Istituzione “Cav. Paolo Sartori” – Comune di Valdastico (VI)

PIANO DI PROTEZIONE E MODELLO ORGANIZZATIVO PER LA PROTEZIONE DEI DATI PERSONALI

In applicazione del GDPR 2016/679 e del D.Lgs. 196/2003

Approvato con determinazione del Direttore n. 154 del 27.11.2020

Sommario

PARTE PRIMA: INTRODUZIONE

Articolo 1): PREMESSA DI CARATTERE NORMATIVO

Il presente Piano in materia di protezione dei dati personali (così detta “privacy”) è uno strumento di applicazione del vigente D.lgs. 30 giugno 2003, n. 196 (cosiddetto "Codice sulla privacy” come novellato dal recente D.lgs. 10 agosto 2018 n. 101) e, in particolare, del nuovo Regolamento Europeo n. 2016/679, nell'ambito dell'organizzazione dell’Istituzione “Cav. Paolo Sartori”.

A far data dal 25 maggio 2018 ha trovato diretta ed immediata applicazione, sul territorio nazionale, il nuovo Regolamento Europeo n. 2016/679 (così detto GDPR ossia “*General Data Protection Regulation*”) sulla privacy, approvato il 27 aprile 2016 e pubblicato sulla Gazzetta Ufficiale dell’Unione Europea il 4 maggio 2016.

Ciò ha comportato il superamento delle disposizioni legislative di cui al previgente Codice della privacy (D.lgs. 196/2003), così come delle norme regolamentari emanate negli anni dall’Autorità Garante per la protezione dei dati personali, nella misura in cui le norme nazionali risultino contrastanti o incompatibili con quelle europee.

Il principio cardine, di matrice anglosassone, introdotto dal nuovo Regolamento Europeo è quello della “responsabilizzazione” (*accountability* nell’accezione inglese) che pone in carico al Titolare del trattamento dei dati l’obbligo di attuare politiche adeguate in materia di protezione dei dati, con l’adozione di misure tecniche ed organizzative, anche certificate, che siano concretamente e sempre dimostrabili, oltre che conformi alle disposizioni europee (principio della “conformità” o *compliance* nell’accezione inglese); vi è quindi l’obbligo di porre in essere comportamenti proattivi, tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l’applicazione del Regolamento UE.

Nell’ottica del Legislatore europeo, quindi, in materia di privacy ciascun Titolare può scegliere autonomamente il modello organizzativo e gestionale che ritiene più adatto alla propria realtà e dotarsi delle misure di sicurezza che ritiene più efficaci in quanto Egli risponde delle proprie azioni e deve essere in grado, in qualsiasi momento di darne conto verso l’esterno.

Il presente provvedimento si rende necessario per recepire, in un unico testo, i precetti normativi a maggior rilevanza, sia di carattere aziendale che nazionale in tema di trattamento dei dati personali, al fine darne collocazione sistematica nel contesto di questo ente.

Il presente provvedimento è sottoposto ad aggiornamento periodico, in linea con le novità normative, giurisprudenziali e con le pronunce del Garante per la protezione dei dati personali.

Articolo 2): PREMESSA DI CARATTERE ORGANIZZATIVO

Dall'esame della materia emerge come sia oramai imprescindibile un cambiamento di mentalità che porti alla piena tutela della privacy, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma, soprattutto, come garanzia, per il cittadino-utente che si rivolge alla struttura, di una completa riservatezza sotto il profilo sostanziale.

Il diritto alla privacy costituisce, anche secondo il Legislatore europeo, un vero e proprio diritto inviolabile dell’essere umano, che non si limita alla tutela della riservatezza o alla protezione dei dati, ma implica il pieno rispetto dei diritti e delle libertà fondamentali e della dignità del singolo individuo.

Per questi motivi, la “cultura della privacy” necessita di divenire un vero e proprio elemento cardine dell’organizzazione di questo ente, che deve impegnarsi perché la cultura di cui si tratta possa crescere e rafforzarsi, in quanto solo con la conoscenza minima dei principi fondamentali che stanno alla base della vigente normativa potranno essere adottati correttamente tutti gli adempimenti di carattere tecnico ed organizzativo nel trattamento dei dati di competenza.

PARTE SECONDA: DISPOSIZIONI GENERALI

Articolo 3): OGGETTO DEL PIANO

Il presente Piano disciplina, all'interno dell'Istituzione "Cav. Paolo Sartori", la tutela delle persone in ordine al trattamento dei dati personali, nel rispetto di quanto previsto dal Codice in materia di protezione dei dati personali (Decreto Legislativo del 30/06/2003 n. 196 e ss.mm.ii.) ed in conformità all'emanazione della nuova normativa sovranazionale, il Regolamento UE n. 679 del Parlamento Europeo e del Consiglio del 27/04/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Articolo 4): FINALITÀ DEL PIANO

L'Istituzione "Cav. Paolo Sartori" garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

La protezione delle persone fisiche, con riguardo al trattamento dei dati personali, è un diritto fondamentale. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano (Articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione Europea).

Articolo 5): SENSIBILIZZAZIONE E FORMAZIONE

L'Istituzione "Cav. Paolo Sartori" sostiene e promuove, al suo interno, ogni strumento di sensibilizzazione che possa consolidare il pieno rispetto del diritto alla riservatezza e migliorare la qualità del servizio offerto all'utenza.

A tale riguardo, uno degli strumenti essenziali di sensibilizzazione, anche in materia di privacy, è l'attività formativa del personale e l'attività informativa diretta a tutti coloro che hanno rapporti con l'ente.

L'Istituzione "Cav. Paolo Sartori" organizza, nell'ambito della formazione continua e obbligatoria del personale, specifici interventi di formazione e di aggiornamento in materia di protezione dei dati personali, finalizzati alla conoscenza delle norme, alla prevenzione di fenomeni di abuso e illegalità nell'attuazione della normativa, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni agli interessati.

La formazione in materia di prevenzione dei rischi di violazione dei dati personali viene integrata e coordinata con la formazione in materia di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza, accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera l'Ente.

Articolo 6): DEFINIZIONI

Come stabilito dall'art. 4 del Regolamento Europeo n. 2016/679, ai fini di questo disciplinare si intende per:

a) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può esser identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
b) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione,

l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

c) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
d) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
e) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
f) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
g) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
h) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
i) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
j) «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
k) «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
l) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
m) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
n) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'art. 51 del Regolamento UE.

Quelle sopra riportate, di cui si è data evidenza, rappresentano le "definizioni" su cui ha inciso maggiormente il nuovo Regolamento europeo: per le altre "definizioni" si fa espresso rinvio al testo dell'art. 4 del Regolamento Europeo n. 2016/679 ed al D.lgs. 196/2003.

