REGOLAMENTO AZIENDALE
IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Revisione	Data	Causale
0	Non datato	Redazione
1	28/02/2022	Adeguamento al RGPD 2016/679 e al D.Lgs. 196/20003 e s.m.i.

Fasi	Funzioni	Nome e Cognome	Firma	Data
Redazione	Incarico funzionale Coordinatore personale e attività amministrative a supporto dei percorsi sanitari e Adempimenti Privacy	Dr.ssa Claudia Chesi		2/3/2022
Verifica	Direttore sanitario	Dr. Roberto Gusinu		
	Direttore Amministrativo	Dr.ssa Maria Silvia Mancini		
	Responsabile protezione dati	Dr.ssa Nicoletta Minutella		
Approvazione	Direttore Generale	Prof. Antonio Davide Barretta		
Emissione	Responsabile UOSA Accreditamento e Qualità dei Percorsi Assistenziali	Dr.ssa Anna Grasso		

Luogo di archiviazione e conservazione del documento in originale: Segreteria UOC Igiene e Epidemiologia

La diffusione del seguente documento è assicurata mediante la pubblicazione su:

- intranet aziendale alla sezione "*Moduli e documenti* > Privacy;
- sul sito web istituzionale dell'AOUS alla sezione "*Privacy*".
- sul sito web istituzionale dell'AOUS alla sezione "*Amministrazione trasparente*".
- Avviso a liste utenti

Essa inoltre sarà distribuita mediante lettera di diffusione a:

- Direttori di Dipartimento
- Direttori di Unità Operativa
- Responsabili di Unità Operativa Professionale
- Responsabili Infermieristici di Dipartimento
- Responsabili Amministrativi di Dipartimento
- Coordinatori Infermieristici

Validità doc fino a:	Parole chiave		
28/02/2025	A.REG.DG.03	Protezione	Dati personali

La procedura nella precedente versione REV.0/ è stata redatta, a cura di:

- Dr. Frosini – UOC Affari Legali

L'UOSA Accreditamento e Qualità dei percorsi Assistenziali ha provveduto per il presente documento ad effettuare: controllo formale del documento e allineamento ai documenti aziendali

INDICE

INTRODUZIONE

PREMESSA DI CARATTERE NORMATIVO

Il presente Regolamento in materia di protezione dei dati personali è uno strumento di applicazione del nuovo **Regolamento Europeo n. 2016/679**, anche conosciuto come **"RGPD" e, in particolare,** del vigente **D.lgs. 30 giugno 2003, n. 196** (cosiddetto "Codice sulla Privacy" come novellato dal **D.lgs. 10 agosto 2018 n. 101**) nell'ambito dell'organizzazione dell'Azienda ospedaliero – universitaria Senese.

A far data dal 25 maggio 2018 ha trovato infatti diretta ed immediata applicazione, sul territorio nazionale, il nuovo Regolamento Europeo n. 2016/679 (così detto RGPD ossia "*General Data Protection Regulation"*) sulla Privacy, approvato il 27 aprile 2016 e pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 04 maggio 2016.

Ciò ha comportato l'adeguamento delle disposizioni legislative nazionali di cui al previgente Codice della Privacy (D.lgs. n. 196/2003) al RGPD, con il D.lgs. n. 101 del 10 agosto 2018 di adeguamento al RGPD; le norme regolamentari emanate negli anni dall'Autorità Garante per la protezione dei dati personali rimangono applicabili solo in quanto compatibili con la nuova normativa Privacy.

Il presente Regolamento aziendale si rende necessario per recepire, in un unico testo, i precetti normativi a maggior rilevanza, sia di fonte europea che nazionale in tema di trattamento dei dati personali, al fine darne collocazione sistematica nel contesto d'Azienda ospedaliero – universitaria Senese.

Il principio cardine, di matrice anglosassone, introdotto dal nuovo Regolamento Europeo è quello della **"responsabilizzazione" (*accountability*** nell'accezione inglese**)** che pone a carico al Titolare del trattamento dei dati l'onere di valutare il grado di tutele adeguato ai propri trattamenti e 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 pro-attivi, 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 termine *accountability*, infatti, rinvia letteralmente al concetto di "resa di conto") e all'Autorità Garante per la protezione del dati personali.

Ciò premesso, questo Regolamento verrà pubblicato sul sito web aziendale in aggiunta a tutta la documentazione aziendale adottata sino ad oggi in attuazione del RGPD.

Il "sistema aziendale Privacy" adottato dall'Azienda ospedaliero – universitaria Senese, in attuazione del principio europeo dell'accountability, è oggi infatti interamente fruibile sul sito internet aziendale, nell'apposita sezione denominata **"***Privacy*".

La pagina di cui si tratta contiene diverse "sezioni", rispetto alle quali trovano progressivo inserimento (in ciascuna sezione e a seconda dei diversi argomenti) i nuovi atti e le nuove modulistiche che, man mano, vengono approvati, così come gli aggiornamenti e le revisioni dei documenti esistenti. Obiettivo di questa azienda è infatti quello di dotarsi di un sistema organizzativo efficace e trasparente, che sia immediatamente fruibile e che risponda alle esigenze concrete e quotidiane dei propri operatori ed utenti.

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 sanitaria, 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, ma implica il pieno rispetto dei diritti e delle libertà fondamentali e della dignità del singolo individuo.

Per questi motivi la "cultura della Privacy" deve diventare un vero e proprio elemento cardine dell'organizzazione, che deve impegnarsi perché la cultura di cui si tratta possa crescere e rafforzarsi, principalmente fra gli operatori della sanità, in quanto solo con la conoscenza 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, con la

consapevolezza di non affrontare un inutile gravame, bensì di contribuire concretamente al miglioramento della qualità del rapporto con l'utenza.

1. SCOPO

Il presente Regolamento disciplina, all'interno dell'Azienda ospedaliero – universitaria Senese, 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.

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.)

2. CAMPO DI APPLICAZIONE / DESTINATARI

Il presente Regolamento ha come destinatari tutti coloro che operano all'interno dell'Azienda ospedaliero – universitaria Senese; a titolo puramente esemplificativo e non esaustivo si indicano le seguenti figure:

- dipendenti ospedalieri ed universitari convenzionati;
- collaboratori a qualsiasi titolo;
- medici in formazione specialistica:
- contrattisti e borsisti;
- studenti e ii tirocinanti dei corsi di laurea di Area sanitaria;
- associazioni di volontariato;
- etc.….

