinati i rischi, occorre effettuare la valutazione degli impatti per singolo processo operativo supportato da ICT, così come prevista dall'art. 35 del GDPR.
Sul punto, occorre operare riferimento - oltreché al richiamato art. 35 del GDPR - alle "Linee Guida in materia di valutazione di impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato ai fini del regolamento (UE) 2016/679" del Gruppo di lavoro Articolo 29 per la Protezione dei Dati adottate il 4 aprile 2017 e modificate il 4 ottobre 2017 (WP 248 rev.01), l'Infografica del Garante conforme alle richiamate Linee Guida ed il Provvedimento del Garante dell'11 ottobre 2018 riportante l'elenco delle tipologie di trattamenti soggetti al requisito di una valutazione di impatto.
Inoltre, sempre sul punto, è importante evidenziare che il Garante, al fine di agevolare i soggetti tenuti ad effettuare la valutazione di impatto, con Comunicato del 6 gennaio 2018 ha reso disponibile e liberamente scaricabile sul proprio sito istituzionale il software a tal fine predisposto dall'Autorità francese per la protezione dei dati. Detto software offre un percorso guidato alla realizzazione della valutazione di impatto secondo una sequenza conforme alle più volte citate Linee Guida.

2.1 - Analisi preliminare del rischio

Nell'ambito della Sanità elettronica, da un'attenta ricerca condotta sulle priorità fissate dall'Autorità Garante in questo ambito (si faccia riferimento alle Relazioni annuali del Garante Privacy), emerge quella di assicurare la massima protezione dei dati sanitari dei pazienti favorendo, al contempo, lo sviluppo di nuove tecnologie nella cura delle persone. Ciò comporta che l'Azienda, nella sua veste di Titolare del trattamento, deve porsi nella stessa prospettiva garantista incentrata sui diritti dell'interessato, operando continui bilanciamenti tra i benefici connessi all'uso delle tecnologie e i rischi potenzialmente lesivi dei diritti e delle libertà dei pazienti.
A tal proposito, si ritiene di continuare a fare riferimento alle regole e prescrizioni dettate negli anni dal Garante Privacy nell'ambito di specifici settori o tematiche individuati dall'Autorità stessa, in quanto caratterizzati quali aree potenzialmente ad alto livello di rischio. In particolare, si fa riferimento ai seguenti ambiti:

- fascicolo sanitario elettronico

- dossier sanitario elettronico
- refertazione *on line*
- monitoraggio a distanza dei pazienti portatori di defibrillatori cardiaci
- prenotazione di visite specialistiche (es. presso i Cup e presso le farmacie)
- interconnessione delle banche dati
- IoT (*Internet of Things*).

L'obiettivo primario delle prescrizioni del Garante Privacy, in perfetta assonanza con le previsioni del GDPR, è quello di garantire che le strutture sanitarie che raccolgono, utilizzano, conservano dati lo facciano avendo preventivamente sotto controllo l'entità del rischio per ogni attività di trattamento e che lo stesso sia preventivamente valutato onde provvedere alla messa in sicurezza sotto il profilo della protezione dei dati.

L'analisi dei rischi di un trattamento sulla protezione dei dati deve tener conto del processo in cui viene operato il trattamento dei dati, potendosi distinguere tra processi principali e di supporto.

Conseguentemente, al fine di determinare il profilo di rischio di un tipo di trattamento (con successiva valutazione della necessità o meno di avviare una valutazione d'impatto sulla privacy di quel trattamento) è utile tenere presente:

- le casistiche previste dal GDPR;
- le casistiche previste dalle Linee Guida del Gruppo ex art. 29 -wp 248-(denominato "WP29");
- le risultanze dell'analisi di adeguatezza dei presidi operate nell'ambito di ulteriori attività di analisi dei rischi (ad es. analisi condotte nell'ambito del Sistema di gestione della qualità, analisi dei rischi cyber relativi all'uso di ICT ecc.).

In proposito, si segnala che il GDPR prevede la possibilità di effettuare la DPIA in base al livello di rischio. In ogni caso – trattandosi di contesto sanitario - la tipologia di dati trattati e la complessità dei processi organizzativi supportati da ICT (che nella maggioranza dei casi richiedono continuità operativa h24) è altamente probabile che la maggior parte dei trattamenti siano a rischio elevato.

MISURE/AZIONI DA ATTUARE

(codice misura E)

A seguito della implementazione del Registro delle attività di trattamento sarà effettuata una analisi di rischi e impatti per ogni macro-processo operativo nel quale vengono trattati dati personali e sensibili. In tal senso, il DPO/Gruppo multidisciplinare di supporto al DPO/Servizio Informatico/RTD provvederanno a formalizzare apposito documento in stretto raccordo e con il supporto della Direzione Medica dei Presidi (per i dati di natura sanitaria) e delle Unità di Staff e del Dipartimento Tecnico Amministrativo. Tale documento così redatto sarà esaminato congiuntamente alla Direzione Generale ai fini della relativa validazione.

2.1.1 – Analisi del rischio: rischio inerente e rischio residuo

Il GDPR prevede in capo al Titolare del trattamento l'onere di procedere ad una valutazione oggettiva del rischio, avendo riguardo della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento.

Da tale valutazione sarà possibile stabilire che tipo di rischio comporti ogni attività di trattamento di dati. È utile però precisare che vi sono due tipologie di analisi previste all'interno del GDPR, distinte e complementari.

Una è il *Data Protection Impact Assessment* (DPIA), che è un'analisi degli impatti (non del rischio) volta ad individuare i trattamenti che presentino un rischio elevato per i diritti e le libertà delle persone fisiche, riconducibile all'art. 35 del GDPR. La DPIA può portare all'esigenza di adottare delle misure di sicurezza volte ad attenuare adeguatamente il rischio.

La seconda analisi, riconducibile principalmente all'art. 32 del GDPR, è un'analisi del rischio, che ha lo scopo di valutare in generale l'adeguatezza delle misure di sicurezza volte ad attenuare il rischio per i dati personali. Quest'ultima, a differenza della prima, è dovuta in generale laddove avvenga un trattamento di dati personali (lo sarà a maggior ragione dove la DPIA avrà individuato degli impatti potenzialmente elevati).

Posto che la crescente digitalizzazione dei processi genera costantemente nuovi scenari di rischio (informatico e non solo), sia all'interno che all'esterno dell'organizzazione, il GDPR, focalizzandosi sulla protezione dei dati personali, evoca la necessità di un cambiamento significativo nell'approccio di gestione degli stessi. Ciò, in particolare, perché le nuove tecnologie consentono di erogare servizi sempre più personalizzati per i cittadini, ma nel contempo aumentano la complessità e la pervasività dei trattamenti di dati personali svolti nell'ambito dell'erogazione di tali servizi.

Il trattamento dei dati personali deve essere conforme ai principi generali previsti dal GDPR nonché dalle prescrizioni del Garante Privacy nei settori di riferimento come, tra gli altri, il settore sanitario.

Tali principi devono trovare piena soddisfazione a prescindere dal livello di rischio stimato tramite analisi del rischio e valutazione degli impatti del trattamento. In sostanza, l'insieme di tali principi costituisce lo sfondo di ogni valutazione di impatto che il Titolare del trattamento effettuerà. In ogni caso l'attuazione di questi principi generali, sarà in concreto verificabile in corrispondenza del livello di rischio riscontrato per il trattamento oggetto di valutazione.

L'analisi dei rischi, pertanto, si configura nel GDPR come una attività funzionale al mantenimento della sicurezza e alla prevenzione di trattamenti in violazione delle prescrizioni ivi dettate.

Ciò posto, tale attività di analisi dei rischi va condotta sia per i nuovi trattamenti sia per tutti i trattamenti posti in essere dal Titolare avendo cura di provvedere ad una costante e puntuale mappatura degli stessi utile a preservare un adeguato livello di sicurezza e a prevenire in modo tempestivo eventuali non conformità al GDPR.

Sarà anche utile procedere ad analizzare l'eventuale insorgere o aggravamento di rischi al prefigurarsi di un sopraggiunto cambiamento organizzativo, tecnologico o di processo che possa incidere significativamente sul livello di conformità alle previsioni del GDPR da parte di trattamenti già oggetto di mappatura ed analisi precedentemente al cambiamento intervenuto (anche al fine di aggiornare il Registro delle attività di trattamento).

La protezione dei dati e dei sistemi aziendali costituisce un fattore determinante di efficienza sanitaria. Il processo di digitalizzazione della Sanità (c.d. *E-Health*) comporta una attività sempre più puntuale di valutazione dei rischi connessi all'uso di nuove tecnologie in tale ambito, rispetto al quale l'assenza di valutazioni preventive della pericolosità di un trattamento o di un piano organico di sicurezza potrebbe mettere a rischio non solo banche dati essenziali ma, insieme, viola diritti e libertà delle persone.

I rischi che il trattamento di dati personali può astrattamente sollevare riguardo ai diritti e alle libertà dei soggetti ai quali si riferiscono le informazioni raccolte e utilizzate devono essere considerati nell'ambito delle attività di analisi nell'ottica di "probabili conseguenze". Queste ultime potranno essere identificate come:

• danni materiali (ad es. un danno fisico)

• danni immateriali (ad es. discriminazione).

In primo luogo, dovrà essere rilevato **il rischio inerente ad un trattamento** (cioè la combinazione tra la gravità della conseguenza - in astratto configurabile - e la probabilità del suo accadimento in assenza di misure atte a ridurlo) e si procederà poi ad un confronto con le caratteristiche e modalità fattuali del tipo di trattamento oggetto di analisi.

In secondo luogo, andranno individuate le misure appropriate per minimizzare il livello di rischio per il trattamento rilevato, nell'ottica di conformità rispondente a principi di scalabilità e proporzionalità. L'adozione delle misure a garanzia dei diritti e delle libertà degli interessati permetterà di valutare come il rischio inizialmente configurabile in astratto come inerente al trattamento possa essere concretamente mitigato.

A questo punto, sarà possibile valutare l'eventuale **livello di rischio residuo** (ovverosia la porzione residuale di rischio ponderata appunto in considerazione delle misure individuate).

