Servizio Sanitario Nazionale - Regione Veneto
AZIENDA ULSS N. 8 BERICA
Viale F. Rodolfi n. 37 – 36100 VICENZA
COD. REGIONE 050–COD. U.L.SS.508 COD.FISC. E P.IVA 02441500242–Cod. iPA AUV
Tel. 0444 753111 - Fax 0444 753809 Mail protocollo@aulss8.veneto.it
PEC protocollo.centrale.aulss8@pecveneto.it
www.aulss8.veneto.it

REGOLAMENTO AZIENDALE

IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

sulla base del

Regolamento Europeo 2016/679 del 27 aprile 2016

*2^ Edizione aggiornata alla data del **02 Aprile 2019***

(1^ edizione originaria: 03 maggio 2018)

INDICE del Regolamento aziendale

PARTE PRIMA: INTRODUZIONE

PARTE SECONDA: DISPOSIZIONI GENERALI

PARTE TERZA: DIRITTI DELL'INTERESSATO

PARTE QUARTA: TITOLARE DEL TRATTAMENTO E ALTRE FIGURE

PARTE QUINTA: SICUREZZA DEI DATI PERSONALI E MISURE DI CARATTERE INFORMATICO E TECNOLOGICO

PARTE SESTA: ATTUAZIONE IN AMBITO AZIENDALE DEGLI ADEMPIMENTI EUROPEI

***

PARTE PRIMA: INTRODUZIONE

ARTICOLO 1): PREMESSA DI CARATTERE NORMATIVO

Il presente Regolamento 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**, anche conosciuto come **"GDPR"**), nell'ambito dell'organizzazione dell'Azienda U.L.SS. n. 8 Berica.

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 04 maggio 2016.

Ciò ha comportato il superamento, a far data dal 25 maggio 2018, delle disposizioni legislative di cui al previgente **Codice della privacy** (D.lgs. 196/2003 come successivamente modificato dal Legislatore italiano con il **D.lgs. 101 del 10 agosto 2018** di adeguamento al GDPR), 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 termine *accountability*, infatti, rinvia letteralmente al concetto di "resa di conto").

Questa Azienda ULSS n. 8 Berica, nella persona del Suo Direttore Generale, ha fatto proprio l'approccio del Legislatore europeo relativo all'*accountability* ed alla *compliance,* adottando, con congruo anticipo rispetto all'entrata in vigore del Regolamento UE, la **Deliberazione n. 86 del 24 gennaio 2018** ad oggetto *"Prime azioni di carattere organizzativo, gestionale e documentale volte ad ottemperare, nell'ambito dell'U.L.SS. n. 8 Berica, agli obblighi del Regolamento Europeo n. 2016/679 sulla privacy",* per poi proseguire ad adottare ulteriori delibere attuative della norma europea, anche sulla base delle indicazioni nel frattempo dettate da **Azienda Zero** (ente di governance della sanità veneta e di coordinamento delle aziende sanitarie della regione del Veneto), tra le quali spicca la **Deliberazione n. 153 del 30 gennaio 2019** ad oggetto *"Privacy europea: approvazione del nuovo Piano operativo di distribuzione delle competenze all'interno dell'ULSS n. 8 al fine di recepire le indicazioni fornite da Azienda Zero per l'attuazione del GDPR".*

Ciò detto, anziché allegare a questo Regolamento tutte le deliberazioni nonché la numerosa documentazione aziendale adottata sino ad oggi in attuazione del GDPR, pare preferibile rinviare, *in toto*, alla consultazione del **sito web aziendale.**

Il ***"sistema aziendale privacy"*** adottato dall'ULSS n. 8, in attuazione del principio europeo dell'*accountability*, è oggi infatti interamente fruibile nel sito internet **(www.aulss8.veneto.it)** di questa ULSS n. 8, nell'apposita pagina web denominata **"PRIVACY EUROPEA" (www.aulss8.veneto.it/privacy)**.

In detta pagina web è pubblicato l'intero **percorso di adeguamento** che, dal mese di gennaio 2018 ad oggi, l'ULSS n. 8 ha posto in essere per ottemperare alle previsioni europee e sono disponibili i testi normativi, gli opuscoli descrittivi del Garante Privacy, il presente Regolamento aziendale in materia di protezione dei dati personali e tutti i documenti *tecnici* e le nuove *modulistiche* aziendali relative alla materia in rilievo.

La pagina di cui si tratta contiene diverse **"sezioni"**, rispetto alle quali – a partire dal mese di gennaio 2018 e *pro futuro* – trovano progressivo inserimento (in ciascuna sezione e a seconda dei diversi argomenti) i nuovi regolamenti e le nuove modulistiche che, man mano, vengano approvate; obiettivo di questa ULSS 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.

Le suddette "sezioni" sono, al momento di approvazione della presente versione del regolamento, le seguenti (per il contenuto delle medesime si rinvia, come detto, alla consultazione del sito web aziendale):

1. *Accountability – Cronologia delibere emanate in attuazione delle norme europee*
2. *Responsabile della Protezione dei Dati (RPD) – Nomina e dati di contatto*
3. *Apparato giuridico-documentale: modulistica aziendale in materia di privacy europea*
4. *Registro elettronico delle attività di trattamento (adempimento GDPR)*
5. *Garanzia dei diritti degli interessati e gestione istanze in materia di privacy*
6. *Gestione del Risk Assessment e del Data Protection Impact Assessment*
7. *Applicazione del principio di Privacy by Design e Privacy by Default*
8. *Valutazione degli incidenti di sicurezza e gestione delle violazioni (Data Breach)*
9. *Privacy Europea: normativa generale e particolare*
10. *Privacy Europea: altra documentazione*
11. *Privacy Cookie Policy ULSS n. 8 Berica*
12. *Informazioni ed esercizio dei diritti*
13. *Link utili*

Il presente Regolamento aziendale 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 questa ULSS n. 8 Berica.