Articolo 7): PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI

Come stabilito dall'art. 5 del Regolamento Europeo n. 2016/679, i dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'art. 89, paragrafo 1 del Regolamento UE, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»). A tale proposito, il Regolamento UE ricalca i principi sostanziali di "necessità, pertinenza, indispensabilità e non eccedenza" (rispetto alle finalità del trattamento) contenuti nel D.lgs. 196/2003;
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'art. 89, paragrafo 1 del Regolamento UE, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Articolo 8): CONDIZIONI DI LICEITÀ DEL TRATTAMENTO

Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è **necessario all'esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di **misure precontrattuali** adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la **salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'**esecuzione di un compito di interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per il **perseguimento del legittimo interesse del titolare del trattamento o di terzi**, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. Tale condizione non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

Articolo 9): CONDIZIONI PER IL CONSENSO

Per i trattamenti basati sul consenso dell'Interessato, il Titolare del trattamento deve essere in grado di dimostrare che l'Interessato abbia acconsentito al trattamento. In particolare, nel contesto di una dichiarazione scritta relativa a un'altra questione debbono esistere garanzie che assicurino che l'Interessato sia consapevole del fatto di prestare un consenso e della misura in

cui ciò avviene. Risulta opportuno prevedere una dichiarazione di consenso predisposta dal Titolare del trattamento in una forma comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro e non contenga clausole abusive.

Il consenso non viene considerato liberamente prestato se l'Interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio.

Si presume che il consenso non sia stato liberamente prestato se non è possibile prestare un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione.

Articolo 10): TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI

Premesso che l'Istituzione "Cav. Paolo Sartori" gestisce un centro servizi per anziani non autosufficienti e un centro diurno per anziani, il *core business* dell'ente è rappresentato dai servizi socio-assistenziali-sanitari svolti a favore degli ospiti. Al fine di svolgere tali servizi, l'ente necessita di trattare anche dati c.d. "particolari".

Come stabilito dall'art. 9 del Regolamento Europeo n. 2016/679, è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Detta disposizione non si applica, secondo il Regolamento UE, quando incorrono alcune condizioni, riportate al summenzionato art. 9, tra le quali si evidenzia quella di cui alle lettere

- "h", ai sensi della quale "*il trattamento è necessario per finalità di […] diagnosi, assistenza o terapia sanitaria o sociale […]*"
- "g" ai sensi della quale "*il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri […]*".

A tal proposito l'art. 2-sexies del D.lgs. 196/2003 (come novellato dal D.lgs. 101/2018), prevede che "*si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie: […]*

- *s) attività socio-assistenziale a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci;*
- *u) compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario;*
- *v) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale*".

Si fa integrale rinvio all'art. 2-septies del D.lgs. 196/2003 (come novellato dal D.lgs. 101/2018) contenente specifiche disposizioni relative alle "misure di garanzia" per il trattamento dei dati genetici, biometrici e relativi alla salute.

Si richiama inoltre il provvedimento del Garante per la protezione dei dati personali n. 55 del 07.03.2019, ad oggetto "*Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*", il quale specifica che "*Gli eventuali trattamenti attinenti, solo in senso lato, alla cura, ma non strettamente necessari, richiedono, quindi, anche se effettuati da professionisti della sanità, una distinta base giuridica da individuarsi, eventualmente, nel consenso dell'interessato o in un altro presupposto di liceità*".

Articolo 11): DOSSIER SANITARIO ELETTRONICO AZIENDALE

Il Dossier Sanitario Elettronico (abbreviato "D.S.E.") raccoglie l'insieme dei dati personali generati da eventi clinici presenti e trascorsi che riguardano il paziente, messi in condivisione logica al fine di documentarne la storia clinica e di offrirle un migliore processo di cura.

Per poter costituire il Dossier Sanitario Elettronico ed accedere a tutte le informazioni sarà necessario che il paziente rilasci il proprio consenso, dopo aver ricevuto l'apposita nota informativa. In ogni caso l'eventuale mancato consenso al trattamento dei dati personali mediante il Dossier sanitario non inciderà sulla possibilità di accedere alle cure mediche richieste.

Il Dossier sarà consultabile esclusivamente dal personale sanitario della struttura o da altro personale sanitario quando si renda necessaria una specifica consulenza specialistica concordata con l'interessato.

Si richiamano espressamente le "*Linee guida in materia di dossier sanitario*" predisposte dal Garante nell'allegato A alla deliberazione del 04.06.2015.

Articolo 12): TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI (DATI GIUDIZIARI)

Come stabilito dall'art. 10 del Regolamento Europeo n. 2016/679, "*il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza […] deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica*".

Posto quanto sopra, si fa integrale rinvio all'art. 2-octies del D.lgs. 196/2003 (come novellato dal D.lgs. 101/2018) dedicato al trattamento dei dati relativi a condanne penali e reati.

Articolo 13): CIRCOLAZIONE DEI DATI PERSONALI

Fatto salvo il rispetto di specifiche e puntuali disposizioni normative che lo vietino, l'Ente favorisce la circolazione all'interno dei propri uffici dei dati personali dei cittadini il cui trattamento sia necessario ai sensi degli articoli 6, 9 e 10 del GDPR. La circolazione, ove possibile, è assicurata mediante l'accessibilità diretta delle banche dati informative detenute da ciascun ufficio, previa creazione di appositi profili di utenza che tengano conto dei profili di autorizzazione conferiti. Forme similari di accessibilità sono garantite in favore di contitolari e responsabili del trattamento, limitatamente ai dati personali diversi da quelli contemplati dagli articoli 9 e 10 del GDPR.

Articolo 14): COMUNICAZIONE DI DATI VERSO L'ESTERNO

La comunicazione di dati sensibili e giudiziari da parte di un soggetto pubblico ad altro soggetto pubblico è ammessa quando è prevista da una norma di legge o regolamento e comunque quando è ritenuta necessaria per lo svolgimento di funzioni istituzionali, anche a seguito di un bilanciamento degli interessi in gioco.

Articolo 15): INFORMATIVA

Come stabilito dall'art. 13 del Regolamento Europeo n. 2016/679, in caso di raccolta presso l'Interessato di dati che lo riguardano, il Titolare del trattamento fornisce all'Interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

a) l'identità e i dati di contatto del titolare del Trattamento e, ove applicabile, del suo rappresentante;
b) i dati di contatto del Data protection officer (DPO);

c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) qualora il trattamento si basi sull'art. 6, paragrafo 1, lettera f) del Regolamento UE, i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione, nei termini previsti dal Regolamento UE.

In aggiunta alle informazioni di cui sopra, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

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

Ai fini dell'informativa, nell'ambito delle attività dell'Ente si identificano i seguenti ambiti:

a) prestazioni sanitarie, socio-assistenziali ed assimilate;
b) contratto di impegnativa economica;
c) rapporto di lavoro e assimilati;
d) rapporto di prestazione di servizi;
e) informazione generale pubblicata sul sito web;
f) breve informazione da porre in calce alle comunicazioni tramite e-mail.

Articolo 16): PERIODO DI CONSERVAZIONE

Per quanto concerne il periodo di conservazione dei dati personali raccolti da questo ente, i dati verranno conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello strettamente necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

A tale riguardo, il Titolare del trattamento provvederà ad approvare l'elenco della tipologia dei documenti con il rispettivo tempo di conservazione (limitato o illimitato); detto strumento permetterà di gestire in modo organizzato l'archivio aziendale, permettendo di conservare solo ciò che mantiene un rilievo giuridico o ha assunto un valore storico e di eliminare la documentazione non più necessaria.