2.1.2 - Analisi del rischio: profili tecnici

Secondo la norma ISO 31000 "Gestione del rischio", di riferimento in materia di rischio per tutta la famiglia di norme ISO, il rischio è l'effetto dell'incertezza sugli obiettivi. Questa definizione è in linea con il concetto più comune ed informale che descrive il rischio come funzione di una probabilità (l'incertezza) e di un impatto (l'effetto). Anche il GDPR si allinea a tale impostazione laddove all'art. 32 richiama il "rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche".

L'analisi dei rischi richiede, quindi, di valutare sia la componente probabilistica che quella di impatto. Si tratta, in generale, di stime in quanto le valutazioni su possibili eventi del futuro comportano sempre un'aleatorietà difficilmente quantificabile.

L'analisi di impatto comprende due prospettive: quella della DPIA, richiesta esplicitamente dal GDPR, e quella dell'impatto sui processi aziendali data da possibili incidenti di sicurezza. Quest'ultima è richiesta per valutare l'adeguatezza delle misure di sicurezza adottate. Si tratta quindi di due prospettive diverse, entrambe da considerare per individuare i componenti del sistema informativo la cui compromissione avrebbe un impatto importante sui processi aziendali (e quindi di nuovo, indirettamente, anche sui dati personali) o sugli interessati. Mentre le valutazioni di impatto sono a carico principalmente dei responsabili dei diversi processi, le valutazioni di probabilità, tolta una valutazione "generica" di rischiosità dell'ambito di attività dell'Azienda, sono di competenza del Responsabile del Sistema informativo/RTD. Per semplificare l'esecuzione della DPIA e la valutazione di impatto di sicurezza sui processi aziendali, può essere utile fare riferimento a delle fasce di impatto. L'obiettivo di questa attività consiste nel formulare ipotesi condivise circa la gravità degli impatti e la probabilità di accadimento per poi individuare il rischio.

Nel valutare la componente probabilistica occorre formulare e fornire risposta ai seguenti quesiti:

a) Cosa si vuole proteggere (vale a dire identificazione dei Beni Aziendali o *Asset* Informativi) (a)
b) Da cosa ci si vuole proteggere (vale a dire identificazione delle Minacce) (m)
c) Perché proteggersi (vale a dire Identificazione delle Vulnerabilità) (v)
d) Come proteggersi (vale a dire misure Tecnico Organizzative e Applicative, controlli di sicurezza) (c)

Il punto di partenza per un'analisi del Rischio è l'analisi del contesto e l'individuazione dei beni da proteggere, identificare le minacce, identificare le vulnerabilità e i controlli di sicurezza, rapportare le minacce alle vulnerabilità, definire l'impatto su ciascun bene in relazione al mancato rispetto dei requisiti, quindi valutare il rischio per ciascun bene.

Il Rischio potrà essere calcolato attraverso una relazione del tipo:

Rischio(m,a,v) = probabilità(m,v)*impatto(m,a,v)

dove la vulnerabilità è inversamente proporzionale al controllo di sicurezza adottato (c).

Il passo successivo consiste nell'identificazione delle minacce che possono determinare la gravità degli impatti.

La ISO/IEC 27000 fornisce questa definizione: *minaccia: causa potenziale di un incidente, che può comportare danni ad un sistema o all'organizzazione* dove incidente è relativo alla sicurezza delle informazioni e l'analisi del rischio richiede di identificare e valutare tutte le minacce relative alla sicurezza delle informazioni, quindi non solo quelle informatiche o quelle più significative.

Gli elementi di rischiosità che derivano dal Trattamento di dati e che occorre tenere in considerazione sono quelli che portano alla:

- distruzione o non disponibilità
- perdita

- modifica
- divulgazione non autorizzata
- accesso accidentale o illegale dei dati personali trasmessi, conservati o comunque trattati (art. 32 c.2 del GDPR).

Questi elementi di rischiosità possono essere sintetizzati attraverso i parametri della Terna RID:

- Riservatezza (R)
- Integrità (I)
- Disponibilità (D)

Le minacce, per essere identificate, devono essere correlate ai parametri RID e poiché possono avere impatti su uno o più di questi parametri è utile utilizzare una struttura a matrice. Per rendere sistematica l'analisi delle minacce, è opportuno disporre di un elenco come risultante dall'allegata tabella:

MINACCIA	**R**	**D**	**I**
Malware	X	X	X
Diffusione documenti	X		
Modifica scorretta sistema IT	X	X	X
Furto di identità (credenziali)	X	X	X
Modifica non autorizzata di documenti informatici da non malintenzionati		X	
Modifica non autorizzata di documenti informatici da malintenzionati		X	
Attacchi di *Denial of Service*			X
Uso eccessivo e involontario delle risorse da parte degli utenti			X

Blackout elettrici		X	X
Guasto impianto			X
Incendio		X	X
Ransomware	X	X	X
Lettura e copia non autorizzata di documenti digitali	X		
Invio di dati a persone non autorizzate	X		
Danneggiamento di apparecchiature fisiche	X	X	X
Danneggiamento dei programmi informatici	X	X	X
Accesso non autorizzato ai sistemi IT	X	X	X
Furto di apparecchiature informatiche o fisiche	X	X	X
Social Engineering	X	X	X
Lettura, furto copia o alterazione di documenti in formato fisico	X	X	X
Trattamento scorretto delle informazioni rispetto alla normativa	X		

Le minacce dovrebbero essere inizialmente individuate dai Referenti delle Informazioni o dai Responsabili di Struttura/Processo ma la necessità di competenze specifiche e la loro natura probabilistica come cause potenziali di incidente rende necessario il coinvolgimento del Responsabile dei Sistemi Informativi.

Senza identificare tutte le possibili vulnerabilità di un sistema informatico ci si limita ad elencare, in via non esaustiva, le seguenti tipologie più comuni:

- vulnerabilità strutturali
- vulnerabilità connesse all'architettura di rete
- vulnerabilità organizzative/procedurali
- vulnerabilità di sistemi/applicazioni
- vulnerabilità del s*oftware*, *overflow*, *format string*
- errori di configurazione
- vulnerabilità dei protocolli
- debolezza di progettazione attacchi *Spoofing, Hijacking, Sniffing*
- errori implementazione dello *stack* di rete: attacchi *Dos, DdoS*

I controlli di sicurezza più utilizzati da mettere in atto per contrastarle sono quelli noti come:

- *Antivirus*
- *Antispyware*
- *Firewall*
- Firma digitale, Crittografia
- *Backup*
- *Intrusion Detection System (IDS)*
- *Network Intrusion Detection System (NIDS)*
- Sistema di autenticazione/autorizzazione

Dove il Rischio è elevato le misure di sicurezza applicate dovranno essere adeguate. Si evidenzia, a tal proposito, come le linee guida del Garante in ambito dossier sanitario elettronico già richiedessero misure appropriate come:

- Tracciabilità degli accessi e delle operazioni effettuate
- Sistemi di *audit log*
- Separazione e cifratura dei dati
- *Data breach*
- *Data protection officer*

Da un punto di vista operativo, l'analisi dei rischi è finalizzata a:

- identificare i rischi maggiori, per i quali devono essere necessariamente adottate delle contromisure atte a mitigarli fino a ridurli ad un livello adeguato;

- definire, tenuto conto delle risorse disponibili, l'elenco degli interventi secondo un ordine di priorità;
- dare evidenza del rischio residuo, che i responsabili dei diversi processi dovranno esplicitamente accettare.

E' importante evidenziare che la responsabilità di individuazione del rischio residuo non è, in generale, in capo al Responsabile dei Sistemi Informativi, bensì in capo ai Responsabili delle Strutture/Processi aziendali nel cui ambito si manifestano gli impatti.

2.2 - Ambito di applicazione della Valutazione di Impatto (DPIA)

La DPIA può riguardare una sola operazione di trattamento dei dati oppure una singola valutazione può affrontare una serie di operazioni di trattamento simili che presentano rischi simili elevati (come, ad esempio, il caso in cui l'Azienda voglia adottare un dispositivo tecnologico del tutto simile ad uno già in uso per raccogliere lo stesso tipo di dati per le medesime finalità).

Quando il trattamento coinvolga diversi Contitolari, essi devono definire i propri rispettivi obblighi con precisione e, in particolare, ogni DPIA eseguita deve indicare quale Titolare è responsabile in ordine alle varie misure individuate per mitigare i rischi.

2.2.1 - Come effettuare una DPIA: approccio metodologico

Posto che il GDPR, le richiamate Linee guida del WP29 ed il Provvedimento del Garante Privacy (pubblicato sulla Gazzetta Ufficiale Generale in data 19.11.2018) offrono esempi di casistica di trattamenti a rischio elevato, l'Azienda – prima di avviare un tipo di trattamento ad elevato rischio – dovrà effettuare una DPIA più complessa e dettagliata in rapporto a quel "tipo" di trattamento che si articolerà nelle sotto-fasi di seguito riportate:

Valutazione della probabilità totale di accadimento delle minacce

Analogamente a quanto avviene in caso di trattamento a rischio non elevato, lo scopo di questa fase è analizzare qualitativamente la probabilità di accadimento delle principali minacce che insistono sui dati personali.

La probabilità di accadimento di tali minacce sarà connessa al livello di implementazione delle misure organizzative/ operative e tecniche implementate a protezione dei dati personali.

Valutazione del livello di gravità per ogni binomio minaccia-danno

In questa fase, alla probabilità calcolata nella precedente fase, dovrà essere associata una valutazione della gravità per ciascun binomio minaccia - danno.

Essendo in presenza di un livello di rischio elevato ("Alto" nella scala di ponderazione) dovrà essere effettuata una valutazione più di dettaglio (appunto richiesta espressamente dall'art. 35

del GDPR), valutando la gravità per una serie di danni ad un **livello di granularità maggiore** rispetto al caso dell'analisi preliminare di trattamenti a rischio non elevato.
In particolare, per i trattamenti a rischio elevato i danni considerati sono di due tipologie: danni materiali e danni immateriali.
Con riferimento alla gravità, essa dovrà essere valutata a livello qualitativo sulla base della scala di valutazione richiamata in sede di analisi preliminare di rischio.