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.

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 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 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 questa ULSS, 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 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, con la consapevolezza di non affrontare un inutile gravame, bensì di contribuire concretamente al miglioramento della qualità del rapporto con l'utenza ed alla implementazione del "processo di umanizzazione" in corso di realizzazione, nell'ambito di questa ULSS, oramai da molti anni.

PARTE SECONDA: DISPOSIZIONI GENERALI

ARTICOLO 3): OGGETTO DEL REGOLAMENTO

Il presente Regolamento disciplina, all'interno dell'Azienda U.L.SS. n. 8 Berica, 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 REGOLAMENTO

L'Azienda 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, a prescindere dalla nazionalità o dalla residenza dell'interessato.

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

L'Azienda ULSS n. 8 Berica 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, come stabilito dal successivo articolo n. 27 del presente Regolamento, al quale si fa rinvio, al momento dell'ingresso in servizio è fornita, a cura della U.O.C. Gestione Risorse Umane, ad ogni dipendente *(oltre che ad ogni collaboratore, consulente o titolare di borsa di studio)* una specifica comunicazione in materia di privacy mediante apposita clausola inserita nel contratto di lavoro (o nella lettera di incarico per i summenzionati soggetti non dipendenti),

con la quale detti soggetti (dipendenti e non dipendenti) vengono nominati quali "autorizzati al trattamento dei dati" ai sensi del D.lgs. 196/2003 e del Regolamento UE 2016/679, impartendo loro anche le opportune *"istruzioni operative",* mediante consegna di un apposito foglio cartaceo.

Detta comunicazione conterrà anche i riferimenti per reperire il Regolamento aziendale sul sito internet nonché sullo spazio intranet aziendale, cosicché l'interessato, nel sottoscrivere il contratto di lavoro (o la lettera di incarico), sia reso edotto dell'esistenza del Regolamento e delle modalità di consultazione del medesimo.

ARTICOLO 6): DEFINIZIONI

Come stabilito dall'articolo n. 4 del Regolamento Europeo n. 2016/679, ai fini di questo disciplinare aziendale 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;

l) «**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;

m) «**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;

n) «**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;

o) «**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

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

p) «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 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'articolo n. 4 del Regolamento Europeo n. 2016/679 ed al D.lgs. 196/2003.

ARTICOLO 7): PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI

Come stabilito dall'articolo n. 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'articolo 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'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**»);*

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**»).*

Come stabilito dal Regolamento UE, il Titolare del trattamento (Direttore Generale dell'Azienda UL.SS. n. 8) è competente per il rispetto di quanto sin qui esposto ed è in grado di comprovarlo verso l'esterno (principio europeo dell'*«**accountability**»* o *«**responsabilizzazione**»).*

ARTICOLO 8): TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI (DATI SENSIBILI)

Come stabilito dall'articolo n. 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 articolo n. 9, tra le quali si evidenzia quella di cui alla lettera "h", applicabile a questa Azienda U.L.SS., 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 sulla 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 U.L.SS., 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 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 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"* (articolo n. 9, paragrafo n. 4).

Posto quanto sopra, si fa integrale rinvio agli **articoli 2-sexies, 2-septies e 2-octies del D.lgs. 196/2003** (come novellato dal D.lgs. 101/2018) contenenti specifiche disposizioni relative al trattamento delle categorie particolari di dati personali ed alle **"misure di garanzia"** per il trattamento dei **dati genetici, biometrici e relativi alla salute**.

ARTICOLO 9): TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI (DATI GIUDIZIARI)

Come stabilito dall'articolo n. 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 sulla base dell'articolo 6, paragrafo 1, 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'**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.

ARTICOLO 10): 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.

A tale proposito, in attesa di eventuali precisazioni da parte del Legislatore Regionale sulla base delle novità intervenute per effetto della normativa europea, si fa rinvio al **Regolamento della Regione Veneto** (tempo per tempo vigente) **per il trattamento dei dati personali sensibili e giudiziari** (di cui si dirà anche all'articolo 14 del presente regolamento), emanato in ottemperanza al Codice della privacy al fine di disciplinare le *"finalità di rilevante interesse pubblico perseguite".*

Detto documento permette di distinguere le diverse ipotesi (e le diverse modalità) in cui è possibile, oppure no, comunicare i dati (anche sensibili e giudiziari) verso l'esterno, sia che i destinatari della comunicazione siano soggetti pubblici sia che (assai più raramente) si tratti di soggetti privati.

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.

Il Dossier Sanitario Elettronico 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.

Ciascuna delle Strutture di questa ULSS n. 8 già dispone singolarmente della tecnologia digitale indispensabile alla gestione ed archiviazione dei dati sanitari del paziente: immagini radiografiche, tracciati, referti ed ogni altra tipologia di informazione sanitaria; ma, nel pieno rispetto della riservatezza dei dati personali e sensibili del paziente medesimo, ogni struttura aziendale (U.O.) può consultare esclusivamente le informazioni sanitarie prodotte e prescritte all'interno della struttura stessa. Per fare un esempio: la *U.O. Cardiologia non può conoscere, del paziente che ha in cura, gli esami ematochimici effettuati precedentemente presso altra struttura aziendale (U.O.).*

Nel Dossier Sanitario Elettronico, una volta costituito, confluiscono invece **tutte le informazioni sanitarie che riguardano uno stesso paziente presenti in questa Azienda ULSS**. 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 poter costituire un Dossier Sanitario Elettronico ed accedere a tutte le informazioni di cui si è detto, secondo normativa vigente e secondo prassi consolidata nell'ambito di questa ULSS, è necessario che il paziente rilasci, in forma orale e dopo aver letto l'apposita **nota informativa**, il proprio **consenso.**

Il cittadino / paziente può, inoltre, decidere, attraverso rilascio di specifico consenso orale, se inserire o non inserire nel Dossier Sanitario Elettronico le informazioni relative ad eventi sanitari pregressi all'istituzione del Dossier prodotti nell'Azienda ULSS n. 8 Berica.