Qualora il Titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'Interessato informazioni in merito a tale diversa finalità.

Articolo 17): SMALTIMENTO E DISTRUZIONE DEI DOCUMENTI

I principi elencati all'articolo 5 del Regolamento UE prevedono che anche la cancellazione (smaltimento e distruzione) dei documenti che contengono dati personali avvenga secondo il principio di responsabilizzazione del Titolare del trattamento. Tali documenti possono essere sia di tipo elettronico, conservati quindi su archivi informatici (cloud, hard disk, chiavette usb, cd-rom, dvd, …), sia di tipo cartaceo.

Per quanto riguarda la distruzione dei documenti elettronici si richiamano le istruzioni fornite dal Garante per la protezione dei dati personali, in particolare con il provvedimento "*Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali*" del 13 ottobre 2008. Prima di effettuare la distruzione dei supporti si rende comunque opportuno acquisire un parere dell'Amministratore di sistema, vista la particolare competenza tecnica necessaria al fine della distruzione sicura dei dati personali contenuti nei supporti digitali.

Per quanto riguarda la distruzione della documentazione cartacea, si considera conforme alla disciplina del Regolamento UE la distruzione effettuata mediante macchina distruggi documenti con livello di sicurezza di almeno P-4 secondo la normativa DIN 66399 (supporti dati con dati particolarmente sensibili e riservati, nonché dati personali che richiedono una maggiore protezione). È pertanto fatto obbligo a tutti i dipendenti di utilizzare tali apparecchiature per la distruzione di tutti i documenti cartacei contenenti dati personali.

Articolo 18): PRIVACY E OBBLIGHI DI PUBBLICAZIONE

Con il D.Lgs. n. 33/2013 il legislatore ha disciplinato in maniera organica i casi di pubblicità per finalità di trasparenza mediante inserzioni di dati, informazioni, atti e documenti sui siti web istituzionali degli enti. In particolare, gli obblighi di pubblicazione online di dati per finalità di "trasparenza" sono quelli indicati nel D.lgs. n. 33/2013 e nella normativa vigente in materia avente a oggetto le "*informazioni concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche*".

Accanto a questi obblighi di pubblicazione permangono altri obblighi di pubblicità online di dati, informazioni e documenti della PA – contenuti in specifiche disposizioni di settore diverse da quelle approvate in materia di trasparenza – come, fra l'altro, quelli volti a far conoscere l'azione amministrativa in relazione al rispetto dei principi di legittimità e correttezza, o quelli atti a garantire la pubblicità legale degli atti amministrativi (es.: pubblicità integrativa dell'efficacia, dichiarativa, notizia).

I principi e la disciplina di protezione dei dati personali devono essere rispettati anche nell'attività di pubblicazione di dati sul web per finalità di trasparenza. In particolare, la "diffusione" di dati personali da parte dei soggetti pubblici è ammessa unicamente quando la stessa è prevista da una specifica norma di legge o di regolamento. È, quindi, consentita la diffusione dei soli dati personali la cui inclusione in atti e documenti da pubblicare sia realmente necessaria e proporzionata alla finalità di trasparenza perseguita nel caso concreto (cd. "principio di pertinenza e non eccedenza"). Di conseguenza, i dati personali che esulano da tale finalità non devono essere inseriti negli atti e nei documenti oggetto di pubblicazione online. In caso contrario, occorre provvedere, comunque, all'oscuramento delle informazioni che risultano eccedenti o non pertinenti.

Si richiamano espressamente i seguenti provvedimenti del Garante per la protezione dei dati personali:

- "Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati" del 15.05.2014;
- "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" del 14.06.2007;
- "Linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali" del 19.04.2007.

Tali provvedimenti indicano alcune azioni che le PA devono intraprendere al fine di bilanciare correttamente gli obblighi di trasparenza e il diritto alla riservatezza dei dati personali, in particolare:

- per rendere effettivamente "anonimi" i dati pubblicati online occorre oscurare del tutto il nominativo e le altre informazioni riferite all'interessato che ne possano consentire l'identificazione anche a posteriori;
- inserire nella sezione "Amministrazione trasparente" del proprio sito web un *alert* in cui si informi il pubblico che i dati personali pubblicati sono "*riutilizzabili solo alle condizioni previste dalla normativa vigente sul riuso dei dati pubblici (direttiva comunitaria 2003/98/CE e d. lgs. 36/2006 di recepimento della stessa), in termini compatibili con gli scopi per i quali sono stati raccolti e registrati, e nel rispetto della normativa in materia di protezione dei dati personali*";
- nella pubblicazione dei curricula, provvedere ad oscurare tutti i dati eccedenti le finalità di trasparenza; possono essere ritenute pertinenti le informazioni riguardanti i titoli di studio e professionali, le esperienze lavorative, conoscenze linguistiche o nell'uso di tecnologie; non devono invece essere oggetto di pubblicazioni dati personali eccedenti quali i recapiti personali ed il codice fiscale;
- per quanto riguarda i concorsi e le selezioni, possono essere pubblicati dolo i dati pertinenti e non eccedenti ai fini del corretto espletamento delle procedure, quindi è lecito pubblicare elenchi nominativi con i risultati delle prove intermedie, elenchi degli ammessi alle prove, punteggi totali ottenuti; non risulta invece lecito riportare negli atti delle graduatorie altri dati come ad esempio recapiti telefonici o codice fiscale;
- ove la normativa imponga la pubblicazione concernenti corrispettivi e compensi, risulta proporzionato indicare il compenso complessivo percepito, ma non la versione integrale di documenti o eventuali dichiarazioni fiscali.

Per quanto riguarda gli atti di organizzazione degli uffici contenenti dati personali, appare opportuno oscurare tutti i dati riferiti al dipendente interessato rendendo anonimo il dato nei documenti oggetto di pubblicazione online. L'atto completo di tutte le informazioni sarà invece trattato dall'ufficio preposto.

Fermo restando che i presupposti, le modalità ed i limiti per l'esercizio del diritto di accesso ai documenti amministrativi e del diritto di accesso civico, semplice e generalizzato e la relativa tutela giurisdizionale, così come gli obblighi di pubblicità e pubblicazione, restano disciplinati dalla normativa di settore - gli uffici dovranno interpretare la vigente normativa in materia di trasparenza ed accesso in modo da garantire la più rigorosa tutela dei dati personali degli interessati, anche tenendo in considerazione le motivazioni addotte dal soggetto controinteressato.