Valutazione del rischio complessivo del trattamento: implementazione misure o consultazione preventiva

In funzione della valutazione della gravità e della probabilità per ciascun binomio minaccia-danno, si determineranno i principali danni per l'interessato e i rischi. Pertanto, si procederà alternativamente:

- con l'implementazione di misure e accorgimenti opportuni, che dovranno ridurre il rischio ad un livello contenuto;
- con la consultazione dell'autorità di controllo in caso di assenza di misure adeguate per attenuare il rischio elevato rilevato.

Implementazione delle misure e calcolo del rischio residuo

Dovrà essere valutato, a monte, il livello di adeguatezza delle misure da implementare, in termini organizzativi/operativi e tecnici, in ragione dell'efficacia di mitigare significativamente il rischio.
Individuate le misure, è necessario effettuare nuovamente la valutazione di gravità e probabilità per ciascun binomio minaccia-danno, al fine di valutare il rischio residuo connesso al trattamento. Qualora il giudizio della DPIA considerasse che il trattamento dei dati personali in oggetto, mediante l'implementazione delle misure adottate, conduca ad un rischio residuo per i diritti e le libertà degli interessati determinabile come corrispondente a un livello "Basso" (non elevato), si procederà alla loro implementazione.
Andrà poi monitorata l'effettiva implementazione delle misure nel rispetto della pianificazione prevista.

Consultazione preventiva dell'Autorità di controllo in assenza di misure adeguate alla mitigazione del rischio ai sensi dell'art. 36 del GDPR

Se non sussistano misure adeguate e si ritiene che il trattamento possa violare le previsioni del GDPR, il Titolare consulta preventivamente il Garante Privacy il quale fornirà, entro un termine di otto settimane (prorogabile tenendo conto della complessità del trattamento), un parere scritto.
Nella richiesta di consultazione andranno indicate le seguenti informazioni:

- le responsabilità del Titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento;
- le finalità e i mezzi del trattamento;

- le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del GDPR;
- i dati di contatto del DPO;
- le risultanze della DPIA.

Il Garante potrà, poi, richiedere informazioni integrative.

Ulteriori criteri per la conduzione di un'adeguata DPIA sono riportati nell'allegato 2 alle richiamate linee guida del WP art 29 e agli stessi si potrà, comunque, operare riferimento.

3 – Modello di *governance* e piano di adeguamento: Misure Organizzative

La terza area di attività comprende i seguenti i seguenti ambiti:

- Definizione Organigramma *Privacy*
- Nomina *Data Protection Officer*
- Definizione Titolarità/Contitolarità
- Nomina dei Responsabili dei trattamenti
- Nomina degli Autorizzati al trattamento (già "Incaricati" nell'ambito del precedente Codice Privacy)
- Gestione documentale degli interventi di Sicurezza e *Privacy* (documentazione Organizzativa e Tecnica)
- Notifica dei *Data Breach*.

Il Garante Privacy ha espresso l'opportunità che Titolari e Responsabili del trattamento mantengano in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento così come delineatesi negli anni anche attraverso gli interventi del Garante stesso. In tale contesto, altresì, si segnala l'opportunità, presente nell'art. 28, comma 6, del GDPR, di utilizzare "contratti tipo" per le nomine del personale autorizzato al trattamento qualora svolga attività omogenee (ad es. personale infermieristico, personale medico, ecc...) semplificando la gestione documentale della *privacy*.

3.1 – Titolare del trattamento

Il Titolare del trattamento, nella persona del Legale rappresentante *pro tempore* dell'Azienda, è definito nell'art. 4 del GDPR come "l*a 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*", e *"quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri".*

Al Titolare competono, anche unitamente ad altro Titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Il Titolare è il soggetto su cui grava la responsabilità generale del trattamento, che deve adempiere alle prescrizioni contenute nelle varie disposizioni del Regolamento e che deve essere in grado di dimostrare che il trattamento dei dati personali è effettuato conformemente al Regolamento secondo il principio di responsabilità e l'efficacia delle misure adottate ("*accountability*").

Gli artt. 24 e 25 del GDPR individuano gli obblighi generali in capo al Titolare del trattamento, mentre obblighi specifici sono contenuti in varie altre disposizioni del GDPR stesso ed espressamente richiamate nel presente documento.

Il Titolare può dimostrare il rispetto degli obblighi a suo carico anche attraverso l'adesione a codici di condotta o a meccanismi di certificazione di cui agli artt. 40 e 42 del GDPR.
In particolare, fra gli obblighi generali del Titolare è prevista l'adozione di misure tecniche ed organizzative adeguate onde perseguire le seguenti finalità:

- garantire, ed essere al contempo in grado di dimostrare, che il trattamento è effettuato in conformità al GDPR; ciò comportando l'attuazione di adeguate politiche in materia di protezione, quali ad esempio, effettuare una notificazione della violazione dei dati nel rispetto delle tempistiche previste (art. 33) e fornire dare un riscontro tempestivo all'interessato che eserciti i propri diritti (artt. 12 e ss.);
- proteggere i dati fin dalla fase di ideazione e progettazione del trattamento o di un sistema e nel corso del trattamento stesso (c.d. "*Privacy by Design*"), ad esempio mediante tecniche di pseudonimizzazione (art. 25);
- assicurare che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni singola finalità del trattamento (c.d. "*Privacy by Default*") rendendo inaccessibili i dati personali ad un numero indefinito di persone fisiche senza l'intervento della persona fisica, e ciò con riferimento alla quantità dei dati personali raccolti, alla portata del trattamento, al periodo di conservazione ed all'accessibilità (art. 25).

Nell'individuazione delle misure tecniche ed organizzative adeguate, il Titolare deve tener conto dei seguenti elementi:
- lo stato dell'arte ed i costi di attuazione limitatamente all'approccio di *Privacy by Design*;
- la natura del trattamento;
- l'ambito di applicazione;
- il contesto;
- le finalità del trattamento;
- i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

Relativamente a tale ultimo elemento, il Considerando n. 75 del GDPR precisa che i rischi per i diritti e le libertà delle persone fisiche aventi probabilità e gravità diverse "possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico materiale o immateriale". La probabilità e gravità del rischio devono essere determinati dal Titolare tenendo conto degli stessi elementi considerati per l'individuazione delle misure tecniche ed organizzative adeguate.
Con riferimento alle misure in grado di soddisfare i principi della *Privacy by Design e by Default* sono di ausilio le indicazioni contenute nel Considerando n. 78 del GDPR che indica a titolo esemplificativo:
- la riduzione al minimo del trattamento dei dati personali;
- l'adozione di tecniche di pseudonimizzazione;
- la trasparenza per quanto riguarda le funzioni e il trattamento di dati personali;
- la facoltà dell'interessato di controllare il trattamento dei dati e del Titolare del trattamento di creare e migliorare caratteristiche di sicurezza.

3.2 - Titolare e Contitolare

Il tema della contitolarità di cui all'art. 26 del GDPR riguarda trattamenti che possono esser svolti da più titolari su uno specifico processo di cura. Ci si riferisce, a titolo esemplificativo, all'utilizzo di modelli organizzativi di tipo trasversale (ospedale-territorio-domicilio) - denominati PDTA - per il trattamento della cronicità; detti modelli organizzativi comportano un trattamento svolto da più professionisti in luoghi e tempi diversi ma anche appartenenti a realtà aziendali diverse.

La definizione di contitolarità presente nel GDPR all'art. 26 si attaglia esattamente al PDTA e consente di impostare sia l'informativa che il consenso in modo conseguente: un'unica informativa ed un solo consenso che riguardano l'intero PDTA. Quindi il paziente, concedendo il proprio consenso al PDTA, acconsente al fatto che i dati detenuti dai singoli Contitolari vengano fra essi condivisi e resi accessibili ai fini della gestione del PDTA.

Il PDTA, dunque, è equiparabile ad un ricovero ospedaliero con la relativa cartella clinica elettronica: di conseguenza tutti i dati facenti parte del PDTA sono consultabili dagli attori coinvolti nella gestione del PDTA. Pertanto, così come la cartella clinica è l'insieme dei dati sanitari che afferiscono ad un unico episodio di cura, accessibili quindi a tutti i professionisti coinvolti nella cura del paziente fintanto che il paziente è "in cura", analogamente un PDTA raccoglie dati nell'ambito di un intervallo di tempo all'interno del quale diversi professionisti operano in modo contemporaneo o sequenziale (anche non continuativo) per curare il paziente in un unico percorso che ha un momento (evento) di inizio e un momento (evento) di chiusura. Fra questi due istanti di tempo (inizio e fine) il paziente è "in cura" nel PDTA e i dati del PDTA sono accessibili da parte di tutti i professionisti coinvolti in questo specifico processo di cura (PDTA).

L'art. 26 del GDPR disciplina espressamente l'ipotesi di contitolarità del trattamento, situazione che si ravvisa quando due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento.

In tal caso, i contitolari hanno l'obbligo di determinare in modo trasparente e mediante uno specifico accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento.

Pertanto, qualora l'Azienda - già Titolare del trattamento - rivestisse il ruolo di Contitolare del trattamento deve verificare se, anzitutto, esiste una norma di legge che determini le responsabilità di ciascun Contitolare; diversamente provvederà a redigere specifico accordo interno con l'altro Contitolare contenente i seguenti elementi:

- rispettivi ruoli e i rapporti dei contitolari con gli interessati;
- responsabilità dei Contitolari con riferimento all'esercizio dei diritti dell'interessato e all'obbligo di informativa all'interessato.

Il contenuto essenziale dell'accordo è, inoltre, messo a disposizione dell'Interessato.

In ogni caso, l'accordo interno tra Contitolari non pregiudica i diritti dell'interessato il quale, indipendentemente dalle disposizioni di tale accordo, può esercitare i propri diritti nei confronti di ciascun Titolare del trattamento.