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 ULSS 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.

L' **"Oscuramento" dell'evento clinico** (revocabile nel tempo) avverrà 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 *(cd. "Oscuramento dell'oscuramento").*

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'ULSS 8 Berica.

Criteri di profilazione degli utenti: 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"* 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.

I server presso cui sono custoditi i dati sono inoltre dotati di sistemi di *Back-up* e di sistemi antivirus e anti intrusione.

I medici di questa Azienda, che dovessero trovarsi ad operare in **situazioni di emergenza** potranno consultare il Dossier Sanitario Elettronico del paziente previa autorizzazione di un familiare del medesimo, o qualora ciò sia ritenuto indispensabile per la salvaguardia della salute di un terzo o della collettività.

I dati personali utilizzati per la costituzione del Dossier Sanitario Elettronico vengono trattati rispettando i **principi di correttezza, liceità, necessità e finalità** stabiliti dal Decreto Legislativo 196/2003 e osservando le misure di sicurezza previste dall'Allegato "B" - *Disciplinare Tecnico* del medesimo Decreto Legislativo.

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 196/2003):

- ✓ **revocare il consenso** ad alimentare il Dossier con l'inserimento di esami o referti *("istanza di revoca")*;
- ✓ esercitare la **facoltà di oscurare** eventi clinici che lo riguardano *("istanza di oscuramento")*;
- ✓ **esercitare il diritto di accesso ai dati personali** contenuti nel Dossier Sanitario Elettronico *("istanza di esercizio dei diritti");*
- ✓ **visionare gli accessi** che sono stati effettuati sul proprio Dossier Sanitario Elettronico da parte dei soggetti abilitati alla consultazione *("istanza di accesso")*;

Nella nota informativa, questa ULSS provvede quindi ad indicare espressamente le modalità per il contatto con il Titolare del Trattamento:

- PEC istituzionale dell'ULSS n. 8 Berica: protocollo.centrale.aulss8@pecveneto.it

- Punto di primo contatto, per il cittadino, per richieste di accesso o di chiarimenti relativamente al Dossier Sanitario Elettronico: UFFICIO RELAZIONI CON IL PUBBLICO, indirizzo e-mail: urp@aulss8.veneto.it / Telefono Segreteria: 044475-3535.

Per quanto concerne, infine, la modulistica aziendale completa relativa al Dossier sanitario Elettronico, si fa rinvio all'*Allegato n. 2* del presente Regolamento: modulistica che è già affissa anche nei locali di attesa delle prestazioni sanitarie, nonché pubblicata sul sito internet aziendale della ULSS n. 8 Berica.

ARTICOLO 12): FASCICOLO SANITARIO ELETTRONICO REGIONALE

Il Fascicolo Sanitario Elettronico Regionale (abbreviato "FSEr"), la cui istituzione è prevista dalla Legge, è l'insieme dei dati e dei documenti digitali di tipo sanitario e socio-sanitario, generati da eventi clinici presenti e trascorsi, riguardanti l'assistito.

L'avvento della digitalizzazione ha infatti rivoluzionato il mondo dei servizi, contribuendo a sviluppare nuove modalità con cui le istituzioni possono rispondere efficacemente ai bisogni dei cittadini. Questo vale anche per l'ambito sanitario: a tale proposito, la Regione del Veneto, in collaborazione con le aziende sanitarie ed ospedaliere e il coordinamento del Consorzio *Arsenàl.IT*, sta portando avanti la realizzazione del **Fascicolo Sanitario Elettronico regionale (FSEr),** ovvero lo strumento digitale nel quale in futuro tutti i dati relativi alla storia

sanitaria di un paziente (ricette farmaceutiche e specialistiche, referti di laboratorio, etc.) saranno raccolti, organizzati e resi accessibili allo stesso paziente e, solo per il tempo necessario e nel pieno rispetto della privacy, a chi lo prenderà in cura.

L'obiettivo è quello di abbattere tempi e costi, perché con la digitalizzazione, ove possibile, saranno i dati a spostarsi e non più le persone. Si tratta di un primo passo verso un mondo in cui, grazie alle tecnologie digitali, i dati e i servizi relativi alla salute siano sempre più facilmente disponibili, aggiornati, completi e rapidamente accessibili.

Il FSEr è alimentato in maniera continuativa, previo consenso libero e informato dell'assistito, dai soggetti che lo prendono in cura nell'ambito del Servizio Sanitario Nazionale (SSN) e dei Servizi socio-sanitari regionali - anche fuori dalla regione di residenza - e può essere da essi consultato, previo ulteriore consenso dell'assistito stesso.

L'accesso al FSEr permette agli operatori del SSN e dei Servizi socio-sanitari regionali, che hanno in cura l'assistito, di visualizzare tanto i dati sanitari più recenti, quanto **l'intera storia clinica**.

L'alimentazione dei dati del FSEr, quindi, ha lo scopo di documentare la storia clinica dell'assistito, al fine di ottimizzare le procedure di cura. Il FSEr si basa su tecnologie digitali che permettono di migliorare e semplificare le modalità di intervento sanitario.

La Regione del Veneto istituisce il Fascicolo Sanitario Elettronico regionale (FSEr): a tale proposito si rinvia ai contenuti pubblicati sul sito internet regionale alla sezione denominata ***"Sanità Km zero"*** (https://salute.regione.veneto.it/web/fser/cittadino/app-sanita-km-zero).