3. ABBREVIAZIONI E DEFINIZIONI

3.1. Abbreviazioni

AOUS	Azienda ospedaliero – universitaria Senese
RGPD	General data protection regulation (acronimo italiano, Regolamento generale protezione dati)
RPD	Responsabile della protezione dati personali
RES	Responsabile del procedimento per la fase di esecuzione del contratto (Regolamento 13 febbraio 2018, n. 7/R, in attuazione art. 101.1, comma 5 della legge regionale 24 febbraio 2005, n. 40)
DEC	Direttore dell'esecuzione (Regolamento 13 febbraio 2018, n. 7/R, in attuazione art. 101.1, comma 5 della legge regionale 24 febbraio 2005, n. 40)
ESTAR:	Ente di Supporto Tecnico Amministrativo Regionale

3.2. Definizioni

Come stabilito dall'articolo 4 del Regolamento Europeo n. 2016/679, le definizioni adottate sono le seguenti:

- «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia cartaceo o informatizzato (è opportuno specificare) o sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento UE;
- «**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;
- «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome e cognome, 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;

- «**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;
- «**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;
- «**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;

per le tipologie di "dati" sopra indicate, si fa rinvio, per la disciplina di dettaglio, alle disposizioni di cui al D.lgs. n. 101 del 2018 che ha novellato il D.lgs. n. 196/2003 *(vedasi, in particolare, il Titolo 1° della Parte 1^, rubricato "Disposizioni generali").*

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

4. PARTE PRIMA – Disposizioni generali

4.1. Sensibilizzazione

L'Azienda ospedaliero – universitaria Senese 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 aziendale e l'attività informativa diretta a tutti coloro che hanno rapporti con l'Azienda.

Per garantire la conoscenza capillare delle disposizioni introdotte dal nuovo Regolamento europeo, e di conseguenza dal presente nuovo Regolamento aziendale, al quale si fa rinvio, al momento dell'ingresso ogni dipendente *(oltre che ad ogni collaboratore, contrattista o titolare di borsa di studio, ecc.)* viene nominato Incaricato al trattamento dei dati ai sensi del D.lgs. 196/2003 e s.m.i. e del Regolamento UE 2016/679, impartendo anche le opportune *"istruzioni operative"* e i riferimenti per reperire il presente Regolamento aziendale sul sito Internet e intranet aziendale, in modo che l'incaricato sia reso edotto dell'esistenza del Regolamento e delle modalità di consultazione del medesimo.

4.2. Principi applicabili al Trattamento dei Dati

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

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato *(«**liceità, correttezza e trasparenza**»);*
- 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'articolo 89, paragrafo 1 del Regolamento UE, considerato incompatibile con le finalità iniziali *(«**limitazione della finalità**»);*
- 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. n. 196/2003;
- 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**»);*
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 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**»);*
- 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**»).*

4.3. Trattamento di Categorie Particolari di Dati

Come stabilito dall'articolo 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 ricorrono alcune condizioni, riportate al summenzionato articolo 9, tra le quali se ne evidenziano alcune tra cui quella di cui alla lettera "h", ai sensi della quale *"il trattamento è 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 s****ulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità (..)"*, nonché quella di cui alla lettera "i", anch'essa applicabile a questa Azienda, ai sensi della quale *"il trattamento è necessario per* ***motivi di interesse pubblico nel settore della sanità pubblica,*** *quali la protezione da gravi minacce per la salute o la* ***garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici,*** *sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale".*

Si fa presente, inoltre, che il Regolamento UE consente di *"mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute".*

Posto quanto sopra, si fa integrale rinvio agli articoli 75, 2-sexies e 2-septies del D.lgs. n. 196/2003 (come novellato dal D.lgs. 101/2018) contenenti specifiche disposizioni relative al trattamento delle categorie particolari di dati personali relative al trattamento dei dati genetici, biometrici e relativi alla salute. Con la nuova formulazione dell'articolo 75 del D.lgs. n. 196/2003 e s.m.i. è infatti chiarito che non occorre più il consenso per il trattamento dei dati per finalità di diagnosi e cura (art. 2-septies del Codice Privacy emendato). Per un approfondimento circa il consenso al trattamento dati si rinvia al paragrafo 6. 2..

4.4. Trattamento dei Dati Personali relativi a Condanne Penali e Reati (Dati Giudiziari)

Il trattamento dei dati personali relativi a condanne penali e reati (articolo n. 10 del Regolamento Europeo n. 2016/6799 riguarda i dati c.d. "giudiziari", cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.

Come stabilito dall'articolo n. 10 del Regolamento Europeo n. 2016/679, il trattamento "*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.*"

Posto quanto sopra, si fa integrale rinvio all'articolo 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.

4.5. Comunicazione di Dati verso l'Esterno

La comunicazione di dati particolari e giudiziari da parte di un soggetto pubblico ad altra persona fisica o giuridica, autorità pubblica, servizio o un altro organismo, che si tratti o meno di terzi, 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 coinvolti.

4.6. Dossier Sanitario Elettronico Aziendale

Il Dossier Sanitario Elettronico 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.

Il paziente, dopo aver preso visione dell'apposita **nota informativa,** deve prestare il proprio **consenso** in forma scritta alla costituzione del Dossier Sanitario Elettronico che rappresenta un trattamento di dati personali specifico e ulteriore rispetto a quello effettuato dal professionista sanitario con le informazioni acquisite in occasione della cura del singolo evento clinico, volto a documentare parte della storia clinica dell'utente attraverso la realizzazione di un sistema integrato di informazioni circa il relativo stato di salute accessibile dal personale sanitario autorizzato.

Nel Dossier Sanitario Elettronico, una volta costituito, confluiscono tutte le informazioni sanitarie che riguardano uno **stesso** paziente presenti **in questa Azienda**. Tuttavia, in caso di rifiuto dell'interessato alla costituzione del Dossier Sanitario Elettronico, in nessun modo vengono pregiudicate le prestazioni sanitarie presenti e future.

Per quanto concerne le informazioni sanitarie ricomprese tra quelle "a maggior tutela dell'anonimato", come per esempio: *Test HIV, Interruzioni Volontarie di Gravidanza, utilizzo di sostanze stupefacenti, parto anonimo, atti di violenza sessuale o di pedofilia,* è necessario che il paziente fornisca esplicito consenso all'inserimento di dette informazioni nel Dossier Sanitario Elettronico rispetto al quale, altrimenti, saranno escluse.

Questa Azienda assicura, a tutela della riservatezza del paziente, che una volta manifestata la volontà del medesimo in merito al trattamento dei dati personali mediante costituzione di Dossier Sanitario Elettronico, lo stesso interessato possa decidere di **oscurare** taluni dati o documenti sanitari consultabili tramite tale strumento.

Il Dossier è consultabile esclusivamente dal personale sanitario della struttura presso la quale il paziente ha rilasciato l'autorizzazione o da altro personale sanitario quando si renda necessaria una specifica consulenza specialistica concordata con l'interessato.

