AZIENDA SOCIO- SANITARIA TERRITORIALE DELLA VALCAMONICA
Sede legale: Breno (Bs) - Via Nissolina, 2 - tel. 0364.3291 - fax 0364.329310 - CF/P.IVA n.03775830981
www.asst- valcamonica.it PEC: protocollo@pec.asst- valcamonica.it

Sistema Socio Sanitario
Regione Lombardia

INDICE

Ed.	Rev.	Data	Descrizione delle modifiche	Redazione	Verifica di conformità al SGQ	Approvazione
01	00	27.12.2021	Prima emissione	Avv. M. Bazzana	Dr.ssa B. Bertoli	Dr. M. Galavotti

VERIFICA E CONFERMA DEI CONTENUTI

Ed.	Rev.	Data	Approvazione

PARTE PRIMA – INTRODUZIONE

ARTICOLO 1) PREMESSA DI CARATTERE NORMATIVO

Nell'ambito dell'organizzazione dell'Azienda Socio Sanitaria della Valcamonica (di seguito anche ASST della Valcamonica), il Regolamento in materia di protezione dei dati personali (così detta "privacy") rappresenta uno strumento di applicazione del nuovo **Regolamento Europeo n. 2016/679** (General Data Protection Regulation, di seguito anche "Regolamento (UE)", "Regolamento Generale Protezione Dati" o "RGPD") e del vigente Decreto Legislativo 30 giugno 2003, n. 196 (cosiddetto "Codice sulla privacy") come modificato dal D.lgs. 10/08/2018 n. 101.
A far data dal 25 maggio 2018 trova diretta applicazione, sul territorio nazionale, l'anzidetto, nuovo Regolamento Europeo sulla privacy, approvato il 27 aprile 2016 e pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 04 maggio 2016.
Il RGPD disciplina la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché la libera circolazione di tali dati. Esso abroga la precedente Direttiva 95/46/CE.

Le prescrizioni stabilite dal RGPD trovano diretta ed immediata applicazione, indipendentemente dalla preesistenza di differenti norme nazionali in materia che, quindi, sono automaticamente superate dai precetti del Regolamento n. 2016/679, ove con essi in contrasto.
Le disposizioni legislative di cui al vigente Codice della privacy (*D.lgs. 196/2003 e ss.mm.ii.*), sono state adeguate dal D.lgs. 10/08/2018 n. 101, che tra l'altro ha abrogato le parti del D.lgs. n. 196/2003 incompatibili con le disposizioni del RGPD.
In attesa dell'emanazione da parte dell'Autorità Garante per la protezione dei dati personali di specifiche disposizioni regolamentari, continuano ad avere efficacia quelle emanate negli anni dalla stessa Autorità, che non siano contrastanti o incompatibili con quelle europee.
E' necessario pertanto dotarsi sin da ora di un apposito "Regolamento" che disciplini compiti, attività e *policy* interne che garantiscano l'assolvimento degli adempimenti (non pochi) imposti dalle norme europee.
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.

1.1 RIFERIMENTI E ABBREVIAZIONI

La redazione del presente documento è stata effettuata sulla base delle seguenti fonti normative:
– Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
– Decreto Legislativo n. 196/2003 (c.d. Codice Privacy) così come novellato dal D.lgs. n. 101/2018
– Titolario e Massimario del Sistema Sociosanitario lombardo Revisione 04 del 2018;
– Autorizzazioni, provvedimenti, linee guida, relazioni e comunicati stampa del Garante per la protezione dei dati personali;
– P DMP 001 "Gestione Delle Attività Della Direzione Medica Di Presidio";
– PT DMP 001 "Gestione della Cartella clinica";
– Atti, procedure e modelli aziendali;
– Norme comportamentali desunte dalla miglior prassi.
Per quanto riguarda gli acronimi, si fa riferimento al M GEN 004 "Elenco acronimi, sigle e simboli".

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 all'ente, 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 Azienda Socio Sanitaria Territoriale, che deve impegnarsi perché la cultura

di cui si tratta possa crescere e rafforzarsi, principalmente fra gli operatori delle attività sanitarie, 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.

ARTICOLO 3) PREMESSA DI CARATTERE METODOLOGICO

Il presente Regolamento dovrà essere integrato da una serie di **Disposizioni Attuative**, alcune di queste già adottate ed altre in corso di preparazione, necessarie a dare compiuta attuazione, sia verso l'interno che verso l'esterno, ai dettami della nuova "privacy europea": documenti ai quali viene data massima pubblicità e diffusione, tramite la pubblicazione sul sito *internet* aziendale, nella rete intranet e mediante invio alle caselle di posta elettronica di dipendenti e collaboratori.
In particolare troveranno idonea e specifica attuazione: a) la disciplina dei diritti e delle modalità di esercizio degli stessi da parte degli interessati; b) le procedure di gestione dei c.d. "Data Breach"; c) la disciplina aziendale sull'utilizzo dei mezzi informatici e telematici, nonché eventuali ed ulteriori Disposizioni Attuative a loro volta necessarie a dare piena attuazione al presente Regolamento.

E' doveroso infatti rimarcare, sin da ora, che il principio cardine introdotto dal nuovo Regolamento (UE) 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.

ARTICOLO 4) RESPONSABILITÀ

La procedura è redatta dal Responsabile per la Protezione dei Dati (RPD) ed è validata dalla Direzione Generale che ne è responsabile. La responsabilità della corretta applicazione della procedura è attribuita al Titolare, ai Responsabili interni privacy di area ed agli incaricati del trattamento dei dati personali, ciascuno in relazione all'ambito di rispettiva competenza.