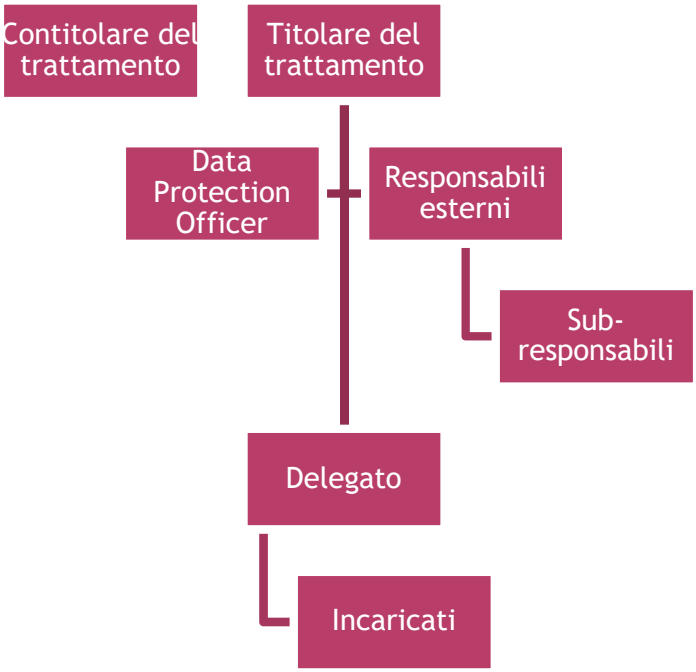
PARTE QUARTA: TITOLARE DEL TRATTAMENTO E ALTRE FIGURE

Articolo 19): ASSETTO ORGANIZZATIVO PRIVACY

Il D.lgs. 196/2003, come novellato dal D.lgs. 101/2018 di armonizzazione del Codice italiano della privacy alle novità del GDPR Europeo n. 2016/679, stabilisce, all'articolo 2-quaterdecies, comma 1, che il Titolare può "*prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la propria autorità*".

L'Istituzione "Cav. Paolo Sartori", in qualità di Titolare del trattamento di dati personali, è tenuta a delineare al proprio interno un'adeguata ed efficace articolazione delle responsabilità al fine di assicurare il rispetto delle disposizioni vigenti in materia, e ciò sulla base del principio europeo di *accountability*, che prevede il coinvolgimento e la responsabilizzazione, ad ogni livello, delle strutture dell'azienda nel percorso di adeguamento ai precetti europei.

Ai fini del rispetto del principio di accountability si definisce un "assetto organizzativo privacy", raffigurabile come indicato di seguito:



Articolo 20): TITOLARE DEL TRATTAMENTO

L'art. 4 n. 7 del GDPR precisa che il titolare del trattamento (interpretando la norma rispetto alla pubblica amministrazione) è "*l'autorità pubblica*" che "*determina le finalità e i mezzi del trattamento di dati personali*". Il concetto di Titolare del trattamento serve a determinare in primissimo luogo chi risponde dell'osservanza delle norme relative alla protezione dei dati.

Competenze e responsabilità

Le competenze e le responsabilità che il GDPR assegna al Titolare del trattamento possono così essere riassunte:

- determinare le finalità ed i mezzi del trattamento dei dati personali: in considerazione del carattere pubblico che contraddistingue questa Amministrazione, le finalità sono determinate e circoscritte in quelle necessarie a garantire il corretto svolgimento delle funzioni istituzionali e dei compiti di interesse pubblico (art. 4);
- mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR (c.d. accountability) (art. 24);
- garantire che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali non tratti tali dati se non è adeguatamente istruito in tal senso (artt. 29 e 32);
- individuare i responsabili del trattamento, controllarne e garantirne l'operato (art. 28);
- agevolare l'esercizio dei diritti dell'interessato (art. 12) e fornire agli interessati le informazioni previste dal GDPR (art. 13);
- designare il Responsabile della protezione dei dati (art. 37) ponendolo in grado di svolgere adeguatamente l'attività (art. 38);
- istituire e tenere aggiornato un registro delle attività di trattamento svolte sotto la propria responsabilità (art. 30);
- effettuare, prima di procedere al trattamento, una valutazione dell'impatto sulla protezione dei dati personali (art. 35);
- comunicare all'autorità di controllo (art. 33) ed all'interessato (art. 34) eventuali violazioni dei dati;

- ricevere ed osservare provvedimenti, notifiche e ingiunzioni dell'autorità di controllo (art. 58);
- rispondere per il danno cagionato dal trattamento che violi il GDPR (art. 82);
- rispondere delle violazioni amministrative ai sensi del GDPR (art. 83).

Alla luce del testo normativo e delle interpretazioni correnti, si ritiene che Titolare sia l'Ente nel suo complesso in quanto la legislazione nazionale gli ha affidato il compito di raccogliere e trattare certi dati personali. Le competenze e le responsabilità quali delineate dal GDPR e dalla normativa nazionale in tema di protezione dei dati personali sono attribuite agli organi dell'ente in relazione alle funzioni agli stessi assegnati dallo statuto. Tale ripartizione è così intesa da questa Amministrazione:

A. al **Consiglio di Amministrazione** sono assegnate:
   a) le competenze di tipo regolatorio o programmatorio generale in materia di riservatezza dei dati;

B. al **Presidente** spettano i seguenti compiti:
   a) vigilare sulla corretta informazione e sull'esercizio dei diritti degli interessati;
   b) disporre l'adozione dei provvedimenti imposti dal Garante, per quanto di competenza;
   c) collaborare con il Responsabile della protezione dei dati personali al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;

C. al **Direttore** spettano i seguenti compiti (con elencazione meramente esemplificativa):
   a) attribuisce le nomine e le designazioni rilevanti in materia di protezione dei dati personali, con riferimento in particolare al Responsabile della protezione dei dati, ai soggetti designati con funzioni di coordinamento e al referente;
   b) verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura;
   c) disporre le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;
   d) implementare una valutazione dei rischi legata al trattamento dei dati personali;
   e) adottare soluzioni di *privacy by design* e *by default*;
   f) aggiornare costantemente il registro delle attività di trattamento;
   g) implementare il registro dei *data-breach* qualora necessario;
   h) garantire la corretta informazione e l'esercizio dei diritti degli interessati;
   i) individuare e sottoscrivere il contratto con i responsabili del trattamento, ai sensi dell'art. 28, comma 3, del Regolamento UE 2016/679;
   j) individuare i soggetti Incaricati a compiere operazioni di trattamento (di seguito anche "Incaricati al trattamento") fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite;
   k) autorizzare altresì anche eventuali collaboratori "esterni" (persone fisiche), a prescindere dal rapporto contrattuale intrattenuto con l'Amministrazione (ad es. stagisti, tirocinanti, singoli volontari, …) purché non dotati di potere decisionale autonomo e stabilmente presenti in struttura per un dato periodo;
   l) disporre l'adozione dei provvedimenti imposti dal Garante, per quanto di competenza;
   m) collaborare con il Responsabile della protezione dei dati personali al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
   n) garantire al Responsabile della protezione dei dati personali ed al personale designato Amministratore di Sistema i necessari permessi di accesso ai dati ed ai

sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza;

o) la preventiva valutazione d'impatto ai sensi dell'art. 35 del Regolamento, nei casi in cui un trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche e le eventuali consultazioni con il Garante ai sensi dell'art. 36 del Regolamento;

p) gestire la procedura in relazione alle violazioni di dati personali, curando la notifica all'Autorità di controllo e l'eventuale comunicazione agli interessati.

Il Direttore può delegare uno o più compiti ad altro personale specificatamente individuato.

Articolo 21): CONTITOLARE DEL TRATTAMENTO

Come stabilito dall'art. 26 del Regolamento Europeo n. 2016/679, allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono Contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento UE, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni.

Tale accordo può designare un punto di contatto per gli interessati e riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli Interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'Interessato.