Il Dossier è consultabile anche da parte dei professionisti che agiscono in *libera professione intramuraria* ovvero nella erogazione di prestazioni *al di fuori del normale orario di lavoro* utilizzando le strutture ambulatoriali e diagnostiche dell'Azienda ospedaliero – universitaria Senese. Sempre con il consenso del paziente, i professionisti sanitari che operano all'interno dell'azienda potranno consultare le informazioni relative alle prestazioni erogate dai professionisti in regime di prestazione intramoenia.

Per la protezione dei dati personali del paziente da specifici rischi di accesso non autorizzato e di trattamenti non consentiti, il personale sanitario *"Incaricato del Trattamento" (vedi articolo 5.6)* è in possesso di una propria *password* che consente la tracciabilità degli accessi e delle modifiche effettuate, garantendo così anche l'esattezza e l'integrità dei dati.

Il paziente, in sede di nota informativa, è anche informato del fatto che in qualsiasi momento, rivolgendosi al *Titolare del Trattamento dei dati,* è in grado di (così come previsto dall'articolo 7 del Decreto Legislativo n.196/2003 e s.m.i.):

- **revocare** il consenso ad alimentare il Dossier con l'inserimento di esami o referti;
- esercitare la facoltà di **oscurare** eventi clinici che lo riguardano con modalità tali da garantire che i soggetti abilitati all'accesso non possano venire a conoscenza del fatto che l'interessato ha effettuato tale scelta;
- esercitare il diritto di **accesso** ai dati personali contenuti nel Dossier Sanitario Elettronico;

- **visionare** gli accessi che sono stati effettuati sul proprio Dossier Sanitario Elettronico da parte dei soggetti abilitati alla consultazione.

Nella nota informativa, questa Azienda provvede quindi ad indicare espressamente le modalità per il contatto:

- Titolare del trattamento: Azienda ospedaliero-universitaria Senese, sede legale in Strada delle Scotte 14, 53100 Siena. Rappresentante Legale: Direttore Generale, tel.0577585519, e-mail dirgen@ao-siena.toscana.it; PEC ao-siena@postacert.toscana.it;
- Responsabile della protezione dei dati personali: tel. 0577585593, e-mail: privacy@ao-siena.toscana.it; PEC: ao-siena@postacert.toscana.it ;
- Ufficio Relazioni con il Pubblico), indirizzo e-mail: urp@ao-siena.toscana.it Lotto didattico piano 1S. Orario: dal lunedì al venerdì 9.00 - 13.00; martedì e giovedì anche 14.30 - 16.30 Telefono: 0577 585518 - Fax: 0577 585488.

Per quanto concerne, infine, la modulistica aziendale completa relativa al Dossier Sanitario Elettronico e all'esercizio dei diritti da parte dell'interessato, si fa rinvio alla relativa pubblicazione nella sezione *Privacy* del sito internet della Azienda ospedaliero – universitaria Senese.

5. PARTE SECONDA – Il Titolare del trattamento ed altre figure

5.1. TITOLARE del Trattamento

Il ***"Titolare"*** del trattamento dei dati personali è la persona fisica, giuridica, la Pubblica Amministrazione, e qualsiasi altro Ente, Associazione od organismo cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, compreso il profilo della sicurezza.

Il Titolare del trattamento dei dati personali, ai sensi e per gli effetti del vigente Codice della Privacy, è l'Azienda ospedaliero – universitaria Senese, nella persona del suo Direttore Generale, in qualità di legale rappresentante dell'Azienda stessa, con sede in viale Bracci, 14 SIENA.

Il Titolare, avvalendosi della supervisione e collaborazione del ***RPD – Responsabile della Protezione dei Dati aziendale*** (vedi paragrafo 5.3), provvede:

- a richiedere al Garante per la protezione dei dati personali l'eventuale autorizzazione al trattamento dei dati personali, nei casi previsti dalla vigente normativa e ad assolvere all'eventuale obbligo di notificazione e comunicazione;
- a nominare con atto deliberativo i *Responsabili del trattamento dei dati personali,* impartendo ad essi, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato previsti dall'art. 7 del Codice della Privacy e all'articolo 12 del Regolamento UE, all'adozione delle misure di sicurezza per la conservazione, alla protezione e sicurezza dei dati;
- a nominare il Responsabile della Protezione dei Dati (RPD), come stabilito dall'articolo 37 del Regolamento UE;
- a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;
- a mettere in atto misure tecniche e organizzative adeguate a garantire che il trattamento dei dati sia effettuato conformemente al presente Regolamento.

Si dà evidenza, inoltre, del fatto che il Regolamento UE pone con forza l'accento sulla **"responsabilizzazione"** (***accountability*** nell'accezione inglese) di Titolari e Responsabili, ovverosia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (si veda la sezione 7 del Regolamento).

Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai Titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

5.2. CONTITOLARI del Trattamento

Come stabilito dall'articolo 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.

5.3. RESPONSABILE AZIENDALE della Protezione dei Dati

Il Regolamento Europeo impone la nomina del ***Data Protection Officer - DPO (***in italiano: **Responsabile della protezione dei dati -** '**RPD**'), nei termini di cui all'articolo 37, 38 e 39 del Regolamento medesimo.

La nomina del RDP è obbligatoria in tutte le organizzazioni, anche pubbliche, che trattano come attività principali i dati personali su larga scala, come ospedali, assicurazioni e istituti di credito.

Chi svolge la funzione di RPD, quindi, 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 RDP anche chi, solo in astratto, possa potenzialmente trovarsi in conflitto di interessi.

Si tratta di una figura dirigenziale o di un funzionario di alta professionalità, a metà tra il *consulente* ed il *revisore* e non dovrebbe ricoprire ruoli gestionali rispetto all'attività dell'azienda o ai fini istituzionali della Pubblica Amministrazione.

Ai sensi degli artt. 37 e 38 del Regolamento UE, il RPD deve:

- 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;
- essere tempestivamente e adeguatamente coinvolto dal Titolare o dal Responsabile in tutte le questioni riguardanti la protezione dei dati personali;
- adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse. In linea di principio, ciò significa che il RPD non può essere un soggetto che ricopre ruoli gestionali e che decide sulle finalità o sugli strumenti del trattamento di dati personali;
- operare alle dipendenze del Titolare oppure sulla base di un contratto di servizio (nel caso di RPD esterno);
- disporre di risorse umane e finanziarie, messe a disposizione dal Titolare, per adempiere ai suoi scopi.

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

- sorvegliare l'osservanza del Regolamento, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione e delle finalità;
- informare, fornire consulenza e pareri al Titolare, ai Responsabili del trattamento dei dati e agli incaricati relativamente all'applicazione degli obblighi europei in materia;
- rispondere agli interessati in merito alle questioni relative al trattamento dei loro dati personali o all'esercizio dei loro diritti;
- collaborare con il Titolare, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA);
- informare e sensibilizzare il Titolare o il Responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;
- cooperare con il Garante e fungere da punto di contatto per il Garante su ogni questione connessa al trattamento;

- supportare il Titolare o il Responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un registro delle attività di trattamento.