3.3 - Il Responsabile del trattamento

Il Responsabile del trattamento, ovvero la persona fisica o giuridica che tratta i dati per conto del Titolare, deve possedere conoscenza specialistica, affidabilità e risorse per mettere in atto misure tecniche ed organizzative che soddisfino i requisiti previsti dal GDPR anche per i profili di sicurezza del trattamento, garantendo in tal senso la tutela dei diritti dell'Interessato.
Dette garanzie – come previsto all'art. 28, comma 5 - potranno essere dimostrate anche con l'adesione ad un codice di condotta approvato (*ex* art. 40) o ad un meccanismo di certificazione (*ex* art. 42).
I trattamenti da parte di un Responsabile del trattamento sono disciplinati da un contratto o da un altro giuridico a norma del diritto dell'Unione o degli Stati membri; tale contratto - da stipularsi tra Titolare e Responsabile del trattamento – deve contenere la materia disciplinata e la durata dei trattamenti, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento; lo stesso atto deve, in particolare, contenere gli elementi previsti dalle lettere a) - h) del terzo comma dell'art. 28.
Pertanto, il compito del Responsabile del trattamento consiste sostanzialmente nel coadiuvare ed assistere il Titolare in tutte le attività finalizzate a garantire il rispetto del GDPR, ed in particolare:

- nei limiti delle istruzioni documentate fornite dal Titolare, svolgere le attività di trattamento dati adottando le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio (art. 28, c. 3, lettere a e c);
- garantire che le persone fisiche che di fatto dovranno operare sui dati siano non solo autorizzate in modo specifico ma si siano impegnate alla riservatezza o abbiano un obbligo legale in tal senso (art. 28, c. 3, lett. b);
- rispettare le condizioni prescritte per ricorrere ad altro responsabile (art. 28, c. 3, lett. d);
- collaborare con il Titolare nel garantire l'esercizio dei diritti degli interessati di cui agli artt. da 12 a 22 e il rispetto degli obblighi in materia di sicurezza del trattamento, *data breach*, valutazione d'impatto sulla protezione dei dati e consultazione preventiva (art. 28, c. 3, lettere e ed f);
- cancellare o restituire, su scelta del Titolare, i dati personali al termine della prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o dello Stato Italiano preveda la conservazione dei dati (art. 28, c. 3, lett. g);
- mettere a disposizione del Titolare tutte le informazioni necessarie per dare evidenza del rispetto degli obblighi previsti dall'art. 28 consentendo attività di ispezione, *audit* o

revisione ed informandolo qualora le istruzioni fornitegli violino le norme in materia di protezione dei dati (art. 28, c. 3, lett. h);

Ma anche:

- coinvolgere tempestivamente ed adeguatamente il DPO (laddove previsto) in tutte le questioni riguardanti la protezione dei dati; (art. 38, c. 1);
- collaborare con l'Autorità di Controllo (artt. 31 e 58) e con gli organismi di certificazione (art. 42, c. 6), laddove necessario.

È importante che la determinazione dettagliata dei compiti e delle responsabilità assegnate al Responsabile sia formalizzata precedentemente (o contestualmente) all'inizio di qualsiasi attività di trattamento.

Al fine di delimitare le responsabilità di tale figura soggettiva e differenziarle da quelle del Titolare, è necessario che i compiti e le attività assegnate, siano quanto più dettagliate nelle "istruzioni" che devono essere formalizzate fra il Titolare e il Responsabile.

Il Responsabile del trattamento può ricorrere, ai sensi dell'art. 28, c. 2, ad altro Responsabile previa autorizzazione scritta, specifica o generale, del Titolare del trattamento.

Resta fermo che agli eventuali Sub-Responsabili dovranno essere imposti gli stessi obblighi del primo responsabile e questi sono solidalmente responsabili in caso di risarcimento danno.

MISURE/AZIONI DA ATTUARE

(codice misura F)

Sulla base del modello di *Data Protection Governance* che si intende adottare in Azienda, i Direttori di Struttura Complessa (ovvero Responsabili facenti funzione), i Responsabili di Struttura semplice dipartimentale nonché i Dirigenti dell'Area Amministrativa e Tecnica – questi ultimi nel caso in cui non sia presente il titolare dell'incarico di direzione della struttura stessa – assumono il ruolo di Responsabili del trattamento dei dati in ragione delle proprie funzioni e attribuzioni. Ai fini della nomina dei Responsabili del trattamento si procederà, quindi, alla relativa formalizzazione con determina del Direttore Generale, contenente tutti gli elementi *ex* art. 28 del GDPR sopra richiamato, nonché alla notifica della stessa a ciascun Responsabile così nominato. La proposta di determina è a cura della UOC Affari Istituzionali/DPO.

Riguardo ai Responsabili del trattamento quali persone giuridiche o fisiche esterne all'Azienda in forza di un contratto di prestazione di servizi, i relativi incarichi sono perfezionati mediante apposito contratto - contenente tutti gli elementi *ex* art. 28 del GDPR sopra richiamato – predisposto a cura delle competenti Unità Operative aziendali (UOC Approvvigionamento di Beni, Servizi e Logistica/UOC Servizio Tecnico e Manutenzioni/UOC Fisica Medica e Tecnologie Biomediche/UOC *Information Communication Technology*). In proposito si evidenzia che è stato elaborato – mediante il supporto del DPO – un modello di contratto da utilizzarsi a tali fini.

3.4 - Il Responsabile della Protezione dei Dati (DPO) *ex* artt. 37-39 del GDPR

Il GDPR, ai sensi dell'art. 37, comma 1, lett. a), prevede l'obbligo per il Titolare o il Responsabile del trattamento di designare il *Data Protection Officer* "quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali".

Al fine di dare attuazione alle disposizioni di cui al GDPR onde assicurare lo svolgimento delle funzioni e dei compiti stabiliti dagli artt. 38 e 39, l'Azienda - con determina DG 449/2018 - ha provveduto a designare quale *Data Protection Officer* un professionista interno; ciò nella logica di promuovere forme di valorizzazione e crescita del personale, intese come incremento delle conoscenze, delle capacità e dello sviluppo professionale.

Il *Data Protection Officer* costituisce il punto di contatto tra il Titolare che lo ha designato e l'Autorità Garante *Privacy*, con la quale deve cooperare per tutte le questioni connesse al trattamento dei dati personali, consultandola anche preventivamente quando necessario.

Il *Data Protection Officer*, comunque tenuto al rispetto delle norme in materia di segreto o riservatezza, deve in ogni modo facilitare l'accesso, da parte dell'Autorità Garante, ai documenti e alle informazioni necessarie per l'adempimento dei suoi compiti istituzionali, compresi quelli finalizzati all'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi.

Il GDPR, all'art. 39, elenca quali compiti del *Data Protection Officer* almeno i seguenti:

a) 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 GDPR nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del 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, tra le quali sono da ricomprendere l'attribuzione delle diverse responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, qualora venga richiesto, un parere relativamente alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;

d) cooperare con l'Autorità di controllo;

e) fungere da punto di contatto per l'Autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 del GDPR stesso ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Il *Data Protection Officer* deve svolgere le sue funzioni valutando debitamente i rischi inerenti ai diversi trattamenti di dati personali, tenendo conto della loro natura, contesto, ambito di applicazione e finalità, definendo un ordine di priorità nell'attività svolta e concentrandosi sulle questioni che paiono presentare maggiori rischi in termini di protezione dei dati.

Per poter svolgere i compiti assegnatigli dal GDPR il *Data Protection Officer* può legittimamente accedere a tutte le informazioni necessarie ad individuare i trattamenti svolti per conto del

Titolare o del Responsabile al fine di effettuare una analisi e verifica dei trattamenti in termini di loro conformità e eventuale necessità di rettifica.
Il Titolare del trattamento deve fornire al *Data Protection Officer* le risorse necessarie per assolvere i compiti assegnati, comprese quelle necessarie ad aggiornare e mantenere la propria conoscenza specialistica, oltre al supporto attivo da parte delle diverse articolazioni aziendali e un tempo sufficiente per l'espletamento dei compiti sopra descritti.
Assicurare le risorse necessarie significa anche fornire al *Data Protection Officer* un supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale. A tale proposito, in considerazione delle dimensioni e della struttura dell'Azienda, sempre con la richiamata determina DG 449/2018, è stato costituito un Gruppo di lavoro multidisciplinare a supporto del DPO (Comitato *Data Protection)*.
Occorre, infine, che il *Data Protection Officer* non svolga contemporaneamente altri compiti che possano generare tale conflitto, quali, ad esempio, l'assunzione in Azienda di ruoli manageriali di vertice o posizioni gerarchicamente inferiori qualora queste comportino la determinazione di finalità o mezzi del trattamento.

3.5 - Incaricati del trattamento

Sono "Incaricati" tutti coloro che operano quali persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o dei Responsabili e rientrano nella previsione di cui all'art. 4, n. 10, e dell'art. 29 del GDPR.
Gli Incaricati sono formalmente nominati, collaborano con il proprio Responsabile e trattano dati esclusivamente per scopi istituzionali nello spirito della legge e secondo le istruzioni ricevute. Nello svolgimento delle proprie mansioni l'Incaricato rispetta il segreto d'ufficio e professionale, oltreché i requisiti di riservatezza e sicurezza durante le operazioni di trattamento di dati personali.

MISURE/AZIONI DA ATTUARE

(codice misura G)

Gli Incaricati sono designati formalmente dai rispettivi Responsabili del trattamento secondo specifiche modalità individuate nell'atto di nomina dei Responsabili medesimi.

3.6 – Altre figure del modello di *Data Protection Governance* aziendale

Nel presente paragrafo si delinea un inquadramento di ulteriori figure che - sebbene non contemplate dal legislatore Europeo e dalle disposizioni attuative di livello nazionale - vengono a rivestire ruoli importanti nell'ambito dell'organizzazione aziendale in relazione alle specifiche funzioni e mansioni svolte.

Comitato *Data Protection*/Gruppo multidisciplinare di supporto al Responsabile della Protezione dei Dati

A supporto delle attività proprie del DPO è stato costituito – con determina DG 449/2018 - apposito Gruppo multidisciplinare con competenze medico/sanitarie, tecnico/informatiche e giuridico/legali.

In sede di formalizzazione del Regolamento aziendale Privacy verranno declinate le specifiche funzioni del predetto Comitato.

Il Responsabile per la transizione al digitale (RTD) ed il Responsabile della sicurezza informatica

Si richiamano in tale contesto i compiti attribuiti al Responsabile per la transizione al digitale di cui all'art. 17 del D.Lgs. 82/2005 e ss.mm.ii. (Codice dell'Amministrazione Digitale) e, tra questi, quelli indicati alla lettera c) ossia *"indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1"*, per il necessario coordinamento con le attività e compiti propri del DPO, coinvolgenti anche gli aspetti attinenti, appunto, la sicurezza del trattamento dei dati personali. Infatti, tale attività deve essere garantita nel rispetto dei paradigmi di *privacy by design e privacy by default* previsti dal GDPR e sulla conformità ad essi il DPO è tenuto a svolgere una specifica attività di vigilanza.