Anche questa ULSS n. 8 è impegnata nel processo di implementazione del FSEr, sulla base delle indicazioni regionali: a tale riguardo si rinvia al sito internet aziendale, alla scheda denominata *"Fascicolo sanitario Elettronico".*

ARTICOLO 14): CENSIMENTO DEI TRATTAMENTI E REGOLAMENTO REGIONALE

Questa Azienda ULSS evidenzia la necessità di avvalersi di un **censimento dei trattamenti dei dati personali** utile sia come strumento di lavoro e di disciplina della materia, sia come mezzo per implementare il contenuto del nuovo *"Registro elettronico delle attività di trattamento"* (vedasi il successivo articolo n. 30 del presente Regolamento).

A tale scopo, questa ULSS fa proprio il **Regolamento Regionale Veneto** (tempo per tempo vigente) **per il trattamento dei dati personali sensibili e giudiziari**, emanato in ottemperanza al Codice della privacy al fine di mappare i trattamenti effettuati per il perseguimento delle *"finalità di rilevante interesse pubblico"* quando non sia possibile perseguire le medesime finalità mediante l'utilizzo di dati anonimi oppure di dati personali non sensibili o giudiziari.

PARTE TERZA: DIRITTI DELL'INTERESSATO

ARTICOLO 14): INFORMAZIONI SUL TRATTAMENTO DEI DATI

Come stabilito dall'articolo n. 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 Responsabile della protezione dei dati (RPD);
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) qualora il trattamento si basi sull'articolo 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'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 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'articolo 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.

Per quanto concerne il **periodo di conservazione** dei dati personali raccolti da questa ULSS, 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 **Prontuario (Massimario) aziendale di conservazione e scarto,** pubblicato sul sito internet di questa ULSS e liberamente consultabile.
Per prontuario (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 modelli aziendali di *"Informativa"* (per utenti, lavoratori e fornitori) pubblicati sul sito web aziendale nell'apposita pagina web dedicata alla *"Privacy Europea".*

ARTICOLO 15): CONSENSO AL TRATTAMENTO DEI DATI: PRINCIPI GENERALI

Il Regolamento UE conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; i fondamenti di **liceità del trattamento** sono indicati all'art. 6 del Regolamento e coincidono, in linea di massima, con quelli previsti attualmente dal vigente Codice della privacy *(consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).*

Per quanto concerne la specifica disciplina del "consenso" in ambito sanitario e nel contesto del Servizio Sanitario Pubblico Nazionale, si fa espresso rinvio al contenuto dell'articolo **2-septies del D.lgs. 196/2003 (come novellato dal D.lgs. 101/2018)** rubricato ***"Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute".***

ARTICOLO 16): DIRITTO DI ACCESSO DELL'INTERESSATO

Come stabilito dall'articolo n. 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'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Oltre al rispetto delle prescrizioni relative alle modalità di esercizio di questo diritto, il Titolare può consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali.

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'articolo 46 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 e regionale nonché dal Garante per la privacy, con particolare riferimento all'ambito sanitario ed ospedaliero.

Si fa espresso rinvio, in particolare, alle vigenti disposizioni normative in materia di **"accesso documentale"**, di **"accesso civico**" e di **"accesso generalizzato"**, come disciplinate dal *Regolamento aziendale sul diritto di accesso*, tempo per tempo vigente.

Nel dare evidenza del fatto che, presso questa ULSS, la competenza sulla materia *de quo* è affidata al **Responsabile aziendale della Trasparenza e della Prevenzione della Corruzione** si rinvia al contenuto delle *schede informative* pubblicate sul sito internet aziendale (www.aulss8.veneto.it), dedicate all'argomento.

ARTICOLO 17): DIRITTO DI RETTIFICA

Come stabilito dall'articolo n. 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 18): DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO)

Come stabilito dall'articolo n. 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 (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" (si veda art. 17, paragrafo 2 del Regolamento UE).

Ha un campo di applicazione più esteso di quello di cui all'art. 7, comma 3, lettera b), del Codice della privacy, poiché l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento (si veda articolo 17, paragrafo 1).

ARTICOLO 19): DIRITTO DI LIMITAZIONE AL TRATTAMENTO

Si tratta di un diritto diverso e più esteso rispetto al "blocco" del trattamento di cui all'art. 7, comma 3, lettera a), del Codice: in particolare, è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì **anche se l'interessato chiede la rettifica dei dati** *(in attesa di tale rettifica da parte del titolare)* **o si oppone al loro trattamento ai sensi dell'art. 21 del regolamento** *(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.

ARTICOLO 20): DIRITTO ALLA PORTABILITA' DEI DATI

Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico).

Non si applica ai trattamenti non 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 21): DIRITTO DI OPPOSIZIONE

Come stabilito dall'articolo n. 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 22): 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.

PARTE QUARTA
TITOLARE DEL TRATTAMENTO E ALTRE FIGURE

ARTICOLO 23): 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 U.L.SS. n. 8 Berica, nella persona del suo Direttore generale, in qualità di legale rappresentante dell'Azienda stessa, con sede in viale Rodolfi n. 37 a Vicenza.

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

a) 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;

b) 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;

c) a nominare il Data Protection Officer, come stabilito dall'articolo 37 del Regolamento UE;

d) a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;

e) a mettere in atto misure tecniche e organizzative adeguate per 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, ovverossia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (si vedano artt. 23-25, in

particolare, e l'intero Capo IV 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.

Questa Azienda ULSS n. 8, nella persona del Suo Direttore Generale, ha fatto proprio l'approccio del Legislatore europeo relativo all'*accountability* sin dalla adozione della Deliberazione n. 86 del 24.01.2018 relativa alle "prime azioni" aziendali utili ad ottemperare alle previsioni legislative di matrice europea.