Il Regolamento UE prevede la pubblicazione sul sito istituzionale dell'Ente dei "dati di contatto" del RDP: dati che debbono essere inseriti anche nelle informazioni aziendali sul trattamento dei dati ai sensi degli artt. 13 e 14 del RGPD così che il RDP sia agevolmente contattabile dai cittadini-utenti ma anche dal Garante per la Privacy.

5.4. RESPONSABILE (ESTERNO) del Trattamento Dei Dati

Nell'ambito della Azienda ospedaliero – universitaria senese, sono inoltre individuati quali Responsabili del trattamento dei dati personali, tutti i soggetti esterni che, per svolgere la propria attività sulla base di una convenzione o un contratto sottoscritto con l'Azienda, trattino dati di cui è Titolare l'Azienda stessa e qualora siano in possesso dei requisiti previsti dalla vigente normativa (esperienza, capacità ed affidabilità).

In ottemperanza all'articolo 28 del Regolamento Europeo 2016/679, i Responsabili esterni vengono nominati con la sottoscrizione di un apposito *atto*, il cui schema è approvato con deliberazione del Direttore Generale e pubblicato nel sito istituzionale dell'AOUS alla sezione "Privacy; l'accettazione della nomina e l'impegno a rispettare le disposizioni del presente Regolamento è condizione necessaria per l'instaurarsi del rapporto giuridico fra le Parti.

L'atto di nomina sottoscritto da parte del Titolare del trattamento e controfirmato per accettazione da parte del Responsabile deve essere richiamato dagli accordi, convenzioni o contratti che prevedono l'affidamento di trattamenti di dati personali esternamente all'Azienda.

La predisposizione dell'atto di nomina è a cura dei RES/DEC dei contratti nominati dall'AOUS con la collaborazione dell'Ufficio Privacy aziendale e della UOC Gestione logistica, economale, contratti e rapporti con Estar.

5.5. PREPOSTO alla Gestione delle Attività di Trattamento dei Dati

Il D.lgs. n. 196/2003, come novellato dal recente D.lgs. n. 101/2018 di armonizzazione del Codice italiano della Privacy alle novità del RGPD Europeo n. 2016/679, stabilisce, al nuovo 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'Azienda ospedaliero – universitaria Senese, in qualità di Titolare del trattamento di dati personali (di seguito "Azienda" o "Titolare"), cioè quale soggetto che determina le finalità e i mezzi dei trattamenti dei dati effettuati nel proprio ambito, 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.

Quindi, con il sistema delle *deleghe* di cui si tratta, sono stati delegati con la deliberazione aziendale n. 1008/2018 i professionisti di questa Azienda che, per il ruolo ricoperto ed in virtù dei poteri di organizzazione e gestione già conferiti da questa stessa Azienda, risultano possedere i requisiti necessari per essere delegati, da parte del Datore di Lavoro, anche all'esercizio delle funzioni di gestione, coordinamento e controllo, le attività di trattamento dei dati personali svolte nell'ambito delle rispettive strutture nonché dei correlati adempimenti previsti dal RGPD.

Detti soggetti, denominati **Preposti** al trattamento dei dati personali sono stati individuati nelle seguenti, specifiche figure:

- Direttori titolari di incarico di Unità Operativa Complessa **(UOC),** di Unità Operativa Semplice Autonoma **(UOSA)** e di Unità Operativa Semplice **(UOS)**, e ai Direttori titolari di incarico "ad interim" o di "facente funzione", attribuito ai sensi delle vigenti disposizioni delle Aree Contrattuali della Dirigenza Medica e Veterinaria e della Dirigenza Sanitaria, Professionale, Tecnica e Amministrativa - già denominati "Preposti", per l'adempimento dei compiti e delle funzioni analiticamente indicati nell'atto di nomina, in materia di trattamento dati personali nell'ambito delle proprie aree di competenza e responsabilità;

- Titolari di incarico di Responsabile di **Unità Operativa Professionale** Diagnostica per Immagini, Unità Operativa Professionale Diagnostica di Laboratorio e Unità Operativa Professionale Personale della Riabilitazione, per l'adempimento dei compiti e delle funzioni analiticamente indicati nell'atto di nomina, in materia di trattamento dati personali nell'ambito delle proprie aree di competenza e responsabilità, in ragione dell'incarico di posizione organizzativa conferito;

I Preposti al trattamento devono sottoscrivere l'atto di delega conferita assumendo tutte le responsabilità dei compiti e delle funzioni attribuite e oggetto di delega, mentre in capo al Titolare permangono il potere di controllo e il potere di avocazione/sostituzione in caso di inerzia del delegato.

I Preposti provvedano inoltre a nominare con atto scritto il personale afferente alla struttura da essi diretta quali "**Incaricati**" del trattamento dati personali (vedi paragrafo successivo), fornendo loro adeguate istruzioni, utilizzando apposito modello disponibile sulla intranet aziendale alla sezione *"Moduli e documenti > Privacy.*

5.6. INCARICATO (INTERNO ED ESTERNO) del Trattamento dei Dati

Sulla base del principio europeo di accountability, il Titolare, nell'ambito del proprio assetto organizzativo, ha stabilito che i Preposti effettuino a loro volta la nomina degli "Incaricati" al trattamento dei dati personali dei dipendenti (o collaboratori con altra forma di impiego) che operano, secondo precise istruzioni, sotto le proprie direttive all'interno delle Strutture assegnate in qualità di persone autorizzate ad effettuare i trattamenti di dati personali nell'ambito delle loro specifiche competenze.

Gli incaricati interni del trattamento dei dati

Al momento dell'ingresso in servizio quindi ogni *dipendente* (oltre che ad ogni *collaboratore, contrattista* o *titolare di borsa di studio*) viene quindi formalmente nominato quale incaricato al trattamento dei dati" ai sensi dell'art. 2-quaterdecies comma 2 del D.lgs. 196/2003 e del Regolamento UE 2016/679 a cura del Preposto (Direttore UOC/UOSA/UOS/UOP di assegnazione), ricevendo anche le opportune "istruzioni operative" (sulla base di apposito schema disponibile sull'intranet aziendale).

Incaricati esterni del trattamento dei dati

Tutti coloro che svolgono un'attività di trattamento dei dati nell'ambito di questa Azienda, pur non essendo dipendenti e neppure titolari di incarichi di collaborazione, studio o contratti conferiti dalla medesima Azienda, debbono essere designati da parte del Responsabile (in questo caso "esterno") ai sensi dell'art. 28 del RGPD mediante una nota di nomina come incaricati/autorizzati esterni.

Allo stesso modo, l'Azienda in qualità di Titolare può designare taluni soggetti esterni che si trovino nella condizione di trattare dati personali sotto l'autorità del Titolare mediante una nota di nomina come incaricati/autorizzati esterni.