Indipendentemente dalle disposizioni dell'accordo anzidetto, l'Interessato può esercitare i propri diritti ai sensi del Regolamento UE nei confronti di e contro ciascun Titolare del trattamento.

Articolo 22): DELEGATO ALLA GESTIONE DELLE ATTIVITÀ DI TRATTAMENTO DEI DATI

In considerazione della complessità e della molteplicità delle funzioni istituzionali dell'Amministrazione viene introdotta la figura "intermedia" del "Delegato alla gestione delle attività di trattamento dei dati".

Tale figura provvede ad eseguire i compiti eventualmente delegati dal Direttore in qualità di Titolare del trattamento.

Articolo 23): RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI

Il concetto di "Responsabile del trattamento" riveste un ruolo importante nel contesto della riservatezza e sicurezza dei trattamenti poiché serve ad individuare le responsabilità di coloro che si occupano più da vicino dell'elaborazione dei dati personali, sotto l'autorità diretta del Titolare del trattamento o per suo conto.

L'esistenza di un Responsabile del trattamento dipende da una decisione presa dal Titolare. Quest'ultimo può decidere di trattare i dati all'interno della propria organizzazione, ad esempio attraverso collaboratori autorizzati a trattare i dati sotto la sua diretta autorità, o di delegare tutte o una parte delle attività di trattamento a un'organizzazione esterna.

A norma dell'articolo 28, paragrafo 1 del GDPR "*Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato*".

Per poter agire come Responsabile del trattamento occorrono quindi due requisiti: essere una persona giuridica distinta dal Titolare ed elaborare i dati personali per conto di quest'ultimo. La liceità dell'attività di trattamento dei dati da parte del Responsabile è determinata dal mandato

ricevuto dal Titolare del trattamento. Se va al di là del proprio mandato e se acquisisce un ruolo rilevante nella determinazione delle finalità o degli aspetti fondamentali dei mezzi del trattamento, il Responsabile diventa (con)Titolare.

Si deve tuttavia prendere atto del fatto che esistano situazioni in cui la relazione tra l'Ente ed un altro soggetto, pubblico o privato, possa generare dei dubbi in merito alla corretta qualificazione del ruolo soggettivo rivestito (Titolare o Responsabile). Con riferimento a tali fattispecie, questo Ente adotta il criterio della valutazione delle circostanze di fatto, suggerito dal Gruppo ex art. 29 nel Parere 1-2010 (WP 169). Il paragrafo 3 dell'articolo 28 del GDPR prevede che "*I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, 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*"; il paragrafo 9, da ultimo, prevede che "*Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico*".

Spetta al Direttore identificare i responsabili e gli eventuali sub-responsabili, e sottoscrivere i contratti/appendici contrattuali per il trattamento dei dati, avendo cura di tenere costantemente aggiornata la relativa documentazione nonché acquisire dai responsabili e dagli eventuali sub responsabili l'elenco nominativo delle persone fisiche che, presso gli stessi, risultano autorizzate al trattamento dei dati ed a compiere le relative operazioni. Il Direttore ha il dovere di verificare che il soggetto esterno osservi le predette prescrizioni; l'Amministratore del sistema informatico verifica che siano osservate le norme riferite all'attuazione delle misure minime di sicurezza. La periodicità delle predette verifiche, previste nel provvedimento o contratto di affidamento, è determinata in funzione della natura dei dati, della probabile gravità dei rischi, dei mezzi da utilizzare per il trattamento e della durata dell'affidamento. Le verifiche e i risultati delle stesse sono registrate in appositi distinti verbali, sottoscritti, in duplice originale, dal Responsabile del trattamento e dal soggetto che svolge ciascuna verifica.

Articolo 24): SUB-RESPONSABILE DEL TRATTAMENTO DEI DATI

Il Responsabile del trattamento non ricorre a un altro Responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare del trattamento.

Nel caso di autorizzazione scritta generale, il Responsabile del trattamento informa il Titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri Responsabili del trattamento, dando così al Titolare del trattamento l'opportunità di opporsi a tali modifiche.

Quando un Responsabile del trattamento ricorre a un altro Responsabile del trattamento per l'esecuzione di specifiche attività, su tale altro Responsabile sono imposti, mediante un contratto o un altro atto giuridico, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il Titolare del trattamento e il Responsabile del trattamento, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate.

Qualora l'altro Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro Responsabile.

Articolo 25): INCARICATO (INTERNO ED ESTERNO) AL TRATTAMENTO DEI DATI

Il D.lgs. 196/2003, come novellato dal D.lgs. 101/2018 stabilisce, all'art. 2-quaterdecies, comma 2, che il Titolare "*individua le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta*".

Ciò detto, sulla base del principio europeo di *accountability*, il Titolare del trattamento provvede ad individuare le persone "incaricate al trattamento dei dati" ai sensi dell'art. 2-quaterdecies, comma 2, del D.lgs. 196/2013.

Al momento dell'ingresso in servizio è fornita, a cura dell'ufficio di gestione delle risorse umane, ad ogni dipendente (oltre che ad ogni collaboratore esterno) una specifica comunicazione in materia di privacy, con la quale detti soggetti (dipendenti e non dipendenti) vengono nominati quali "incaricati al trattamento dei dati" ai sensi del D.lgs. 196/2003 e del Regolamento UE 2016/679, impartendo loro anche le opportune "istruzioni operative".

Al fine di dare evidenza di quale tipologia di dati possono trattare le varie figure (interne/esterne), si espone una matrice per il trattamento dei dati:

	DATI COMUNI OSPITI (oltre ai congiunti, rappresentanti legali e familiari)	DATI PARTICOLARI DEGLI OSPITI (relativi alla salute)	DATI COMUNI DEI DIPENDENTI (e del nucleo familiare)	DATI PARTICOLARI DEI DIPENDENTI (e del nucleo familiare)	DATI COMUNI DEI COLLABORATORI ESTERNI E DEI FORNITORI
Direttore					
Coordinatore dei Servizi			(solo dati di contatto)	(solo limitazioni alle mansioni)	
Personale amministrativo					
Assistente sociale					
Infermieri professionali			(solo dati di contatto)		
Operatori socio-assistenziali					
Educatore					
Fisioterapista - Logopedista					
Medico					
Psicologo					
Manutentore	(solo dati identificativi)				
Personale delle funzioni ausiliarie (lavanderia, pulizie, cucina)	(solo dati identificativi)				
Volontari	(solo dati identificativi)				

Al fine di dare completa informazione e formazione agli Incaricati che utilizzano i sistemi informatici, è predisposto un apposito "disciplinare sulle misure di sicurezza degli strumenti informatici", di cui all'Allegato A, che viene consegnato a cura dell'ufficio di gestione delle risorse umane a tutti gli Incaricati destinatari.

Articolo 26): DATA PROTECTION OFFICER

Il Regolamento Europeo impone alle autorità ed agli organismi pubblici la nomina del Data Protection Officer (in italiano: Responsabile della protezione dei dati o 'RPD'), nei termini di cui agli artt. 37, 38 e 39 del Regolamento medesimo.