ARTICOLO 24): CONTITOLARI DEL TRATTAMENTO

Come stabilito dall'articolo n. 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 25): DELEGATO INTERNO ALLA GESTIONE DELLE ATTIVITA' DI TRATTAMENTO DEI DATI

Il D.lgs. 196/2003, come novellato dal recente D.lgs. 101/2018 di armonizzazione del Codice italiano della privacy alle novità del GDPR 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 ULSS n. 8 Berica, 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.

Ciò detto, anche sulla base delle indicazioni metodologiche ricevute da Azienda Zero, Ente di governance della sanità veneta, si rende necessario attribuire le ***deleghe*** di cui si tratta ai dirigenti di questa ULSS che, per il ruolo ricoperto ed in virtù dei poteri di organizzazione e gestione già conferiti da questa stessa ULSS, risultano possedere i requisiti necessari per essere delegati, da parte del Datore di Lavoro, anche all'esercizio delle funzioni di gestione, coordinamento e controllo delle attività di trattamento dei dati personali svolte nell'ambito delle rispettive strutture nonché dei correlati adempimenti previsti dal GDPR.

Tenuto conto del grado di complessità e soprattutto di vastità che caratterizza questa Azienda ULSS (azienda che consta, al 31.12.2018, di ben 6.000 dipendenti a tempo indeterminato), si reputa opportuno individuare i soggetti da "designare" ai sensi del D.lgs. 101/2018 in quelli stessi soggetti che, già nell'ambito della ex ULSS n. 6 'Vicenza' e nella ex ULSS n. 5 'Ovest Vicentino' così come nell'ambito della ULSS n. 8 Berica in base alla prima versione del Regolamento aziendale attuativo del GDPR adottato il 03 maggio 2018, ricoprivano le funzioni di *"Responsabile interno del trattamento dei dati".*

Detti soggetti, oggi definiti dal D.lgs. 101/2018 come ***"Delegati interni alla gestione delle attività di trattamento dei dati personali e degli adempimenti previsti dal Regolamento UE n. 2016/679"*** sono individuabili, in base al vigente Atto Aziendale, nelle seguenti, specifiche figure:

- I Direttori delle **UOC** (unità operative complesse) e delle **UOSD** (unità operative complesse a valenza dipartimentale) **dell'area dei Servizi Professionali, Tecnici ed Amministrativi dell'Azienda** *(come previste dall'articolo 31 del vigente atto aziendale)*;

- I Direttori delle **UOC** e delle **UOSD dell'area del Dipartimento di Prevenzione** *(come previste dall'allegato n. 2 del vigente atto aziendale)*

- I Direttori delle **UOC** e delle **UOSD dell'area Ospedaliera** *(come previste dall'allegato n. 3 del vigente atto aziendale)*

- I Direttori delle **UOC** e delle **UOSD dell'area Territoriale** *(come previste dall'allegato n. 4 del vigente atto aziendale)*

- I Direttori delle **UOC in staff alla Direzione Aziendale** *(come previste dall'articolo 38 del vigente atto aziendale)*

- I Responsabili delle **UOS *(non incardinate in una UOC)*, degli Uffici e delle Strutture collocate direttamente "in staff" alla Direzione Aziendale** *(come previste dall'articolo 38 del vigente atto aziendale)*, e qui di seguito richiamate per maggiore chiarezza:

- Ufficio Innovazione e Sviluppo Organizzativo
- Ufficio Relazioni col Pubblico
- UOS Servizio di Prevenzione e Protezione aziendale
- Medico Competente
- UOS Formazione
- Ufficio Trasparenza e Anticorruzione
- Ufficio Legale
- Nucleo Aziendale di Controllo
- UOS Risk Management
- UOS Qualità
- Interna Auditing
- UO per il Sociale
- Centrale Operativa Territoriale

Ciò premesso, questa ULSS provvede a conferire, con apposito atto deliberativo e con le conseguenti comunicazioni personali, le *deleghe* di cui si tratta ai Direttori / Responsabili delle strutture specificatamente richiamate qui sopra, relativamente all'esercizio delle **funzioni di gestione, coordinamento e controllo delle attività di trattamento dei dati personali,** svolte nell'ambito delle attività di competenza di ciascuna struttura di riferimento, e ciò al fine di ottemperare agli adempimenti previsti dal GDPR Europeo.

Inoltre, sulla base delle indicazioni ricevute da Azienda Zero, con il provvedimento succitato l'Azienda impartirà ai precitati "Delegati" le specifiche *istruzioni* ed i *compiti operativi* cui attenersi nell'esercizio della delega.

ARTICOLO 26): RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI

Nell'ambito della ULSS n. 8 Berica, sono inoltre individuati quali **Responsabili "esterni" 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'ULSS, trattino dati di cui è titolare l'ULSS medesima 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 verranno nominati con la sottoscrizione di un apposito ***"Accordo per la nomina a Responsabile Esterno del trattamento dei dati personali"***, il cui modello aziendale è pubblicato sul sito web aziendale nell'apposita pagina web dedicata alla *"Privacy Europea".*

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

Dopo l'approvazione del presente Regolamento, la UOC Affari Generali provvederà a

trasmettere il presente Regolamento ai tutte le strutture aziendali interessate, evidenziando la necessità di provvedere alle nomine dei *Responsabili esterni* utilizzando la nuova modulistica pubblicata anche sul sito web aziendale.

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.