Ci si riferisce, a mero titolo esemplificativo, ai professionisti sanitari, al personale *tirocinante o* al *personale volontario* che opera temporaneamente all'interno dell'Azienda in virtù di un accordo o di una convenzione con un Ente esterno pubblico o privato *(es. altra Azienda Sanitaria, Associazione di volontariato o Istituto scolastico)* per lo svolgimento di consulenze specialistiche, di tirocini formativi piuttosto che di attività di volontariato a sostegno dei pazienti ricoverati nei reparti ospedalieri.

Il personale di cui si parla è soggetto agli stessi obblighi cui sono sottoposti tutti gli incaricati "interni", in modo da garantire il pieno rispetto della tutela della riservatezza dei dati.

Nel caso di Incaricati esterni, ovviamente, l'accesso ai dati deve essere limitato, con particolare rigore, ai soli dati personali la cui conoscenza sia strettamente necessaria per l'adempimento dei compiti assegnati e connessi all'espletamento dell'attività prevista dall'accordo o dalla convenzione.

I soggetti in servizio già incaricati formalmente ma trasferiti successivamente presso una diversa Unità Operativa dovranno ricevere altra autorizzazione al trattamento dei dati da parte del nuovo Direttore della Struttura di nuova assegnazione.

Si precisa, infine, che le persone "Incaricate" potranno consultare, in ogni momento, la sezione dedicata alla *"Privacy"* contenuta nel sito web aziendale, all'interno della quale è pubblicata, e tenuta costantemente aggiornata dall'Ufficio Privacy, tutta la documentazione (europea, nazionale ed aziendale) relativa alla materia in rilievo.

6. PARTE TERZA – Diritti dell'Interessato

6.1. Informazioni sul Trattamento Dei Dati

Il principio di trasparenza previsto dall'art. 5, par. 1, lett. a) del RGPD impone ai titolari di informare gli interessati sui principali elementi del trattamento, al fine di renderli consapevoli sulle principali caratteristiche dello stesso.

L'Autorità Garante per la protezione dei dati personali, con il Provvedimento n.55 del 7 marzo 2019 ha ritenuto opportuno suggerire ai Titolari/Aziende Sanitarie di fornire all'interessato le informazioni previste dal Regolamento in modo progressivo, vale a dire fornire alla generalità dei pazienti/utenti le informazioni relative ai trattamenti che rientrano nell'ordinaria attività di erogazione delle prestazioni sanitarie e fornire gli elementi informativi relativi a particolari attività di trattamento ai soli pazienti/utenti effettivamente interessati.

Come stabilito dall'articolo 13 del Regolamento Europeo 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:**

- l'identità e i dati di contatto del Titolare del trattamento e, ove applicabile, del suo rappresentante;
- i dati di contatto del Responsabile della protezione dei dati (RPD);
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- se il trattamento è necessario per il perseguimento del legittimo interesse del Titolare del trattamento o di terzi;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- ove applicabile, l'intenzione del Titolare del trattamento di trasferire dati personali a 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:

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

L'Azienda ospedaliero – universitaria Senese ha pubblicato ed affisso in tutte le sale di attesa e nei Reparti una informativa generale per tutti gli utenti dei servizi sanitari. Ha inoltre predisposto ulteriori informative (sempre pubblicati sul sito internet aziendale) per specifici trattamenti di dati personali.

Per quanto concerne il **periodo di conservazione** dei dati personali raccolti da questa Azienda, 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, sia fa rinvio al vigente **Massimario (Prontuario) aziendale di conservazione e scarto,** pubblicato sul sito internet di questa Azienda e liberamente consultabile.

Per Massimario di conservazione e di scarto si intende l'elenco della tipologia dei documenti con il rispettivo tempo di conservazione (limitato o illimitato); detto strumento permette 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.

Alla luce dei principi suesposti, si rinvia ai vigenti moduli aziendali di *"Informativa"* (per utenti, lavoratori e fornitori) pubblicati sul sito web aziendale nell'apposita pagina web dedicata alla *"Privacy"*.

6.2. Consenso al Trattamento dei Dati: Principi Generali

Il RGPD stabilisce un generale divieto di trattamenti dei dati relativi alla salute.

Le deroghe al divieto generale di trattare le cc.dd. "categorie particolari di dati", tra cui rientrano quelli sulla salute, sulla base delle quali è ammesso il trattamento di tali dati, sono ora da individuarsi nell'art. 9 del Regolamento che elenca una serie di eccezioni che rendono lecito il trattamento e che, in ambito sanitario, sono riconducibili, in via generale, ai trattamenti necessari per:

a**) motivi di interesse pubblico rilevante** sulla base del diritto dell'Unione o degli Stati membri (art. 9, par. 2, lett. g) del Regolamento), individuati dall'art. 2-sexies del Codice;

b) **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, sulla base del diritto dell'Unione o degli Stati membri che preveda misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale (art. 9, par. 2, lett. i) del Regolamento e considerando n. 54) (es. emergenze sanitarie conseguenti a sismi e sicurezza alimentare);

c) **finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali** (di seguito "finalità di cura") sulla base del diritto dell'Unione/Stati membri o conformemente al contratto con un professionista della sanità, (art. 9, par. 2, lett. h) e par. 3 del Regolamento e considerando n. 53; art. 75 del Codice) effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza.

Con riferimento alla lettera c**) finalità di cura,** si precisa che i trattamenti per "finalità di cura", sulla base dell'art. 9, par. 2, lett. h) e par. 3 del RGPD, sono propriamente quelli effettuati **da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza**.

Diversamente dal passato, quindi, il professionista sanitario, soggetto al segreto professionale, non deve più richiedere il consenso del paziente per i trattamenti necessari alla prestazione sanitaria richiesta dall'interessato, indipendentemente dalla circostanza che operi in qualità di libero professionista (presso uno studio medico) ovvero all'interno di una struttura sanitaria pubblica o privata.

Con riferimento ai trattamenti in ambito sanitario che richiedono il consenso esplicito dell'interessato (art. 9, par. 2, lett. a) del RGPD, l'Autorità Garante per la protezione dei dati personali ha indicato, nel Provvedimento n.55 del 7 marzo 2019, a titolo esemplificativo:

- consultazione del Fascicolo Sanitario Elettronico (FSE);
- consegna del referto online;
- utilizzo di app mediche;
- fidelizzazione della clientela;
- finalità promozionali o commerciali;
- finalità elettorali;
- trattamenti effettuati attraverso il Dossier Sanitario Elettronico (DSE).