Si dà evidenza che in ambito aziendale il ruolo di RTD è stato formalmente assegnato - con determina DG 265/2018 - al Direttore della UOC Servizio Informatico.

Nell'ambito del sistema di *Data Protection Governance Aziendale* lo stesso Responsabile del Servizio Informatico/RTD è, quindi, Responsabile della sicurezza informatica al fine di:

- assicurare il sistema di autenticazione alla rete aziendale;
- assicurare i sistemi di autenticazione/autorizzazione ai sistemi informativi di settore;
- curare la protezione della rete telematica aziendale;
- individuare l'elenco degli amministratori di sistema dei quali definisce i compiti e le misure per la registrazione e la conservazione delle attività svolte, ad eccezione dei trattamenti affidati ad un Responsabile del trattamento per i quali provvede quest'ultimo;
- elaborare e rendere disponibili misure di sicurezza a protezione della riservatezza, disponibilità e integrità delle banche dati aziendali, tra le quali: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative adottate;
- fornire, per gli ambiti di specifica competenza, il necessario supporto e collaborazione al Titolare, ai Responsabili del Trattamento ed al DPO.

Amministratori di Sistema

Sul punto si richiama il Provvedimento del Garante del 27 novembre 2008 laddove vengono definiti "amministratori di sistema" le *figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti (…) vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.*

Gli amministratori di sistema così ampiamente individuati (…) nelle loro consuete attività sono, in molti casi, concretamente responsabili di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

Sempre lo stesso provvedimento indica le caratteristiche soggettive di tale figura precisando che l'attribuzione delle corrispondenti funzioni debba avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato; quest'ultimo deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

E' previsto, altresì, che la designazione quale amministratore di sistema debba essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

MISURE/AZIONI DA ATTUARE

(codice misura H)

Gli estremi identificativi delle persone fisiche amministratori di sistema, unitamente all'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte delle autorità di controllo, predisposto a cura delle Unità Operative Servizio Informatico/RTD e Fisica Medica e Tecnologie Biomediche/*Information Communication Technology*, ambiti organizzativi presso i quali sono formalmente riconducibili le predette funzioni.

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di una attività di verifica da parte dei Responsabili delle suddette Unità Operative, in modo da accertarne la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti di dati personali previste dalle norme vigenti.

Referenti Privacy di struttura

Un ruolo altrettanto fondamentale è rappresentato da unità di personale che all'interno di ogni struttura/servizio dell'articolazione organizzativa aziendale svolgono la funzione di punto di raccordo per le questioni attinenti la protezione dei dati.

Il modello di *Data Protection Governance* aziendale prevede, appunto, l'individuazione – nell'ambito di ciascuna Struttura/Servizio/Ufficio – di un Referente *privacy* onde assicurare un presidio coordinato delle operazioni di trattamento sulla base di una corretta circolazione di

flussi informativi tra tutti i soggetti coinvolti (Titolare, Responsabili, DPO, Servizio Informatico/RTD, ecc.).
In caso di mancata designazione, il ruolo di Referente *Privacy* si intende assunto dallo stesso Responsabile di Struttura/Servizio/Ufficio.

3.7 - Informative e consenso

3.7.1 - Informativa *ex* art. 13 del GDPR

Con l'entrata in vigore del GDPR, l'informativa per il trattamento dei dati personali e sensibili risulta essere ampliata rispetto a quella prevista dal previgente Codice *privacy*.
Resta invariato l'obbligo di fornire l'informativa prima della raccolta dei dati, se raccolti direttamente presso l'interessato, specificando l'identità del Titolare del trattamento, la finalità, i destinatari dei dati, i diritti degli interessati; se i dati non sono raccolti direttamente presso l'interessato vanno indicate anche le categorie dei dati oggetto del trattamento.
Il GDPR pone rilevanza su alcune caratteristiche indispensabili dell'informativa quali la chiarezza, la trasparenza e la facilità di comprensione da parte dell'interessato, ottenute anche attraverso l'utilizzo di icone - da abbinare comunque sempre al testo esteso - che dovranno essere identiche in tutta la UE e che verranno definite prossimamente dalla Commissione Europea; per i minori fino a 16 anni va prevista un'informativa con un linguaggio ancor più semplice e chiaro adatto alla loro comprensione.
L'informativa va data preferibilmente per iscritto e in formato elettronico, anche se è ammesso il formato orale.
L'Azienda, in sintesi, deve fornire all'interessato le seguenti informazioni minime:

- L'identità e i dati di contatto del Titolare del trattamento
- I dati di contatto del *Data Protection Officer* (DPO)
- Le finalità del trattamento
- I destinatari o le categorie di destinatari dei dati personali
- L'intenzione del Titolare di trasferire i dati raccolti a un paese terzo
- Il periodo di conservazione dei dati personali raccolti
- I diritti dell'interessato relativamente ai propri dati (accesso, rettifica, cancellazione, portabilità, limitazione del trattamento)
- Il diritto per l'interessato di presentare reclamo all'autorità di controllo
- Le conseguenze del mancato conferimento dei dati personali
- L'esistenza di un processo di profilazione, la logica del processo e le conseguenze del trattamento per l'interessato.

L'informativa deve elencare quali trattamenti di dati vengono effettuati nella struttura e specificare per quali di essi è necessario il consenso dell'interessato o del tutore nei casi previsti (ad esempio non è necessario per il trattamento dei dati ai fini amministrativi o richiesto dalle istituzioni).

Le strutture sanitarie trattano, infatti, svariate tipologie di dati personali e sensibili, e in molti casi anche dati definiti "super-sensibili" come quelli sulla sieropositività, sulla dipendenza da alcool o droghe, su violenze subite ecc.; e ancora, dati genetici, dati relativi alla donazione di organi, per fini di ricerca, per campagne di prevenzione, marketing, comunicazione a case farmaceutiche, dati biometrici in caso di raccolta firma grafometrica ecc...

Sulla base di quanto sopra l'Azienda ha provveduto, nell'immediatezza, ad adeguare l'Informativa generale sul trattamento dati alle richiamate disposizioni di cui all'art. 13 del GDPR, pubblicata sul sito *web* istituzionale alla Sezione Privacy e opportunamente diffusa negli ambiti organizzativi interessati. La stessa potrà, comunque, essere suscettibile di eventuali modifiche/integrazioni a seguito degli esiti delle attività di analisi contemplate nell'area *Data Inventory*.

3.7.2 – Consenso al trattamento dei dati personali

Ai sensi dell'art. 4, n. 11, del GDPR il "consenso dell'interessato" è definito come *qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.*

In tal senso, l'Azienda ha operato la scelta di provvedere all'acquisizione del consenso mediante dichiarazione scritta, fornendo alle strutture/servizi interessati apposita modulistica e relative indicazioni operative (anche in ragione di particolari casistiche); tale modulistica è stata, altresì, pubblicata sul sito *web* istituzionale, alla Sezione *Privacy*.

MISURE/AZIONI DA ATTUARE

(codice misura I)

Peraltro, si dà evidenza che sono in fase di valutazione ulteriori soluzioni organizzative per l'acquisizione e gestione del consenso al trattamento dei dati personali mediante modalità semplificate e che, al contempo, ne garantiscano la piena efficacia.

3.8 - I diritti dell'Interessato

Il GDPR - rispetto al precedente quadro normativo - centralizza ulteriormente il ruolo dell'Interessato, quale persona fisica cui si riferiscono i dati personali e che deve essere messa nelle condizioni di averne il controllo. L'insieme dei diritti contemplato dal GDPR consente, infatti, a tutti i soggetti interessati - previa presentazione di specifica richiesta al Titolare - di verificare e assicurarsi che i propri dati personali non vengano utilizzati in maniera non corretta o comunque per finalità diverse dallo scopo legittimo per cui sono stati inizialmente conferiti all'Azienda.

Il Titolare del trattamento, essendo tenuto a soddisfare le richieste dell'Interessato circa l'esercizio dei suoi diritti, è tenuto quindi adottare tutte le necessarie misure e procedure atte a consentire di fornire all'interessato le informazioni richieste in relazione al diritto attivato.

Tali informazioni devono essere fornite "senza ingiustificato ritardo" e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa; termine prorogabile di ulteriori due mesi in casi di particolare necessità. La risposta da fornire all'interessato non deve essere solo intelligibile, ma anche coincisa, trasparente e facilmente accessibile, oltre ad utilizzare un linguaggio semplice e chiaro. L'esercizio dei diritti dell'interessato è in linea di principio gratuito, ma possono esservi delle eccezioni in caso di richieste manifestamente infondate o eccessive. In tali casi il Titolare è tenuto a valutare la complessità del riscontro all'Interessato e a stabilire, quindi, l'ammontare dell'eventuale contributo da versare a carico dell'Interessato stesso.

Tutte le tipologie di diritti dell'Interessato – alcuni già previsti dal precedente quadro normativo, altri di nuova introduzione – sono contemplate dal GDPR nell'ambito del Capo Terzo, dall'art. 12 all'art. 22.

Qui di seguito si riporta una rappresentazione sintetica dei diritti esercitabili dall'Interessato sulla base del GDPR, con indicazione dei rispettivi articoli e considerando di riferimento.

Diritto di Informazione (artt. 12,13,14 e considerando 58,60): sulla base del principio di correttezza e trasparenza, l'Interessato ha il diritto di ricevere precise informazioni sul trattamento dati in Azienda, espressamente elencate all'art. 13.

Diritto di accesso (art. 15 e considerando 63): L'Interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati che lo riguardano e, in tal caso, di vedere o visualizzare i propri dati personali nonché di ottenerne copia degli stessi.

Diritto di rettifica (art. 16 e considerando 65): L'Interessato può rivolgersi al Titolare per ottenere la rettifica dei dati personali inesatti che lo riguardano. Tenuto conto delle finalità del trattamento, ha anche il diritto di ottenere l'integrazione dei dati incompleti, eventualmente fornendo una dichiarazione integrativa. Trattasi di un diritto che consente all'Interessato di mantenere un controllo attivo sui propri dati evitando, così, che il loro uso possa generare pregiudizio all'interessato medesimo.