ARTICOLO 27): AUTORIZZATO (INTERNO ED ESTERNO) DEL TRATTAMENTO DEI DATI

Il D.lgs. 196/2003, come novellato dal recente D.lgs. 101/2018 di armonizzazione del Codice italiano della privacy alle novità del GDPR stabilisce, al nuovo **articolo 2-quaterdecies, comma 2,** che il Titolare *"individui le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta".*

Ciò detto, sulla base delle indicazioni metodologiche ricevute da Azienda Zero, Ente di governance della sanità veneta e sulla base del principio europeo di *accountability*, si rende necessario individuare, nell'ambito di questa ULSS, le **persone *"autorizzate al trattamento dei dati"*** ai sensi dell'articolo 2-quaterdecies, comma 2, del D.lgs. 196/20013.

Tenuto conto del grado di complessità e soprattutto di vastità che caratterizza questa Azienda ULSS, si reputa opportuno individuare tali persone in quelli stessi soggetti che, nell'ambito della ex ULSS n. 6 'Vicenza' e nella ex ULSS n. 5 'Ovest Vicentino' così come nell'ambito della ULSS n. 8 Berica in base al Regolamento aziendale attuativo del GDPR adottato il 03maggio 2018, già ricoprivano le funzioni di *"Autorizzato interno del trattamento dei dati".*

Ciò detto, si stabilisce quanto segue:

- **Autorizzati interni del trattamento dei dati**: al momento dell'ingresso in servizio è fornita, a cura della U.O.C. Gestione Risorse Umane, ad ogni *dipendente* (oltre che ad ogni *collaboratore, consulente* o *titolare di borsa di studio*) una specifica comunicazione in materia di privacy mediante apposita clausola inserita nel contratto di lavoro (o nella lettera di incarico per i summenzionati soggetti non dipendenti), con la quale detti soggetti (dipendenti e non dipendenti) vengono nominati quali "autorizzati al trattamento dei dati" ai sensi del D.lgs. 196/2003 e del Regolamento UE 2016/679, impartendo loro anche le opportune "istruzioni operative", mediante consegna di un apposito foglio cartaceo.

Detta comunicazione conterrà anche i riferimenti per reperire il precitato Regolamento aziendale sul sito internet nonché sullo spazio intranet aziendale, cosicché l'interessato, nel sottoscrivere il contratto di lavoro (o la lettera di incarico), sia reso edotto dell'esistenza dell'anzidetto Regolamento e delle modalità di consultazione del medesimo.

- **Autorizzati esterni del trattamento dei dati:** tutti coloro che svolgono un'attività di trattamento dei dati nell'ambito di questa ULSS n. 8, pur non essendo dipendenti e neppure titolari di incarichi di collaborazione, studio o consulenza conferiti dalla medesima ULSS, debbono essere designati da parte del Responsabile (in questo caso

"esterno") tramite una lettera (o una nota) di nomina come autorizzati esterni.

Ci si riferisce, a mero titolo esemplificativo, 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. Associazione di volontariato o Istituto scolastico)* per lo svolgimento, appunto, 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.

Per quanto riguarda gli autorizzati "interni", va detto che, una volta individuati i medesimi soggetti nei termini di cui al presente Regolamento, questa ULSS provvederà, con apposito atto deliberativo, a impartire loro idonee istruzioni operative, approvando in tal senso l'apposito documento fornito da Azienda Zero e denominato ***"Istruzioni operative ai dipendenti e collaboratori ex articoli 29 e 32 del GDPR e 2-quaterdecies comma 2 del D.lgs. 196/20003".***

Quanto alla diffusione del documento in parola, la UOC Risorse Umane avrà cura di consegnare, al momento dell'ingresso in Azienda, dette "Istruzioni" ad ogni nuovo dipendente (oltre che ad ogni nuovo collaboratore, consulente o titolare di borsa di studio) affinché dette persone (dipendenti e non dipendenti) nominate quali "autorizzati al trattamento dei dati" siano, fin dall'inizio del rapporto di lavoro, resi edotti del contenuto delle istruzioni e adeguatamente istruiti sulla materia in rilievo e ciò per quanto concerne, appunto, i lavoratori e collaboratori neo-assunti.

Per quanto riguarda, invece, la maggior parte dei lavoratori, già in servizio presso questa ULSS, le "istruzioni" verranno pubblicate nella pagina web aziendale dedicata alla "Privacy Europea" provvedendo altresì a trasmetterle a tutti i dipendenti e collaboratori con una mail nella modalità "everyone" e pubblicandole anche nell' "Angolo del dipendente", così da assicurarne il massimo grado di pubblicità e diffusione.

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

ARTICOLO 28): RESPONSABILE AZIENDALE DELLA PROTEZIONE DEI DATI

Il Regolamento Europeo impone la nomina del ***Data Protection Officer*** (in italiano: **Responsabile della protezione dei dati** o '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 sensibili 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, 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.
Anche l'ULSS n. 8 Berica provvede al conferimento dell'incarico di cui si tratta, tenendo conto delle prescrizioni sin qui descritte.

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;
- ✓ **fornire consulenza e pareri** al Titolare, ai Responsabili del trattamento dei dati e agli incaricati relativamente all'applicazione degli obblighi europei in materia;
- ✓ 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**.

Ai sensi dell'articolo 37 del Regolamento UE, Egli 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;
- ✓ **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** (RPD esterno);

- ✓ **disporre di risorse umane e finanziarie**, messe a disposizione dal Titolare, per adempiere ai suoi scopi.

Il Regolamento UE prevede la pubblicazione *on line* del curriculum del RDP, nonché la pubblicazione sul sito istituzionale dell'Ente dei **"dati di contatto" del RDP**: dati che debbono essere inseriti anche nell'informativa aziendale sul trattamento dei dati, così che il RDP sia agevolmente contattabile dai cittadini-utenti ma anche dal Garante per la privacy.