Ulteriori indicazioni sono state fornite con il Provvedimento n.146 del 5 giugno 2019 (Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101):

- trattamento di dati genetici per finalità di tutela di un soggetto terzo;
- lo svolgimento dei test genetici nell'ambito delle investigazioni difensive o per l'esercizio di un diritto in sede giudiziaria;
- il trattamento effettuato mediante test genetici, compreso lo screening, a fini di ricerca o di ricongiungimento familiare;
- il trattamento effettuato per finalità di ricerca scientifica e statistica non previste dalla legge.

La norma, infine lascia agli Stati membri la possibilità di "mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute" (comma 4). In tal senso il legislatore italiano ha previsto agli articoli 2-septies e 75 del D.lgs. n. 196/2003 (come novellato dal D.lgs. n. 101/2018), misure di garanzia e regole deontologiche, fissate dall'autorità di controllo nazionale e riviste a cadenza biennale. Inoltre l'Autorità di controllo dovrà anche promuovere delle regole deontologiche per il trattamento dei dati relativi alla salute.

6.3. Diritto di Accesso dell'Interessato

Come stabilito dall'articolo 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 riguarda e in tal caso, di ottenere **l'accesso** ai dati personali e alle seguenti informazioni:

- le finalità del trattamento;
- le categorie di dati personali in questione;
- 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;
- quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- 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;
- il diritto di proporre reclamo a un'autorità di controllo;
- qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora 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 relative al trasferimento.

Il Titolare del trattamento fornisce, se richiesto, 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 esercitare i diritti sopra citati, l'interessato può inviare richiesta al Titolare o al Responsabile della Protezione dei Dati personali. L'interessato ha, altresì, diritto di presentare reclamo al Garante per la protezione dei dati personali. Il modulo per l'esercizio dei diritti è pubblicato nel sito web aziendale www.ao-siena.toscana.it nella sezione "*Privacy*".

Per quanto riguarda, invece, le modalità concrete per mezzo delle quali trova attuazione, nell'attuale contesto normativo ed organizzativo, il diritto di accesso, si fa espresso rinvio, in particolare, alle vigenti disposizioni normative in materia di "accesso documentale" (legge 241/1990 e ss.mm.ii.), di "accesso civico" e di "accesso civico generalizzato" (D.lgs.33/2017 e ss.mm.ii.) come disciplinate dal *Regolamento aziendale sul diritto di accesso*, tempo per tempo vigente.

6.4. Diritto di Rettifica, Cancellazione e Limitazione

Come stabilito dagli articoli 16, 17 e 19 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.
- la **cancellazione** dei dati personali che lo riguardano senza ingiustificato ritardo, se sussiste uno dei motivi seguenti:

  a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

  b) l'interessato revoca il consenso su cui si basa il trattamento, e se non sussiste altro fondamento giuridico per il trattamento;

  c) l'interessato si oppone al trattamento;

  d) i dati personali sono stati trattati illecitamente;

  e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento;

  Il diritto di cancellazione **non è applicabile** nella misura in cui il trattamento sia necessario:

  - per l'adempimento di un obbligo legale che richiede il trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
  - per motivi di interesse pubblico nel settore della sanità pubblica in conformità all'art.9, paragrafo 2, lettera h) e i) e dell'art. 9, paragrafo 3.
- 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 (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri Titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione".
- Il **diritto alla limitazione**: 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** *(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).* Il diritto alla limitazione prevede che il dato personale sia **"contrassegnato"** in attesa di determinazioni ulteriori; pertanto, è opportuno che il Titolare preveda nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

Per esercitare i diritti sopra citati, l'interessato può inviare richiesta al Titolare o al Responsabile della Protezione dei Dati personali.

L'interessato ha, altresì, **diritto di presentare reclamo all'Autorità Garante** per la protezione dei dati personali. Il modulo per l'esercizio dei diritti è pubblicato nel sito web aziendale www.ao-siena.toscana.it nella sezione "*Privacy*".

6.5. Diritto alla Portabilità Dei Dati

Si tratta di uno dei nuovi diritti previsti dal regolamento. Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche **c**ondizioni 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). L'esercizio di tale diritto non deve ledere i diritti e le libertà altrui.
Inoltre, il Titolare deve essere in grado di trasferire direttamente i dati portabili a un altro Titolare indicato dall'interessato, se tecnicamente possibile.
Il diritto alla portabilità dei dati non si applica ai trattamenti necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare.

6.6. Diritto di Opposizione

Come stabilito dall'articolo 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.

6.7. Processo Decisionale Automatizzato (Profilazione)

Come stabilito dall'articolo 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.

7. PARTE QUARTA – Sicurezza dei dati personali e misure di sicurezza di carattere organizzativo e tecnologico

7.1. Protezione dei Dati: Progettazione e Protezione per Impostazione Predefinita

L'articolo 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.

Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio (*"sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso",* secondo quanto afferma l'art. 25, paragrafo 1 del Regolamento UE) e richiede, pertanto, un'analisi preventiva ed un impegno applicativo da parte del Titolare che deve sostanziarsi in una serie di attività specifiche e dimostrabili.

7.2. Registro Elettronico delle Attività di Trattamento

Tutti i Titolari e i Responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio, devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'articolo 30 del medesimo 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'azienda o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio.

Il Registro, in virtù delle dimensioni e della complessità che caratterizzano l'Azienda non può che avere forma elettronica, e deve essere esibito su richiesta del Garante.

La tenuta del registro elettronico dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema tecnologico di corretta gestione dei dati personali.

7.3. Protezione e Sicurezza dei Dati Personali

L'art. 5, par. 1, lett. f) del RGPD, stabilisce che i dati personali devono essere "*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»)*". É importante notare che è l'intero trattamento a dover essere sicuro, non solo i dati come prodotto finale. Ciò comporta anche che le valutazioni di sicurezza vanno sviluppate per ogni tipo di trattamento.

Per questo motivo, non possono esistere dopo l'entrata in vigore del RGPD, obblighi generalizzati di adozione di misure "minime" di sicurezza poiché tale valutazione sarà rimessa, caso per caso, al Titolare e al Responsabile in rapporto ai rischi specificamente individuati.

L'articolo 32, paragrafo 1 del RGPD, ribadisce inoltre che le misure di sicurezza (tecniche ed organizzative) devono ***"garantire un livello di sicurezza adeguato al rischio***" del trattamento. Per ogni rischio occorre individuare la probabilità dell'evento, nonché la gravità dello stesso, in modo da stabilire le misure di sicurezza adeguate a mitigare il rischio.

Di seguito, a titolo esemplificativo:

Misure tecniche	Misure organizzative
• Gestione degli accessi • Autenticazione degli utenti • Aggiornamento degli applicativi • Conservazione e condivisione dei dati • Protezione dei dati trasmessi a terzi • Protezione dei dati archiviati • Protezione di dati, sistemi e reti • Impostazione dei log dei sistemi • Misure di Auditing	• Individuazione dei livelli di responsabilità • Informazione e formazione degli incaricati • Controllo dell'accesso ad archivi e basi dati • Redazione di istruzioni • Adozione distanze di cortesia agli sportelli e chiamata anonima • Divieto di esporre liste nominative nei reparti o locali aperti al pubblico • Riservatezza nei colloqui con pazienti e familiari

Sempre in base all'art. 32 del RGPD, "*l'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità …"* al principio di accountability".