Diritto alla cancellazione ovvero diritto all'oblio (art. 17 e considerando 65,66): Tale diritto si configura come un diritto dell'Interessato alla cancellazione dei propri dati personali - in forma rafforzata – al sussistere di determinati motivi espressamente elencati all'art. 17 del GDPR. Il Titolare, nel caso in cui abbia anche reso pubblici i dati dell'interessato, è tenuto ad informare della richiesta di cancellazione gli altri titolari che stiano trattando i dati stessi.

Diritto alla limitazione (art. 18 e considerando 67): Si tratta di un diritto diverso e più esteso rispetto al "blocco" del trattamento di cui al previgente quadro normativo. In particolare, è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche se l'Interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del Titolare) o si oppone al loro trattamento ai sensi dell'art. 21 del GDPR (in attesa di valutazione da parte del Titolare).

Diritto alla portabilità (art. 20 e considerando 68): Si tratta di un diritto nuovo contemplato dal GDPR. Non si applica ai trattamenti non automatizzati (quali archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio. In particolare, sono portabili solamente i dati trattati con il consenso dell'Interessato o sulla base di un contratto stipulato con l'Interessato. Inoltre, il Titolare deve essere in grado di trasferire direttamente i dati portabili ad altro Titolare indicato dall'Interessato, qualora tecnicamente possibile.
È utile sottolineare che il diritto si applica ai dati personali forniti al Titolare, non a quelli generati da quest'ultimo.
Diritto di opposizione (art. 21 e considerando 69,70): Tale diritto consiste nella facoltà per l'Interessato di opporsi in qualsiasi momento, e per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano. Conseguenza dell'esercizio di tale diritto è l'obbligo, in capo al Titolare, di astenersi dal trattamento dei dati. Questo particolare diritto riguarda però situazioni in cui il Titolare stia lecitamente trattando dei dati personali: pertanto, è riconosciuta la facoltà per il Titolare di dimostrare che i suoi interessi specifici connessi al trattamento prevalgono su quelli evidenziati dall'interessato.
MISURE/AZIONI DA ATTUARE
(codice misura L)
L'Azienda ricondurrà la disciplina interna sull'esercizio dei diritti dell'Interessato, secondo i termini rappresentati, nell'ambito del Regolamento aziendale *privacy*.

3.9 - Sistema documentale per la *Data Protection*
Nel presente paragrafo e nei seguenti si riportano le principali indicazioni necessarie per la verifica di adeguatezza, in termini di completezza ed aggiornamento, del sistema documentale *privacy* che l'Azienda si trova a dover gestire per ottemperare agli adempimenti previsti dalla normativa in materia di protezione dei dati personali.
Di seguito vengono delineati i ruoli e le responsabilità delle figure coinvolte nelle attività di tenuta, verifica ed aggiornamento del sistema documentale *privacy*.

Il DPO e il Gruppo multidisciplinare di supporto/Comitato *Data Protection* devono contribuire a:

- mantenere aggiornato l'intero sistema documentale, quali, informative, modulistica, regolamenti, linee guida, registri, ecc.;
- tenuta di verbali o altri documenti emessi e/o ricevuti nell'ambito della cooperazione con l'Autorità di controllo per le questioni connesse al trattamento anche ai fini della relativa archiviazione all'interno del sistema documentale;
- inviare la documentazione aggiornata al Titolare ai fini della conseguente formalizzazione;
- supportare il Titolare del trattamento per le seguenti attività:

a) verificare ed approvare *report*, verbali di *audit*, il Registro del Trattamento ex art.30 del GDPR, e altra documentazione che attenga il sistema di governo della *privacy* all'interno dell'Azienda;

b) approvare gli aggiornamenti del sistema documentale;

c) approvare procedure, linee guida e *policy* attinenti alla protezione dei dati personali in Azienda.

I Responsabili del trattamento devono contribuire a:

- comunicare al DPO le modifiche relative alle attività di trattamento nonché gli eventuali mutamenti organizzativi e tecnici avvenuti all'interno della propria area di responsabilità;
- compilare ed aggiornare, per il tramite degli Incaricati e/o dei Referenti *Privacy* di Struttura/Servizio/Ufficio, il Registro delle attività di trattamento del Responsabile.

3.9.1 – Strutturazione e aggiornamento del sistema documentale *privacy* – modalità di gestione

Con riferimento al sistema documentale *privacy* da implementare in Azienda, si riporta di seguito una griglia rappresentativa della struttura base di un albero documentale in materia di *privacy*.

AREA	**DESCRIZIONE**
Documenti strategici, di indirizzo e di normazione interna	*Procedure, policy, linee guida operative che disciplinano il sistema di governo dei dati personali, Regolamento*
Registro dei trattamenti	*Censimento dei trattamenti, ambito del trattamento consentito, processi operativi, flussi di dati, ecc.*
Registro degli strumenti elettronici di trattamento	- *Mappa dell'infrastruttura tecnologica* - *Topologia di rete* - *Elenco delle applicazioni* - *Elenco dei server e dei sistemi operativi* - *Elenco dei data base*
Analisi dei rischi e degli impatti	- *Reportistica delle analisi dei rischi sui trattamenti di dati personali* - *Reportistica delle valutazioni di impatto per i trattamenti di dati personali che presentano un rischio elevato*
Ruoli e responsabilità	- *Modello organizzativo privacy* - *Atti di nomina e designazione*

	- *Clausole contrattuali*
Misure di sicurezza	- *Documenti di regolamentazione (policy, regolamenti, procedure, istruzioni operative, codici di condotta, ecc.)* - *Misure di sicurezza tecniche (policy tecniche, standard di riferimento, certificazioni tecniche)* - *Misure da provvedimenti specifici e generali del Garante, del Ministero della Salute, della Regione o di altre P.A. di riferimento*
Informative e consensi	*Pazienti in cura, dipendenti, visitatori, familiari, consulenti, fornitori, altri*
Registro delle violazioni di sicurezza	*Registro di tutte le violazioni di sicurezza, valutate a rischio alto, notificate all'Autorità Garante o agli interessati del trattamento*
Esercizio dei diritti degli interessati del trattamento	*Registro delle richieste degli interessati del trattamento in relazione all'esercizio dei diritti (limitazione, opposizione, cancellazione, accesso, rettifica, portabilità)*
Autorità Garante	*Notificazioni, verbali ispezioni, richieste autorizzazioni, consultazioni*
Rapporti di audit	*Rapporti di audit, report periodico sulla conformità agli adempimenti privacy, flussi informativi da/verso il DPO*
Comunicazione e formazione	*Comunicazioni interne, corsi di formazione, evidenze della formazione*

Il sistema di gestione documentale *privacy* deve essere continuamente alimentato in virtù di novità originate da cambiamenti organizzativi o gestionali, dell'adozione di nuovi dispositivi o di nuove tecnologie, a fronte di novità normative, abrogazione di disposizioni legislative e provvedimenti dell'Autorità di controllo.

3.10 - Attività di monitoraggio

A) Come già trattato nell'apposito paragrafo del presente documento, il DPO ha il compito di assistere il Titolare e i Responsabili del trattamento nel controllo dell'effettivo funzionamento dei presidi posti in essere al fine di garantire la protezione dei dati personali.

Il DPO, dunque, assume un ruolo di vigilanza sull'effettivo rispetto delle disposizioni contenute nel GDPR e di quella ulteriore specifica eventualmente vigente per il settore di riferimento.

Nell'ambito della continua attività di monitoraggio circa la corretta applicazione del GDPR, il DPO svolge, in particolare, le seguenti mansioni:

• indirizza e coordina le attività in materia di protezione dei dati personali;

• controlla che le violazioni dei dati personali siano documentate, notificate e comunicate internamente;

• assume (con il Titolare) il compito di punto di contatto per l'autorità di controllo relativamente a questioni connesse al trattamento e, se del caso, consulta l'autorità di controllo di propria iniziativa nel caso in cui sia necessario sottoporre quesiti o istanze di verifica;

• interagisce con le figure a presidio tecnico e fisico in materia di protezione dei dati personali.

Compito del DPO è, altresì, quello di segnalare al Titolare del trattamento, per gli opportuni provvedimenti, quelle violazioni accertate che possano comportare l'insorgere di una responsabilità in capo all'Azienda per non conformità al Regolamento.

Il rapporto con gli organi apicali deve essere su base continuativa: il DPO è tenuto, pertanto, ad instaurare flussi informativi, con cadenza regolare, verso la Direzione aziendale.

A titolo meramente esemplificativo e non esaustivo, il flusso informativo dal DPO verso il Titolare può avere ad oggetto:

• informazioni dettagliate sul livello di adeguatezza della sicurezza e della capacità di prevenzione di trattamenti in violazione del Regolamento;

• evidenze di ipotesi di trattamento a "rischio elevato" (ad es. introduzione di sistemi di trattamento di categorie particolari di dati di soggetti particolarmente vulnerabili, carenza di efficacia di misure a fronte di intervenuti cambiamenti organizzativi o tecnici, ecc.);

• istanze da presentare all'Autorità di controllo;

• ispezioni in loco da parte dell'Autorità di controllo;

• particolari criticità attinenti la protezione dei dati personali, nell'ottica del principio di *accountability*, emerse a seguito di segnalazioni esterne o interne all'organizzazione aziendale.

B) Partecipano all'attività di monitoraggio tutti i soggetti/ruoli individuati nell'ambito del sistema di *Data Protection Governance* aziendale - ognuno per lo specifico ambito di competenza – come di seguito riepilogati:

- Il Gruppo multidisciplinare di supporto al DPO;
- Il Responsabile della sicurezza informatica;
- I Responsabili del Trattamento;
- I Referenti Privacy di Struttura;
- Gli Amministratori di Sistema.