PARTE QUINTA: SICUREZZA DEI DATI PERSONALI E MISURE DI CARATTERE INFORMATICO E TECNOLOGICO

ARTICOLO 29): PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA

L'articolo n. 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.

Per le modalità organizzative con le quali questa ULSS ha stabilito di ottemperare all'adempimento sin qui descritto, si fa espresso rinvio alle Deliberazioni n. 86 del 24.01.2018 e n. 153 del 30.01.2019 pubblicate sul sito web aziendale nell'apposita pagina web dedicata alla *"Privacy Europea".*

ARTICOLO 30): REGISTRO ELETTRONICO DELLE ATTIVITA' 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 (si veda l'articolo 30, paragrafo 5 del Regolamento UE), devono tenere un **registro delle operazioni di trattamento** i cui contenuti sono indicati all'articolo 30 del medesimo Regolamento.

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 questa Azienda ULSS n. 8 Berica (6.000 dipendenti al 31.12.2018), 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.

Si fa rinvio all'articolo 14 del presente Regolamento ad oggetto *"Censimento dei trattamenti e Regolamento regionale"* per ciò che concerne il rapporto tra il contenuto del predetto regolamento regionale e il nuovo Registro elettronico delle attività di trattamenti di questa ULSS.

Per le modalità organizzative con le quali questa ULSS ha stabilito di ottemperare all'adempimento sin qui descritto, si fa espresso rinvio alle Deliberazioni n. 86 del 24.01.2018 e n. 153 del 30.01.2019 pubblicate sul sito web aziendale nell'apposita pagina web dedicata alla *"Privacy Europea"*.

ARTICOLO 31): PROTEZIONE E SICUREZZA DEI DATI PERSONALI

Le misure di sicurezza devono ***"garantire un livello di sicurezza adeguato al rischio***" del trattamento (articolo 32, paragrafo 1 del Regolamento UE); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva ("tra le altre, se del caso").

Per lo stesso motivo, secondo il Regolamento UE non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento.

Si richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate.

Tuttavia, facendo anche riferimento alle prescrizioni contenute, in particolare, nell'Allegato "B" al Codice, l'Autorità potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni; inoltre, per alcune tipologie di trattamenti (quelli di cui all'art. 6, paragrafo 1, lettere c) ed e) del regolamento) potranno restare in vigore (in base all'art. 6, paragrafo 2, del regolamento) le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili: è il caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

Per le modalità organizzative con le quali questa ULSS ha stabilito di ottemperare all'adempimento sin qui descritto, si fa rinvio all'allegata Deliberazione n. 86 del 24.01.2018, che ha posto in capo alla U.O.C. Servizi Tecnici e Patrimoniale e sue relative UOS dell'area informatica, l'obbligo di predisporre le più idonee misure di sicurezza a livello informatico, anche curando l'aggiornamento (e la riedizione) del Documento Programmatico sulla Sicurezza (D.P.S.).

ARTICOLO 32): NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITA' DI CONTROLLO

A partire dal 25 maggio 2018, tutti i titolari, e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi, dovranno **notificare all'Autorità di controllo le violazioni di dati personali** di cui vengano a conoscenza e *"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 gli interessati che spetta, ancora una volta, al Titolare.

Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre *"senza ingiustificato ritardo";* fanno eccezione le circostanze indicate al paragrafo 3 dell'articolo 34 del Regolamento UE, che coincidono solo in parte con quelle attualmente menzionate nell'art. 32-bis del Codice. I contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli art. 33 e 34 del regolamento.

Il Titolare del trattamento, sentito l'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.

Per le modalità organizzative con le quali questa ULSS ha stabilito di ottemperare all'adempimento sin qui descritto, si fa espresso rinvio alle Deliberazioni n. 86 del 24.01.2018 e n. 153 del 30.01.2019 pubblicate sul sito web aziendale nell'apposita pagina web dedicata alla *"Privacy Europea".*

ARTICOLO 33): VALUTAZIONE DI IMPATTO (VIP) SULLA PROTEZIONE DEI DATI

Le misure di sicurezza devono ***"garantire un livello di sicurezza adeguato al rischio***" del trattamento (articolo 32, paragrafo 1 del Regolamento UE); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva ("tra le altre, se del caso").

Fondamentali fra tali attività correlate alla sicurezza sono quelle connesse al secondo criterio individuato nel Regolamento UE rispetto alla gestione degli obblighi dei titolari, ossia il **rischio inerente al trattamento.**

Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (si vedano considerando 75-77); tali impatti dovranno essere analizzati attraverso un apposito **processo di valutazione** (si vedano artt. 35-36) 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.

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 ai sensi dell'articolo 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

Per le modalità organizzative con le quali questa ULSS ha stabilito di ottemperare all'adempimento sin qui descritto, si fa espresso rinvio alle Deliberazioni n. 86 del 24.01.2018 e n. 153 del 30.01.2019 pubblicate sul sito web aziendale nell'apposita pagina web dedicata alla *"Privacy Europea".*

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.

Per le modalità organizzative con le quali questa ULSS ha stabilito di ottemperare all'adempimento sin qui descritto, si fa espresso rinvio alle Deliberazioni n. 86 del 24.01.2018 e n. 153 del 30.01.2019 pubblicate sul sito web aziendale nell'apposita pagina web dedicata alla *"Privacy Europea".*

ARTICOLO 35): 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 web aziendale).

ARTICOLO 36): 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 sul sito web aziendale).

ARTICOLO 37): CODICE DI COMPORTAMENTO DEI DIPENDENTI E COLLABORATORI DELL'AZIENDA

Si fa rinvio alle disposizioni di cui al ***Codice aziendale*** tempo per tempo vigente, che disciplina la materia di cui si tratta (pubblicato sul sito web aziendale).