Gli organismi rappresentanti di categorie o le associazioni di aziende possono cioè elaborare dei **c**odici di condotta che aiutino i titolari ad applicare correttamente il Regolamento europeo. I codici di condotta sono, quindi, delle misure di garanzia, che vengono sottoposti all'approvazione delle autorità di controllo nazionali, incaricate di vigilare sull'attuazione dei medesimi codici. Ovviamente il titolare, e il responsabile se nominato, dovranno tenersi sempre aggiornati sulla disponibilità e l'evoluzione dei codici di condotta.

Analogamente, l'adozione di processi di trattamento certificati può essere utilizzato a dimostrazione del concreto impegno da parte del titolare nell'attuazione del regolamento.

7.4. Notifica di una Violazione dei Dati Personali all'Autorità di Controllo

Tutti i Titolari, devono notificare all'Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza *"senza ingiustificato ritardo",* ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85 del Regolamento UE); questa procedura va sotto il nome di ***"Data Breach".*** Pertanto, la notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per i diritti degli interessati che spetta, ancora una volta, al Titolare.

Il Titolare e il Responsabile della protezione dei dati dell'Azienda devono quindi essere informati tempestivamente dell'esistenza di una violazione (si veda le "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento UE" adottate il 2/10/2017 ed emendate il 06/10/2018).

Il Titolare del trattamento, sentito il RPD aziendale, adotta quindi le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuto a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

La Procedura aziendale relativa alla "Violazione dei dati personali (c.d. Data Breach)" è disponibile nel sito internet (sezione *"Privacy"*) e sulla intranet aziendale (sezione "*Procedure aziendali*" > *"Documenti sanitari").*

7.5. Valutazione di Impatto sulla Protezione dei Dati (VIP)

Come evidenziato nel paragrafo 7.3, le misure di sicurezza devono *"garantire un livello di sicurezza adeguato al rischio*" del trattamento (articolo 32, paragrafo 1 del Regolamento UE).

Il rischio inerente al trattamento è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il Titolare ritiene di dover adottare per mitigare tali rischi.

L'art. 35 del RGPD prevede che quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

È previsto inoltre che l'Autorità di controllo - ovvero il Garante per la protezione dei dati personali - può redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'Autorità di controllo comunica tali elenchi al comitato.

In attuazione della norma europea, con il Provvedimento n.467 dell'11 ottobre 2018 l'Autorità Garante ha individuato l'elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto. Si tratta di trattamenti sistematici e non occasionali, riconducibili al criterio della "larga scala" sulla base dei seguenti fattori:

a. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;

b. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;

c. la durata, ovvero la persistenza, dell'attività di trattamento;

d. la portata geografica dell'attività di trattamento;"

Presso l'AOUS, sono competenti alla redazione della Valutazione d'impatto i Preposti individuati dal Titolare, sulla base di uno schema reso disponibile dall'Azienda con il supporto se necessario del RPD e Ufficio Privacy.

All'esito di questa valutazione di impatto, il Titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'Autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'Autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del Titolare e potrà, ove necessario, adottare tutte le misure correttive: dall'ammonimento del Titolare fino alla limitazione o al divieto di procedere al trattamento.

7.6. Trasferimento di Dati Personali All'estero

I trasferimenti di dati personali verso Paesi non appartenenti allo Spazio Economico Europeo (SEE, ossia UE + Norvegia, Liechtenstein, Islanda) o verso un'organizzazione internazionale sono consentiti a condizione che l'adeguatezza del Paese terzo o dell'organizzazione sia riconosciuta tramite decisione della Commissione europea (art. 45 del Regolamento UE 2016/679).

In assenza di tale decisione, il trasferimento è consentito ove il Titolare o il Responsabile del trattamento forniscano garanzie adeguate che prevedano diritti azionabili e mezzi di ricorso effettivi per gli interessati (art. 46 del Regolamento UE 2016/679).

7.7. Disciplina Aziendale sulla Videosorveglianza

Si fa rinvio alle disposizioni di cui al ***Regolamento aziendale*** tempo per tempo vigente, che disciplina la materia di cui si tratta (pubblicato sul sito aziendale alla sezione "*Privacy*").

7.8. Disciplina Aziendale sull'utilizzo dei Mezzi Informatici e Telematici

Si fa rinvio alle disposizioni di cui al ***Regolamento aziendale*** tempo per tempo vigente, che disciplina la materia di cui si tratta (pubblicato sulla Intranet aziendale alla sezione "*Documenti aziendali*".

7.9. Trattamenti per Ricerca e Sperimentazioni Cliniche

L'Azienda sostiene l'attività di ricerca e ne garantisce la gestione nel rispetto degli aspetti autorizzativi, normativo-regolatori e di protezione dei dati personali dei pazienti coinvolti. L'attività di ricerca si esplica previa specifica informativa da rendere agli interessati e previa raccolta del loro consenso, salve le deroghe sancite dall'Autorità Garante. Infatti, ferma restando l'applicazione dell'art.104 e ss. del Codice, le informazioni di cui agli artt.13 e 14 del Regolamento UE devono essere fornite in modo tale da mettere in grado gli interessati di distinguere con le attività di ricerca da quelle di tutela della salute e, comunque, devono rendere edotto il paziente in modo chiaro ed inequivocabile che le informazioni contenute nella cartella clinica saranno utilizzate ed eventualmente comunicate ad una o più aziende farmaceutiche e/o produttrici di dispositivi medico sanitari e/o chirurgici o di altri Enti o altri committenti pubblici e privati, indicate nominativamente e se i dati comunicati lo rendono identificabile o sono resi anonimi. E così, nello specifico agli interessati saranno sempre comunicate in maniera chiara e comprensibile tutte le informazioni riguardanti le modalità e i fini della ricerca.

In tale ambito l'Azienda/Titolare si avvale dello strumento della delega di funzioni, per attribuire le competenze e le responsabilità in materia di protezione dei dati personali e i relativi compiti, oltre a quelli ulteriori legati alla specifica attività, a ciascun Responsabile Scientifico volta per volta individuato nel provvedimento autorizzatorio per ciascun progetto di ricerca/sperimentazione clinica. Gli aspetti procedurali, amministrativi ed economici per la conduzione di ricerche e sperimentazioni cliniche sono definiti da apposito documento aziendale a cui si fa rinvio. Il trattamento dei dati genetici è consentito nei soli casi previsti dall'art. 9, par. 2 del Regolamento UE, nonché nel rispetto delle relative prescrizioni approvate dall'Autorità Garante nel Provvedimento del 5/6/2019 n. 146 che ha aggiornato, adeguandole al Regolamento UE, le prescrizioni di cui alla previgente n.8/2016 e delle misure di garanzia approvate dall'Autorità.