Il DPO deve presentare caratteristiche di indipendenza ed autorevolezza, oltre che competenze manageriali. Non deve, inoltre, essere in conflitto di interessi in quanto il Regolamento UE vieta di nominare DPO anche chi, solo in astratto, possa potenzialmente trovarsi in conflitto di interessi.

Si tratta di una figura dirigenziale, di alta professionalità, a metà tra il consulente ed il revisore e non dovrebbe ricoprire ruoli gestionali rispetto all'attività della Pubblica Amministrazione.

Ai sensi dell'art. 39 del Regolamento UE, i suoi compiti sono:

a) informare e fornire consulenza al Titolare del trattamento, nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal Regolamento UE nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del Regolamento UE, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito 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 la stessa per questioni connesse al trattamento, tra cui la consultazione preventiva, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Ai sensi dell'art. 37 del Regolamento UE, il DPO deve:

a) possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze;
b) adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse. In linea di principio, ciò significa che il DPO non può essere un soggetto che ricopre ruoli gestionali e che decide sulle finalità o sugli strumenti del trattamento di dati personali;
c) operare alle dipendenze del Titolare oppure sulla base di un contratto di servizio (DPO esterno);
d) disporre di risorse umane e finanziarie, messe a disposizione dal Titolare, per adempiere ai suoi scopi.

Il Regolamento UE prevede la pubblicazione sul sito istituzionale dell'Ente dei "dati di contatto" del DPO; i medesimi dati devono essere inseriti anche nell'informativa aziendale sul trattamento dei dati, così che il DPO sia agevolmente contattabile.

Articolo 27): AMMINISTRATORE DI SISTEMA (AdS)

L'Amministratore di sistema, individuato dal Titolare del trattamento, sovraintende alla gestione e alla manutenzione delle banche dati e, nel suo complesso, al sistema informatico di cui è dotato l'Ente.

La nomina dell'Amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati e in tema di sicurezza. La designazione dell'Amministratore di sistema è individuale e deve recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

In ambito di protezione dei dati personali, l'Amministratore di sistema propone al Titolare del trattamento un documento di valutazione del rischio informatico, da aggiornare con cadenza annuale.

Nel rispetto della normativa in materia di protezione dei dati e della sicurezza, l'Amministratore di sistema deve adottare sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni (*access log*) devono essere complete, inalterabili, verificabili nella loro integrità, e adeguate al raggiungimento dello scopo di verifica

per cui sono richieste. Le registrazioni devono comprendere il riferimento temporale e la descrizione dell'evento che le ha generate e devono essere conservate per un periodo congruo, non inferiore ai sei mesi.

L'Amministratore di sistema applica le disposizioni impartite dal Garante in materia di misure e accorgimenti effettuati con strumenti elettronici.

Articolo 28): REFERENTE PER LA PROTEZIONE DEI DATI PERSONALI

Ai sensi dell'articolo 38 del GDPR, il Titolare ha l'obbligo di assicurarsi che "*il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali*"; il Titolare inoltre sostiene "*il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica*".

In caso di nomina di un DPO esterno all'organizzazione, si ravvisa dunque la necessità - nell'ottica di un adeguamento in qualità ai nuovi istituti previsti dal GDPR, alla luce del contesto, della natura e della complessità dei trattamenti effettuati - di individuare uno o più dipendenti interni all'ente cui assegnare il compito di "Referente" al fine di supportare l'attività del Responsabile della Protezione dei dati personali (DPO), nelle seguenti attività:

a) Informazione e consulenza al Titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR. Tale attività comporta il supporto nella redazione di pareri, note, circolari, policy, newsletter con segnalazione delle novità normative e giurisprudenziali in materia di protezione dei dati personali e delle migliori *best practice* in materia di analisi e valutazione dei rischi.

b) Sorveglianza dell'osservanza del GDPR, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo.

c) Fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del GDPR. Tale attività comporta un supporto nelle interviste a responsabili di settore, ICT, partecipazione a riunioni, analisi di documentazione tecnica, studio degli ambienti di prova dei software e della relativa documentazione tecnica.

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 prevista dall'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione. Tale attività comporta un supporto nel riscontro alle richieste di informazioni inviate dal Garante e nelle eventuali ispezioni dell'Autorità.

Il Referente è tenuto al segreto od alla riservatezza in merito all'adempimento dei propri compiti e alle informazioni e dati di cui potrebbe venire a conoscenza nell'esercizio delle proprie funzioni. Egli è inoltre tenuto a segnalare al DPO ogni possibile situazione di conflitto di interesse, anche potenziale rispetto ai propri compiti, incarichi e funzioni.

Ove i compiti assegnati al Referente vengano svolti in modo collettivo da parte di un team, dovrà essere designato un soggetto coordinatore.

PARTE QUINTA: SICUREZZA DEI DATI PERSONALI E MISURE DI SICUREZZA

Articolo 29): PROTEZIONE DEI DATI

Come esposto nel considerando 78, la tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del Regolamento UE.

L'art. 25 del Regolamento Europeo n. 2016/679 introduce il criterio sintetizzato dall'espressione inglese "*data protection by default and by design*", ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'Interessato di controllare il trattamento dei dati e consentire al Titolare del trattamento di creare e migliorare le caratteristiche di sicurezza.

Articolo 30): REGISTRO ELETTRONICO DELLE ATTIVITÀ DI TRATTAMENTO

Tutti i Titolari e i Responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti che non effettuano trattamenti a rischio devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30 del Regolamento UE.

Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio.

Il Registro deve essere esibito su richiesta del Garante.

Il registro delle attività di trattamento costituisce uno dei principali elementi di *accountability* del Titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività.

Il registro delle attività di trattamento è esposto nell'Allegato B).

Articolo 31): VALUTAZIONE E GESTIONE DEI RISCHI

La valutazione dei rischi è necessaria, tra l'altro:

a) per determinare l'adeguatezza delle misure di sicurezza a protezione dei trattamenti di dati personali;
b) per determinare la necessità di una valutazione d'impatto sui trattamenti e nella valutazione d'impatto stessa;
c) per determinare la necessità di segnalazione di una violazione di dati personali all'autorità di controllo.

La normativa non indica orientamenti specifici per la messa in atto di opportune misure e per dimostrare la conformità da parte del Titolare del trattamento in particolare per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua valutazione in termini gravità e probabilità, e l'individuazione di migliori prassi per attenuare il rischio: le scelte in materia di gestione del rischio sono responsabilità del Titolare del trattamento, secondo il principio di responsabilizzazione.

Articolo 32): VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

La valutazione d'impatto sulla protezione dei dati (DPIA: *data protection impact assessment*, nell'accezione inglese) è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.

La DPIA è uno strumento importante per la responsabilizzazione in quanto sostiene il Titolare non soltanto nel rispettare i requisiti del GDPR, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del medesimo GDPR.

La DPIA sulla protezione dei dati personali deve essere realizzata, prima di procedere al trattamento, dal Titolare del trattamento quando un tipo di trattamento, considerata la natura, il contesto, le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Vengono qui espressamente richiamate le "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato*", predisposte dal Gruppo di lavoro WP29 in data 04.10.2017. In particolare, fra i trattamenti che possono presentare un rischio elevato, viene individuato il criterio dei dati relativi a interessati vulnerabili, nei casi dove sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del Titolare del trattamento. Nei trattamenti di questo ente tali squilibri si possono identificare nei confronti degli ospiti (persone anziane solitamente non autosufficienti) e dei dipendenti.