PARTE SESTA
ATTUAZIONE IN AMBITO AZIENDALE DEGLI ADEMPIMENTI EUROPEI

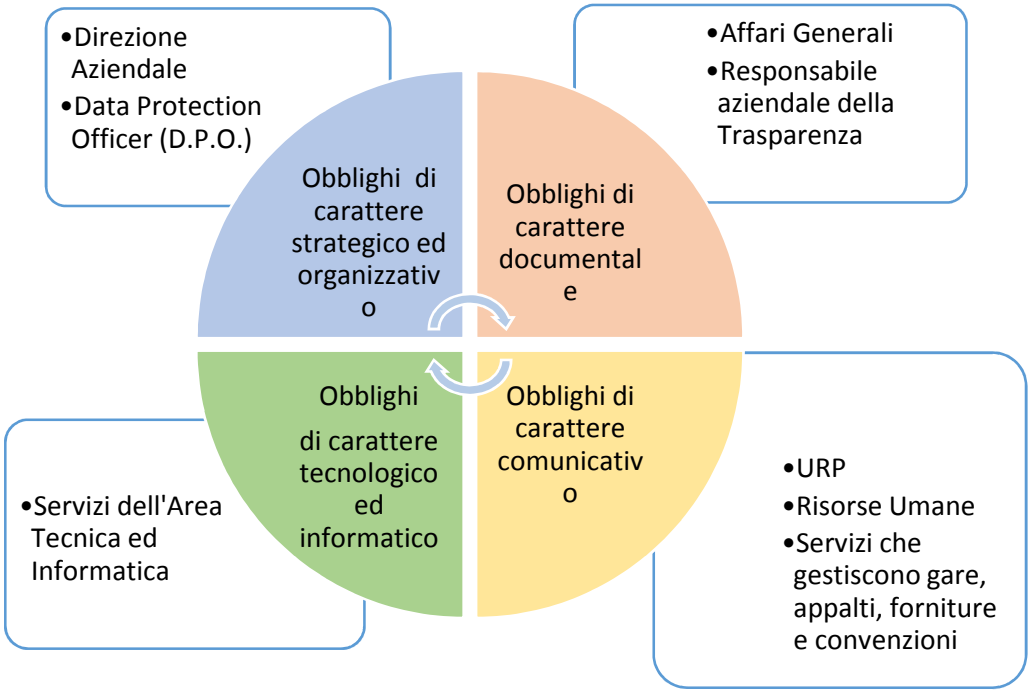
ARTICOLO 38): AMBITI DI ATTIVITA' AZIENDALI CORRELATI AI NUOVI OBBLIGHI EUROPEI

In base alla *Relazione tecnico-programmatica* approvata con la già citata **Deliberazione del Direttore Generale n. 86 del 24 gennaio 2018** (articolo n. 3) risultano esservi **quattro tipologie di adempimenti** agli obblighi europei e quindi quattro 'macro-ambiti' di attività aziendali ad essi collegati.

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, ai sensi della precitata Delibera n. 86/2018, questa ULSS ha posto in essere, sin dal mese di gennaio 2018, per realizzare la *privacy europea*, individuando le strutture dell'U.L.SS. n. 8 coinvolte nel medesimo ciclo:



Con la sopra citata **Delibera n. 86 del 24 gennaio 2018** è stata delineata una prima organizzazione dei compiti e delle responsabilità, a livello aziendale, utile a far fronte agli adempimenti del GDPR prima che lo stesso Regolamento entrasse in vigore, in modo da consentire alle diverse strutture dell'Azienda di intraprendere, in anticipo, le iniziative del caso.

Dopo l'entrata in vigore del D.lgs. 101/2018 (che ha novellato il D.lgs. 196/2003) e sulla base delle indicazioni nel frattempo emanate da Azienda Zero, è stata approvata la **Deliberazione n. 153 del 30 gennaio 2019** ad oggetto ***"Privacy europea: approvazione del nuovo Piano operativo di distribuzione delle competenze all'interno dell'ULSS n. 8 al fine di recepire le indicazioni fornite da Azienda Zero per l'attuazione del GDPR".***

Questa ultima delibera, pubblicata sul sito web aziendale a cui si fa rinvio, è il baricentro fondamentale sui cui si poggia l'attuale disciplina delle attività in quanto, ottemperando alle indicazioni di Azienda Zero e sulla base delle funzioni attribuite *ratione materiae* dall'atto aziendale alle diverse strutture dell'Azienda, individua in modo rigoroso "chi fa che cosa", attribuendo compiti e responsabilità.

Come si evince dal *"Piano operativo",* i complessi obblighi previsti dal GDPR investono, in modo trasversale e a tutti i livelli dell'Azienda, sia aspetti giuridici, che aspetti tecnologici ed informatici, piuttosto che statistici e di controllo e, pertanto, si è reso necessario, oltre che opportuno, coinvolgere più strutture aziendali diverse nel percorso di adeguamento al GDPR.

ARTICOLO 39): ENTRATA IN VIGORE E PUBBLICITA'

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, nuova sezione dedicata alla "privacy europea"), nonché sull*'Intranet* aziendale.

ARTICOLO 40): DISPOSIZIONE FINALE RELATIVA AI DOCUMENTI TECNICI CITATI NEL REGOLAMENTO: RINVIO AL SITO WEB AZIENDALE.

Per la consultazione di tutti i ***regolamenti, modelli*** e ***documenti tecnici*** citati nel testo del presente Regolamento, si fa espresso ed integrale rinvio alla **sezione dedicata alla "Privacy Europea" contenuta nel sito web aziendale**, all'interno della quale è pubblicata, e tenuta costantemente aggiornata a cura della UOC Affari Generali, tutta la documentazione (europea, nazionale ed aziendale) relativa alla materia in rilievo.

***