A titolo meramente esemplificativo e non esaustivo, il flusso informativo verso il DPO da parte dei soggetti interessati nel sistema di *governance* in materia di *data protection* avrà ad oggetto:

- segnalazioni della introduzione di nuove tecnologie;
- segnalazioni di ipotesi violazioni interne da parte del personale dipendente;
- reportistica relativa a verifiche attinenti alle procedure di governo delle aree/direzioni di riferimento (reparti, uffici, laboratori, sale di accesso al pubblico ecc.);
- criticità nella protezione dei dati emerse nelle relazioni con pazienti, dipendenti o fornitori;
- istanze pervenute da parte dei pazienti;
- carenze di efficacia del sistema di contrasto e mitigazione del rischio registrate a fronte di *audit* svolti;
- qualunque comunicazione ricevuta/inviata dalla Autorità di controllo.

3.11 – *Data Breach ex* art. 33 del GDPR

3.11.1 - Processo di *Data Breach management*

I dati personali conservati, trasmessi o trattati dall'Azienda possono essere soggetti al rischio di perdita, distruzione o diffusione indebita (ad esempio a seguito di attacchi informatici), accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità. Si tratta di situazioni che possono comportare pericoli significativi per la *privacy* degli interessati cui si riferiscono i dati.

Il GDPR prevede l'obbligo di notifica all'autorità di vigilanza in caso di violazione dei dati personali nonché la definizione di altri requisiti per l'eventuale ulteriore comunicazione ai soggetti interessati.

Tale obbligo non risulta del tutto nuovo, in quanto il Garante per la protezione dei dati personali aveva già adottato in anni recenti una serie di provvedimenti che introducono, per determinati settori, l'obbligo di comunicare eventuali violazioni di dati personali (c.d. *data breach*) all'Autorità stessa e, in alcuni casi, anche ai soggetti interessati, pena l'applicazione di sanzioni amministrative.

In particolare, si segnala il Provvedimento del Garante privacy n. 331 del 4 giugno 2015 in tema di dossier sanitario elettronico.

Il fondamento della previsione della notifica all'Autorità di controllo - prevista dall'art. 33 del GDPR - si rinviene nella volontà di affrontare e gestire nell'immediatezza una violazione al fine di evitare l'insorgenza o l'aggravamento di danni materiali o immateriali alle persone interessate (perdita di controllo de dati, limitazione dei diritti dell'Interessato, discriminazione, furto o usurpazione dell'identità, perdite finanziarie ecc.).

Il Titolare del trattamento deve notificare all'Autorità di controllo una violazione di cui è venuto a conoscenza appena possibile e comunque entro 72 ore da quando ha avuto cognizione dell'accaduto. Tale notifica non è obbligatoria se il Titolare abbia valutato che sia improbabile

che la violazione dei dati personali di cui è venuto a conoscenza presenti un rischio per i diritti e le libertà delle persone fisiche.

La notifica tardiva (dopo 72 ore dall'avvenuta conoscenza della violazione) è ammessa dal GDPR che però richiede al Titolare l'onere di indicare esattamente i motivi del ritardo. Altresì, qualora non sia possibile per il Titolare fornire tutte le informazioni utili contestualmente alla prima segnalazione della violazione, il GDPR consente allo stesso di fornirle in fasi successive senza ulteriore ingiustificato ritardo.

Il contenuto della notifica è indicato espressamente dal GDPR – sempre nel richiamato art. 33 - che richiede la descrizione:

- della natura della violazione dei dati personali, categorie, numero di interessati; occorrerà dettagliare e circostanziare quanto più possibile la violazione rilevata (ad es. indicare quando è avvenuta se si ha contezza della data precisa o se sia ancora in corso di svolgimento, dove si è verificata nel caso di smarrimento o furto di dispositivi);
- dell'identità del Responsabile della protezione dei dati (DPO) o di un altro punto di contatto (è opportuno indicare riferimenti utili per una effettiva e tempestiva reperibilità quali *mail*/pec, recapiti telefonici, sede ecc.)
- delle conseguenze della violazione (possibili danni stimati in termini di probabilità);
- delle misure proposte o adottate dal Titolare per porne rimedio.

Infine, il Titolare del trattamento deve essere in grado di documentare qualsiasi violazione dei dati personali, comprese le suindicate circostanze ad essa relative, oltreché le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione deve consentire all'Autorità di controllo di verificare il rispetto delle prescrizioni previste nel GDPR.

Oltre alle necessarie notifiche, è fondamentale che venga riconsiderata la capacità complessiva da parte dell'Azienda di trattare e conservare in modo sicuro tutte le informazioni in suo possesso.

Pertanto, dal punto di vista organizzativo, occorrerà porre particolare attenzione su eventuali:

- *"eccedenza di trattamento"*, ovvero dati inutilmente raccolti e memorizzati;
- *"conservazione oltre limite"*, quando i dati sono conservati per più tempo di quanto sia necessario;
- *"utilizzi impropri" di dati personali (*ossia per scopi diversi da quelli per cui sono stati raccolti).

La combinazione di probabilità e gravità consente di stimare il potenziale rischio per i diritti e le libertà delle persone fisiche, e così valutare se procedere o meno con la notificazione all'Autorità Garante e/o agli interessati coinvolti.

MISURE/AZIONI DA ATTUARE

(codice misura M)

L'Azienda ricondurrà la disciplina interna sul *data breach*, secondo i termini rappresentati, nell'ambito del Regolamento aziendale *privacy*.

3.11.2 - Comunicazioni al soggetto Interessato

Relativamente alla notifica verso gli interessati – disciplinata dall'art. 34 del GDPR - il Titolare deve notificare la violazione anche all'interessato i cui dati personali sono stati oggetto della violazione rilevata senza ingiustificato ritardo e in modo chiaro solo in un caso: qualora la violazione dei dati rischi di pregiudicare i diritti e le libertà dell'interessato.

Le ragioni di tale comunicazione si rinvengono nel fatto che, in caso di eventuali pregiudizi, il soggetto Interessato deve essere posto nelle condizioni di prendere le precauzioni necessarie.

La comunicazione, invece, non è dovuta al ricorrere di una delle seguenti condizioni:

- quando il Titolare ha messo in atto adeguate misure tecniche e organizzative di protezione e tali misure sono state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- quando il Titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà dell'Interessato;
- detta comunicazione richiederebbe sforzi sproporzionati. In tal caso si procede ad una comunicazione pubblica o ad una misura simile, tramite la quale gli interessati vengono informati con analoga efficacia.

4 – Modello di *governance e* piano di adeguamento: Misure tecniche e applicative

Sempre secondo i principi della protezione dei dati *by design* e *by default* di cui all'art. 25 del GDPR, nella quarta area di attività trattasi di descrivere e attuare misure tecniche adeguate per garantire un livello di sicurezza adeguato al rischio. Tali misure comprendono, tra le altre, la pseudonimizzazione e la cifratura dei dati personali, la minimizzazione, la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico, una procedura per testare, verificare, valutare regolarmente l'efficacia delle misure al fine di garantire la sicurezza del trattamento (*ex* artt. 25 e 32 del GDPR).

Appare utile richiamare testualmente in tale sede il provvedimento del Garante Privacy Italiano "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015" (sezione 2.2, allegato 2), ove sono riportate talune indicazioni sulle modalità di selezione dei dati oggetto di interscambio:

"*La selezione delle informazioni personali oggetto di accesso deve avvenire nel rispetto dei principi di pertinenza e non eccedenza in relazione a ciascuna delle finalità perseguite dal fruitore. Rispetto ad una medesima banca dati devono essere, infatti, prefigurati diversi livelli e modalità di accesso che offrano al fruitore unicamente i dati necessari per le proprie esigenze istituzionali.*

Le modalità di accesso alle banche dati devono essere, pertanto, configurate offrendo un livello minimo di accesso ai dati, anche limitando i risultati delle interrogazioni a valori di tipo booleano (ad es., web services che forniscono un risultato di tipo vero/falso nel caso di controlli sull'esistenza o sulla correttezza di un dato oggetto di autocertificazione). Livelli di accesso gradualmente più ampi possono essere autorizzati soltanto a fronte di documentate esigenze del fruitore da indicare in convenzione.

È chiaro, inoltre, che per ciascun fruitore possono essere individuate più modalità di accesso ad una medesima banca dati in relazione alle diverse funzioni svolte dai propri operatori per il perseguimento della medesima finalità, modulando così il livello di accesso ai dati. L'erogatore deve, infatti, far sì che sia consentita, per quanto più possibile, la segmentazione dei dati visualizzabili al fine di rendere consultabili dall'utente, anche in base al proprio profilo e in relazione al bacino di utenza del fruitore, esclusivamente i dati necessari rispetto alle finalità in concreto perseguite. In altri termini la convenzione deve prevedere l'accesso alle sole informazioni pertinenti e non eccedenti rispetto alla finalità istituzionale perseguita dalla convenzione stessa.

Particolare attenzione deve essere prestata, inoltre, nella scelta delle informazioni richieste per l'interrogazione diretta della banca dati, ovvero per l'invocazione dei web services, imponendo

un set minimo di dati per l'individuazione puntuale del soggetto cui si riferiscono. Salvo eccezioni rigorosamente motivate e documentate nella convenzione, la risposta fornita all'interrogazione non deve, poi, contenere un elenco di soggetti".