Tuttavia le linee guida prevedono l'obbligo di procedere con la valutazione d'impatto qualora il trattamento soddisfi ulteriori criteri (almeno due) tra quelli elencati.

Considerato che il *core business* dell'Ente è la gestione dell'ospite anziano in stato di bisogno, e che vengono costantemente trattati dati personali sia di tipo comune che di tipo particolare, il Titolare del trattamento può prevedere di realizzare una valutazione di impatto su tale trattamento.

Articolo 33): NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITÀ DI CONTROLLO

Per violazione dei dati personali (in seguito "*data breach*") si intende la violazione di sicurezza che comporti, accidentalmente od in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dall'Ente (tale indicazione operativa pertanto si applica a tutti gli archivi/documenti cartacei ed a tutti i sistemi, anche informativi sui quali siano conservati i dati personali degli interessati, quali ospiti, dipendenti, fornitori, soggetti terzi, ecc.).

La segnalazione di un possibile *Data Breach* può provenire dall'esterno (persone di riferimento degli ospiti, familiari, fornitori esterni, enti istituzionali ecc.) o dall'interno, durante il normale svolgimento dell'attività lavorativa (più frequentemente tali eventi vengono evidenziati da funzioni che svolgono attività di verifica e /o di controllo).

Colui il quale riceve la segnalazione dall'esterno o che rileva dall'interno l'evento anomalo di violazione di dati personali, deve darne immediata notizia al Direttore il quale, con la collaborazione di eventuali delegati, deve:

a) adottare le misure di sicurezza informatiche e/o organizzative per porre rimedio o attenuare i possibili effetti negativi della violazione dei dati personali e, contestualmente, informa immediatamente il DPO per una valutazione condivisa;
b) condurre e documentare un'indagine corretta e imparziale sull'evento (aspetti organizzativi, informatici, legali, ecc.) attraverso la compilazione del "Modello di potenziale violazione di dati personali al DPO" (Allegato C);
c) riferire i risultati dell'indagine inviando il modello al DPO.

Il DPO, ricevuti i risultati dell'indagine, analizza l'accaduto e formula un parere in merito all'evento, esprimendo la propria valutazione, non vincolante. Lo invia quindi al Direttore.

Il Direttore, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione all'Autorità di controllo. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo. Qualora la notifica effettuata nelle 72 ore non sia completa è possibile integrarla in una o più fasi successive (ad es. nel caso di violazioni complesse per le quali occorrono indagini approfondite) corredandola con i motivi (analogamente come in caso di notifica in ritardo). Nel caso in cui la scoperta della violazione non sia contestuale al verificarsi dell'evento che l'ha generata, devono essere indicate nella comunicazione le motivazioni che non hanno consentito l'immediata rilevazione dell'evento stesso e le misure adottate o che si intende adottare affinché ciò non si ripeta in futuro.

La notifica sarà effettuata utilizzando il modello predisposto con provvedimento del Garante del 31.07.2019.

Il Responsabile del trattamento eventualmente coinvolto deve:

a) informare il Direttore tempestivamente ed in ogni caso entro e non oltre 24 ore dalla scoperta dell'evento, tramite PEC, di essere venuto a conoscenza di una violazione e fornire tutti i dettagli della violazione subita, in particolare una descrizione della natura della violazione dei dati personali, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di registrazioni dei dati in questione, l'impatto della violazione dei dati personali sull'Ente e sugli Interessati coinvolti e le misure adottate per mitigare i rischi;
b) fornire assistenza per far fronte alla violazione ed alle sue conseguenze soprattutto in capo agli Interessati coinvolti. Il Direttore si attiverà per mitigare gli effetti delle violazioni, proponendo tempestive azioni correttive. Tali misure sono richieste al fine di garantire un livello di sicurezza adeguato al rischio correlato al trattamento eseguito. Risulta opportuno e di particolare importanza che tutti gli atti di designazione a Responsabile del trattamento contengano una espressa previsione circa la necessità di informare l'Ente, senza ingiustificato ritardo, in caso di avvenuta conoscenza di una violazione di dati personali, anche solo probabile o possibile.

I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:

a) danni fisici, materiali o immateriali alle persone fisiche;
b) perdita del controllo dei dati personali;
c) limitazione dei diritti, discriminazione;
d) furto o usurpazione d'identità;
e) perdite finanziarie, danno economico o sociale;
f) decifratura non autorizzata della pseudonimizzazione;
g) pregiudizio alla reputazione;
h) perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

Ove il Direttore ritenga che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata sia elevato, deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. Prima di procedere alla comunicazione della violazione ai soggetti interessati il testo della comunicazione, le modalità di notifica e le evidenze che attestano il reale livello di pregiudizio, dovranno essere concordate con il DPO. Nel caso in cui la comunicazione dovesse pregiudicare lo svolgimento delle verifiche sull'evento *Data Breach*, il Direttore può chiedere all'Autorità di controllo l'autorizzazione a ritardare la citata comunicazione per il tempo necessario all'espletamento di tali verifiche.

La probabilità e la gravità del rischio, per i diritti e le libertà dell'interessato, dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante

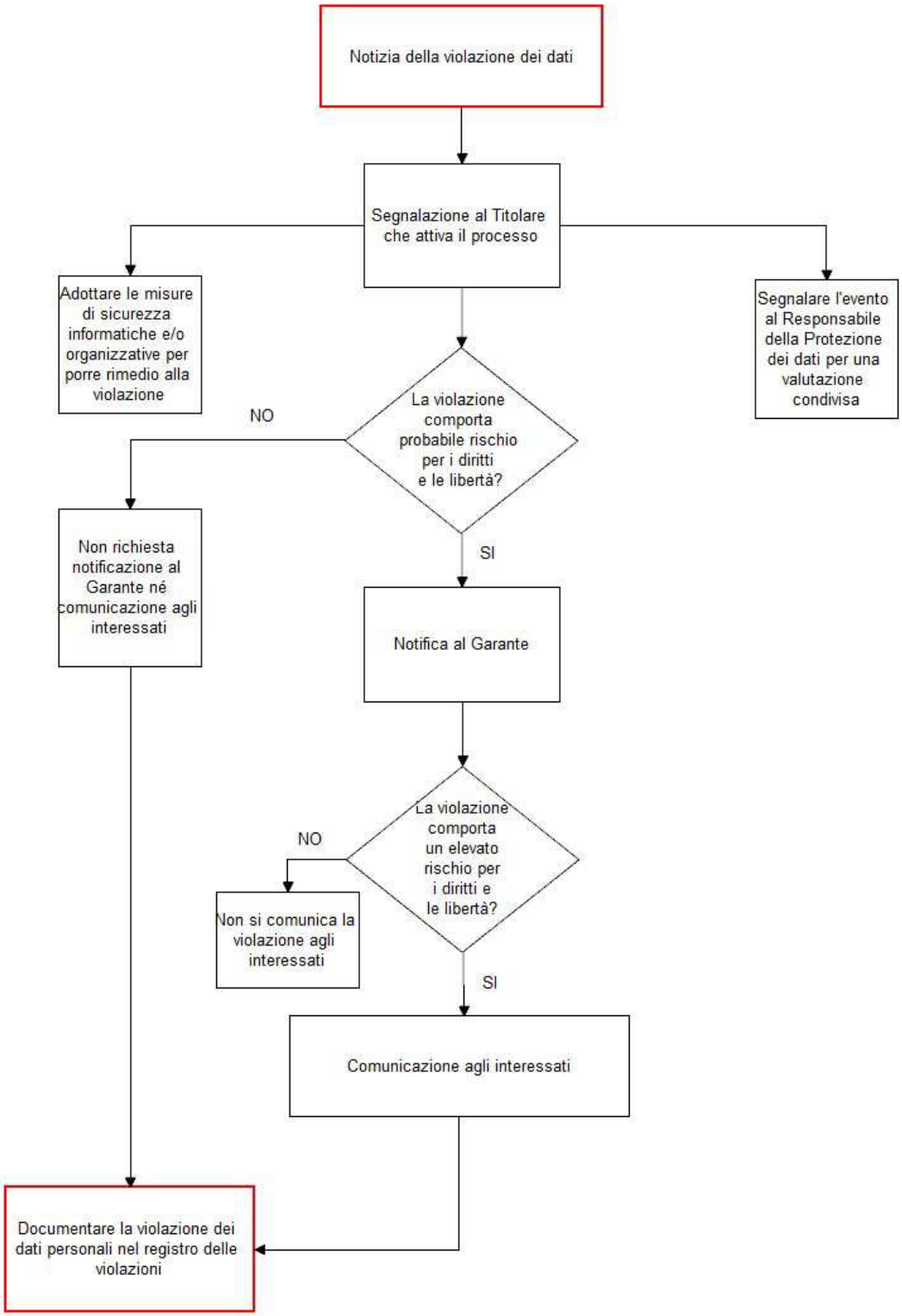
cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

a) coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
b) riguardare categorie particolari di dati personali;
c) comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
d) comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
e) impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

La notifica all'Autorità di controllo deve avere il contenuto minimo previsto dall'art. 33 del GDPR, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al su citato art. 33.

Ciascun ufficio deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. È comunque opportuno che il registro delle violazioni tenga traccia anche delle varie fasi di gestione dell'evento, dalla rilevazione, all'analisi e alla sua risoluzione e conclusione. Il registro dovrà essere dotato di idonee misure di sicurezza atte a garantire l'integrità e l'immodificabilità dei dati in esso registrati. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dall'Autorità di controllo al fine di verificare il rispetto delle disposizioni del GDPR.

Flusso degli adempimenti in caso di violazione dei dati



Articolo 34): TRASFERIMENTO DI DATI PERSONALI ALL'ESTERO

Si fa rinvio ai principi dettati dal Regolamento Europeo agli articoli 44 e seguenti, nonché alle indicazioni che fossero dettate, in materia, dal Legislatore nazionale e dal Garante per la protezione dei dati personali.

PARTE TERZA: DIRITTI DELL'INTERESSATO

Articolo 35): DIRITTO DI ACCESSO DELL'INTERESSATO

Come stabilito dall'art. 15 del Regolamento Europeo n. 2016/679, l'Interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'Interessato di chiedere al Titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo a un'autorità di controllo;
g) qualora i dati non siano raccolti presso l'Interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 22 del Regolamento Europeo, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'Interessato.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'Interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'art. 46 del Regolamento Europeo relative al trasferimento.

Il Titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'Interessato, il Titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'Interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'Interessato, le informazioni sono fornite in un formato elettronico di uso comune.

Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

Per quanto riguarda, inoltre, le modalità concrete per mezzo delle quali trova attuazione, nell'attuale contesto normativo ed organizzativo, il diritto di accesso, si fa rinvio alle vigenti diposizioni normative e regolamentari emanate, negli anni, dal Legislatore statale nonché dal Garante per la privacy, con particolare riferimento all'ambito sanitario.

Si fa espresso rinvio, in particolare, alle vigenti disposizioni normative in materia di "accesso documentale", di "accesso civico" e di "accesso generalizzato".

Articolo 36): DIRITTO DI RETTIFICA

Come stabilito dall'art. 16 del Regolamento Europeo n. 2016/679, l'Interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'Interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Articolo 37): DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO)

Come stabilito dall'art. 17 del Regolamento Europeo n. 2016/679, in capo all'Interessato è riconosciuto il diritto "all'oblio", che si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata.

Si prevede, infatti, l'obbligo per i titolari di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione" (si veda art. 17, paragrafo 2 del Regolamento Europeo).

Articolo 38): DIRITTO DI LIMITAZIONE AL TRATTAMENTO

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 Regolamento Europeo (in attesa della valutazione da parte del Titolare).

Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (consenso dell'Interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).

Articolo 39): DIRITTO ALLA PORTABILITÀ DEI DATI

Si applica ai trattamenti automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili solo i dati trattati con il consenso dell'Interessato o sulla base di un contratto stipulato con l'Interessato (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del Titolare, per esempio), e solo i dati che siano stati "forniti" dall'Interessato al Titolare (si veda il considerando 68 del Regolamento UE).

Inoltre, il Titolare deve essere in grado di trasferire direttamente i dati portabili a un altro Titolare indicato dall'Interessato, se tecnicamente possibile.

Articolo 40): DIRITTO DI OPPOSIZIONE

Come stabilito dall'art. 21 del Regolamento Europeo n. 2016/679, l'Interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'Articolo 6, paragrafo 1, lettere e) o f) del medesimo Regolamento, compresa la profilazione sulla base di tali disposizioni.

Il Titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'Interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Articolo 41): PROCESSO DECISIONALE AUTOMATIZZATO (PROFILAZIONE)

Come stabilito dall'Articolo n. 22 del Regolamento Europeo n. 2016/679, l'Interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Tale principio non si applica nel caso in cui la decisione:

- sia necessaria per la conclusione o l'esecuzione di un contratto tra l'Interessato e un Titolare del trattamento;
- sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà dei legittimi interessi dell'Interessato;
- si basi sul consenso esplicito dell'Interessato.

Articolo 42): DIRITTI RIGUARDANTI LE PERSONE DECEDUTE

L'art. 2-terdecies del D.lgs. 101/2018 prevede che i diritti di cui agli articoli da 15 a 22 del Regolamento UE riferiti ai dati personali concernenti persone decedute possono essere esercitati

da chi ha un interesse proprio, o agisce a tutela dell'Interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.

L'esercizio di tali diritti non è ammesso nei casi previsti dalla legge o quando, limitatamente all'offerta diretta di servizi della società dell'informazione, l'Interessato lo ha espressamente vietato con dichiarazione scritta presentata al Titolare del trattamento o a quest'ultimo comunicata.

La volontà dell'Interessato di vietare l'esercizio dei diritti deve inoltre risultare in modo non equivoco e deve essere specifica, libera e informata.

In ogni caso, il divieto non può produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'Interessato nonché del diritto di difendere in giudizio i propri interessi.