7.10. Codice di Comportamento dei Dipendenti e Collaboratori dell'Azienda

Si fa rinvio alle disposizioni di cui al ***Codice di comportamento aziendale*** tempo per tempo vigente, che disciplina la materia di cui si tratta pubblicato nel sito aziendale (sezione "*Amministrazione Trasparente" --->1. Disposizioni Generali---->2.Atti Generali--->4. Codice Comportamento* oppure alla pagina Intranet nella sezione" *Documenti Aziendali" --->Codice comportamento.*

8. PARTE QUINTA – Attuazione in ambito aziendale degli adempimenti europei

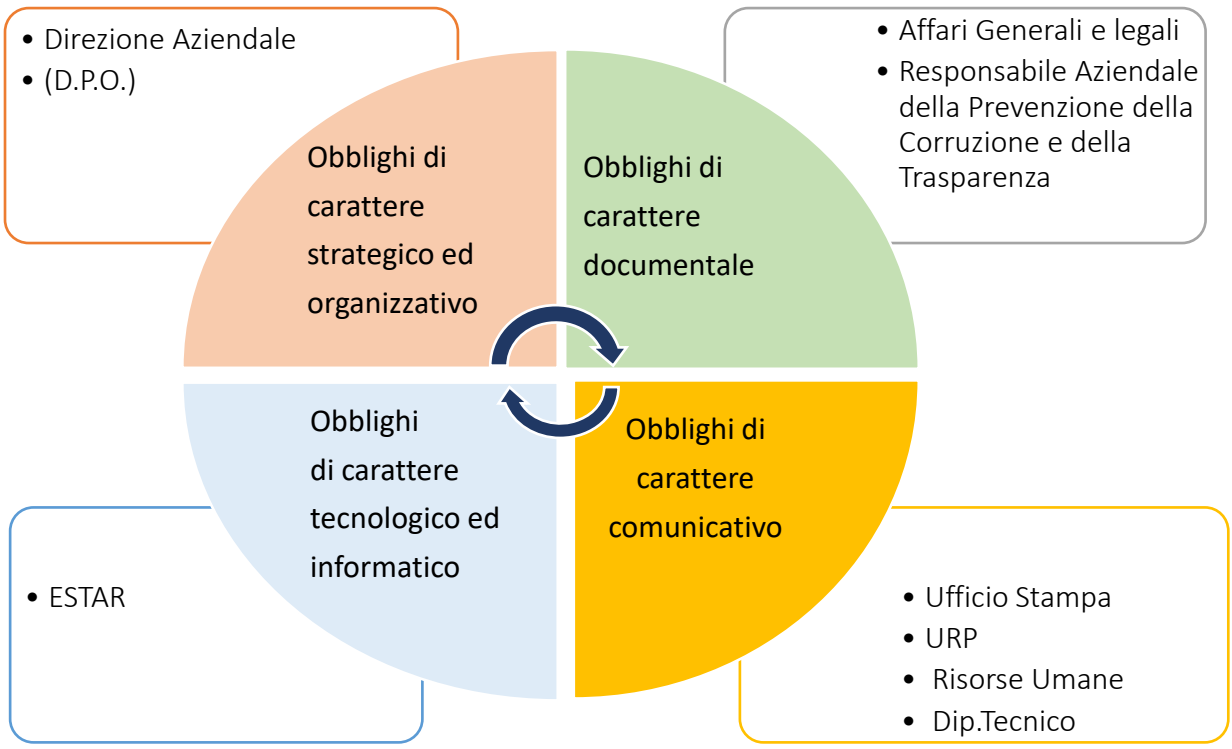
8.1. Ambiti di Attività' Aziendali Correlati agli Obblighi della Normativa

Risultano esservi **quattro tipologie di adempimenti** agli obblighi europei e quindi quattro 'macro-ambiti' di attività aziendali ad essi collegati, che verranno gestiti all'interno dell'azienda dall'Ufficio Privacy.

Il Regolamento europeo, infatti, detta obblighi di carattere:

- **strategico ed organizzativo**
- **documentale**
- **tecnologico ed informatico**
- **comunicativo**

Nel grafico che segue viene rappresentato il "ciclo di adempimenti" che questa Azienda ha posto in essere per realizzare la *Privacy europea*, individuando le strutture aziendali coinvolte nel medesimo ciclo, che verranno coordinate dal responsabile **dall'Ufficio Privacy** aziendale:



8.2. Entrata in vigore e Pubblicità

Il presente Regolamento entra in vigore dalla data di adozione con atto deliberativo del Direttore Generale.

Il Regolamento verrà pubblicato sul sito *internet aziendale* (nell'apposita sezione dedicata alla "P*rivacy*"), nonché sull'Intranet aziendale.

8.3. Disposizione Finale Relativa ai Documenti Tecnici Citati nel Regolamento

Per la consultazione di tutti i regolamenti, modelli e documenti tecnici citati nel testo del presente Regolamento, si fa espresso ed integrale rinvio sito internet aziendale alla sezione *"Amministrazione Trasparente"* e alla sezione dedicata alla "*Privacy*" all'interno delle quali la documentazione europea, nazionale ed aziendale relativa alla materia in rilievo è pubblicata e tenuta costantemente aggiornata a cura della dell'Ufficio Privacy.

8.4. Norma Finale

Per quanto non previsto nel presente Regolamento si fa rinvio alle norme europee, nazionali e regionali vigenti in materia. Il presente Regolamento è sottoposto ad aggiornamento periodico, in linea con le novità normative, giurisprudenziali e con le pronunce del Garante per la protezione dei dati personali.

9. RIFERIMENTI

La normativa di riferimento, a cui si rinvia per tutti gli aspetti non espressamente disciplinati dal presente regolamento, è la seguente:

- Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 "Regolamento Generale sulla Protezione dei Dati", conosciuto anche come RGPD;
- Decreto legislativo 30 Giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", come modificato dal decreto Legislativo 10 Agosto 2018, n. 101;
- Provvedimento del Garante della Privacy n. 55 del marzo 2019 recante: "Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario";
- Decreto del Presidente della Giunta regionale 26 ottobre 2021, n. 13 "Regolamento in attuazione dell'articolo 1, comma 1, della legge regionale 3 aprile 2006 n. 13 (Trattamento delle categorie particolari di dati personali e di quelli relativi a condanne penali e ai reati da parte della Regione Toscana, aziende sanitarie, enti, aziende e agenzie regionali e soggetti pubblici nei confronti dei quali la Regione esercita poteri di indirizzo e controllo).