Tra le misure tecnologiche da porre in essere occorre anche tenere in considerazione le misure minime di sicurezza Agid, di cui alla Circolare 18 aprile 2017, n. 2, destinate alla Pubblica Amministrazione al fine di contrastare le minacce più comuni.
Agid, facendo riferimento al modello CIS *Critical Security Controls for Effective Cyber Defense* predisposto da *Sans Istitute* nel 2015, ha creato un set di controlli di verifica sulle prime 5 aree di rischio previste dal modello *Sans*-20 (le aree del modello sono per l'appunto 20) che, a parere non solo di Agid, rappresentano l'insieme dei controlli indispensabili per assicurare il minimo livello di protezione nella maggior parte delle situazioni.
Tali controlli, definiti con l'acronimo ABSC (Agid Basic Security Control), riguardano le seguenti aree:

ABSC1 inventario dei dispositivi autorizzati e non autorizzati presenti in rete tramite *discovery* dei dispositivi: implementazione del *logging* dei DHCP, gestione dell'inventario delle risorse in rete registrando almeno l'IP, installazione dell'autenticazione a livello di rete per limitare i dispositivi che possono essere connessi in rete;

ABSC2 inventario dei *software* autorizzati e non autorizzati presenti in rete mediante strumenti automatici di *inventory* non consentendo l'installazione di altri *software* esclusi da tale elenco: implementazione di una *whitelist* dei *software* autorizzati bloccando l'esecuzione dei *software* non inclusi nella *whitelist*, gestire l'inventario del *software*;

ABSC3 protezione delle configurazioni *hardware* e *software* sui dispositivi mobili, *laptot*, *workstation* e *server*: definizione e programmazione di configurazioni standard per *software*, *server* e altri tipi di sistemi, regolare validazione e aggiornamento delle immagini d'installazione che devono essere conservate in modalità protetta, esecuzione delle operazioni di amministrazione su tutte le tipologie di macchine per mezzo di connessioni protette, utilizzazione di strumenti possibilmente automatici per verificare l'integrità dei file critici di sistema monitorando che non vengano alterati;

ABSC4 valutazione e correzione continua della vulnerabilità: uso di uno SCAP (*Security Content Automation Protocol*) per eseguire la validazione di vulnerabilità, verifica che gli strumenti di scansione delle vulnerabilità siano utilizzati periodicamente, registrazione ad un sistema che fornisca tempestivamente le informazioni su nuove minacce e vulnerabilità;

ABSC5 uso appropriato dei privilegi di amministratore: limitazione dei privilegi di amministratore ai soli utenti che abbiano adeguate competenze, assegnazione delle utenze di amministratore solo con i privilegi necessari per svolgere attività specifiche, *logging* delle azioni compiute dagli amministratori, mantenimento dell'inventario delle utenze di amministratore con *warning* ogni volta venga aggiunta una nuova utenza, tracciatura nei *log* dei tentativi falliti di creazione di nuove utenze di amministratore, conservazione delle credenziali in modo da garantirne disponibilità e riservatezza.

In aggiunta ai primi 5 set di controlli Agid prevede anche i seguenti controlli:

ABSC8 difese contro i malware: Installare su tutti i sistemi connessi in rete di soluzioni antivirus con archiviazione centrale degli eventi rilevati, installazione di *firewall* e IPS personali, limitazione dell'uso di dispositivi esterni a quelli necessari allo svolgimento delle attività aziendali, monitoraggio dei tentativi di utilizzo di dispositivi esterni, utilizzo di sistemi di *content filtering* e *antisapamming*;

ABSC10 Copie di sicurezza: Effettuazione almeno settimanalmente di *backup* che deve riguardare sistema operativo, applicativi e database, verificare periodica delle funzioni e dei risultati delle procedure di *restore*, effettuazione di *backup multipli* per avere certezza di disponibilità di almeno una copia di backup, assicurarsi che almeno una copia del backup non sia permanentemente accessibile dal sistema.

4.1 - Identità e accesso

In coerenza ai principi applicabili al trattamento di dati personali di cui all'art. 5 del GDPR, nonché alle richiamate disposizioni di cui agli artt. 25 e 32 dello stesso GDPR, un controllo di sicurezza che risulta necessario attuare consiste nell'allineare efficacemente le identità e i privilegi di accesso dei propri utenti alle *policy* aziendali.

Infatti, è proprio la *governance* delle identità che consente di ridurre il rischio di compromissione dei dati diventando strumento principale per la loro protezione.

Per cercare di ridurre il rischio di compromissione dei dati, dovranno essere valutate, a cura del Servizio Informatico, adeguate soluzioni di *identity and access management* che consentano di:

- automatizzare i processi di gestione dei ruoli degli utenti, di gestione delle *policy* di accesso e di gestione dei rischi;
- applicare e rafforzare i corretti livelli di accesso per utenti in continuo mutamento;
- certificare regolarmente i diritti di accesso degli utenti con un elevato livello di precisione;
- rilevare e agire rapidamente in base alle violazioni dei criteri di sicurezza;

Pertanto, al fine di verificare l'adeguatezza o meno delle misure adottate, occorre testare i sistemi aziendali con i seguenti quesiti:

- Chi ha accesso e a quali risorse e perché?
- Quando è stato rilasciato l'accesso?
- Esistono rischi connessi con gli attuali diritti di accesso?

Gli utenti devono avere un accesso sicuro e accedere solo ai dati e alle applicazioni di cui hanno realmente necessità e per cui sono stati autorizzati.

Devono essere eseguiti controlli regolari per garantire che tali diritti di accesso e i relativi privilegi non vengano violati.

In tal senso, le soluzioni di *identity and access management* possono aiutare a garantire la sicurezza dei dati sensibili e a mantenere la *compliance* dell'organizzazione al GDPR, possono fornire informazioni preziose sugli *account*, i privilegi e i diritti di accesso della vasta gamma di utenti colmando le lacune della protezione delle identità e contrastando le minacce di usi involontari non corretti e furti intenzionali. È necessario, quindi, raccogliere le informazioni sull'utente e sui suoi privilegi dall'insieme dei sistemi informativi in uso a livello aziendale.

Inoltre, il presente contesto aziendale – tipico degli ambienti sanitari – è caratterizzato anche da una costante modifica ai gruppi di utenti. Pertanto, onde assicurare che i diritti assegnati rimangano attuali e appropriati, occorre, altresì, testare i sistemi aziendali mediante i seguenti quesiti che si indicano a titolo esemplificativo:

Quando viene assunto nuovo personale vengono rilasciate le utenze con i corretti accessi in base ai ruoli e alle responsabilità? Cosa accade quando un dipendente cambia reparto o lascia l'organizzazione? Chi si preoccupa di aggiornare o revocare l'utenza? Si può verificare, in modo proattivo, che i dipendenti non godano di diritti inutili?

L'accumulo dei privilegi di accesso nel tempo è conosciuto come "*enitlement creep*" - ed è un problema in aumento. L'"*Enitlement creep*" crea un aumento esponenziale della complessità della gestione delle identità e aumenta il rischio di compromissione dei dati.

MISURE/AZIONI DA ATTUARE

(codice misura N)

Per quanto attiene la trattazione di soluzioni volte ad attuare specifiche misure tecniche ed applicative nell'ambito delle diverse componenti del Sistema Informativo aziendale, si rinvia ad apposito documento a cura del Servizio Informatico/RTD.

PIANO DI *GOVERNACE* DELLE ATTIVITA' FINALIZZATE ALL'ADEGUAMENTO DELL'ORGANIZZAZIONE AZIENDALE AL REGOLAMENTO EUROPEO 2016/679 (GDPR) IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

CODICE MISURA	AMBITO	ADEMPIMENTI/OBIETTIVI	UNITA'/RUOLO COMPETENTE	TEMPISTICA
A	Data Inventory	Ricognizione delle categorie di dati personali trattati ai fini della strutturazione del Registro delle attività di trattamento (del Titolare)	DPO/Gruppo multidisciplinare di supporto al DPO	Elaborazione documento entro il 30 giugno 2019
B	Data Inventory	Ricognizione delle categorie dei trattamenti ai fini della strutturazione del Registro delle attività di trattamento (del Responsabile)	DPO/Gruppo multidisciplinare di supporto al DPO/ Direzione Medica dei Presidi/Unità di Staff e del Dipartimento Amministrativo/Servizio Informatico/RTD	Elaborazione documento entro il 30 giugno 2019
C	Data Inventory	Tenuta del Registro del Titolare	DPO	Implementazione del Registro a seguito dell'acquisizione del *software* gestionale *privacy* (tempistica gara)
		Tenuta del Registro del Responsabile	Responsabili/Direttori di Unità Operative	Implementazione del Registro a seguito dell'acquisizione del *software* gestionale *privacy* (tempistica gara)
D	Data Inventory	Inventario degli *asset* tecnologici	Servizio Informatico/RTD/ Fisica Medica e Tecnologie Biomediche/*Informa*	Elaborazione documento contenente la mappatura degli *asset* tecnologici

			tion Communication Technology	entro il 30 aprile 2019
E	Analisi dei rischi e degli impatti	Analisi dei rischi e degli impatti per ogni macro processo operativo nel quale vengono trattati dati personali	DPO/Gruppo multidisciplinare di supporto al DPO/ Servizio Informatico/RTD/Direzione Medica dei Presidi/Unità di Staff e del Dipartimento Amministrativo	Elaborazione documento a seguito dell'implementazione del Registro (tempistica di gara per acquisizione *software* gestionale *privacy*)
F	Misure Organizzative	Nomina Responsabili del trattamento	Affari Istituzionali/DPO	Elaborazione proposta di determina entro il 30 aprile 2019
		Notifica atto di nomina a ciascun Responsabile		Notifica entro 15 giorni dall'atto di nomina
		Istruzioni a Responsabili e Incaricati a corredo degli atti di nomina dei Responsabili	Affari Istituzionali e Generali/DPO/Servizio Informatico/RTD	Entro il 30 aprile 2019
G	Misure Organizzative	Designazione Incaricati del trattamento	Responsabili del trattamento	Secondo modalità e termini da definirsi nell'atto di nomina dei Responsabili
H	Misure Organizzative	Identificazione Amministratori di Sistema e relative funzioni	Servizio Informatico/RTD/Fisica Medica e Tecnologie Biomediche/*Information Communication Technology*	Formalizzazione documento entro il 30 aprile 2019
I	Misure Organizzative	Valutazione ulteriori soluzioni organizzative per l'acquisizione e gestione del consenso al trattamento dei dati personali	Affari Istituzionali e Generali/DPO/Gruppo multidisciplinare di supporto al DPO	Secondo modalità e termini da definirsi a livello di tavolo interaziendale
L	Misure Organizzative	Disciplina interna sull'esercizio dei diritti dell'Interessato	Affari Istituzionali e Generali/DPO/Gruppo multidisciplinare di supporto al DPO	Secondo modalità e termini da definirsi

				nell'ambito del Regolamento aziendale *privacy* la cui elaborazione è prevista entro il 31 dicembre 2019
M	Misure Organizzative	Disciplina interna sul *data breach*	Affari Istituzionali e Generali/DPO/Gruppo multidisciplinare di supporto al DPO/Servizio Informatico/RTD	Secondo modalità e termini da definirsi nell'ambito del Regolamento aziendale *privacy* la cui elaborazione è prevista entro il 31 dicembre 2019
N	Misure tecniche ed applicative	Definizione di specifiche misure tecniche ed applicative nell'ambito del Sistema Informativo aziendale	Servizio Informatico/RTD	Elaborazione documento entro il 30 giugno 2019