PARTE SECONDA - DISPOSIZIONI GENERALI

ARTICOLO 5) OGGETTO DEL REGOLAMENTO

Il Regolamento aziendale disciplina, all'interno dell'ASST della Valcamonica, 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
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*).
L'ASST della Valcamonica adotta, in materia di sicurezza, misure tecniche ed organizzative per garantire un livello di sicurezza adeguato ai rischi di distruzione o perdite anche accidentali dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta.
L'Azienda adotta altresì misure occorrenti per facilitare l'esercizio dei diritti degli interessati.

ARTICOLO 6) FINALITÀ DEL REGOLAMENTO

Con il presente Regolamento, l'Azienda Socio Sanitaria Territoriale della Valcamonica, quale titolare del trattamento, intende dare attuazione al principio cardine del Regolamento (UE) 2016/679 di "***accountability***" ovvero "responsabilizzazione", che si concretizza nel mettere in atto misure adeguate

ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il RGPD, compresa l'efficacia delle misure di sicurezza adottate (art. 5 par. 2 RGPD).
L'Azienda, con questo strumento e con le sue disposizioni attuative, intende documentare le misure tecniche ed organizzative adottate al fine di ottemperare alle disposizioni del predetto RGPD e garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza, all'identità personale ed al diritto alla protezione dei dati personali degli utenti, dei dipendenti, degli operatori e di tutti coloro che hanno rapporti con l'Azienda stessa.

ARTICOLO 7) SENSIBILIZZAZIONE
L'ASST della Valcamonica 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 momento dell'ingresso in servizio, o per il personale già in forza all'Ente al momento dell'entrata in vigore del presente Regolamento, è fornita, a cura di ciascun Responsabile interno privacy di area (*oltre che ad ogni collaboratore, consulente, tirocinante, volontario, ecc.*) una specifica comunicazione, con la quale detti soggetti (dipendenti e non dipendenti) sono nominati quali "**incaricati ed autorizzati al trattamento dei dati**" ai sensi del D.lgs. 196/2003 e ss.mm.ii. e del Regolamento (UE) 2016/679, fatte salve debite eccezioni in relazione alla natura dell'incarico.
Agli stessi viene consegnata, sita tramite la rete intranet aziendale che a mezzo di posta elettronica, una copia del presente Regolamento e delle Disposizioni Attuative approvate.
Il Regolamento contiene, infatti, tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale e il dipendente (o il non dipendente nei termini di cui si è detto sopra), nel sottoscrivere il contratto di lavoro (o la lettera di incarico), è reso edotto dell'esistenza dell'anzidetto Regolamento e delle modalità di consultazione del medesimo.

ARTICOLO 8) DEFINIZIONI
Come stabilito dall'articolo 4 del Regolamento Europeo n. 2016/679, ai fini di questo Regolamento 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) «**titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
h) «**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;
i) «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare;
j) «**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;
k) «**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;
p) «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento (UE).

ARTICOLO 9) PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI

Come stabilito dall'articolo 5 del Regolamento Europeo n. 2016/679, i dati personali di utenti, personale, collaboratori e di chiunque abbia a fornire i propri dati all'ASST della Valcamonica, 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***»);
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***»).

Il Titolare del trattamento (Direttore Generale dell'ASST della Valcamonica) 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 10) TRATTAMENTO DI DATI PERSONALI
Il Regolamento (UE) conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica.
I fondamenti di **liceità del trattamento**, previsti all'art. 6 del Regolamento medesimo, vengono di seguito elencati:
- L'interessato o chi ne ha la rappresentanza legale ha espresso il **consenso** al trattamento dei dati personali per una o più specifiche finalità.
- Il trattamento è necessario nell'ambito di un **contratto** o ai fini della conclusione di un contratto.
- Il trattamento è effettuato in conformità ad un **obbligo di legge** al quale il Titolare del trattamento è soggetto.
- Il trattamento è necessario per la **salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica.
- Il trattamento è necessario per l**'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri** di cui è investito il Titolare del trattamento.
- Il trattamento è necessario per il **perseguimento del legittimo interesse** del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Per quanto concerne il trattamento basato sul "consenso", si chiarisce che:
- il consenso deve essere "**esplicito**";
- non deve essere necessariamente "**documentato per iscritto**", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito"; inoltre, il Titolare deve essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento;
- **il consenso dei minori** è valido a partire dai 16 anni: prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci (articolo 8 del RGPD);
- deve essere, in tutti i casi, **libero, specifico, informato e inequivocabile** e non è ammesso il consenso tacito o presunto (non è quindi possibile utilizzare "caselle pre- spuntate" su un modulo);
- deve essere manifestato attraverso "**dichiarazione o azione positiva inequivocabile**" (per approfondimenti, si vedano considerando 39 e 42 del RGPD).

ARTICOLO 11) TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI (EX DATI SENSIBILI)
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, paragrafo n. 2 tra le quali si evidenziano, in quanto applicabili a questa Azienda, quelle di seguito indicate:
- **lettera b)** *applicabile in generale ai "Datori di Lavoro", ai sensi della quale "il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia*

autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato";
- **lettera g)** *applicabile a questa Azienda ai sensi del quale: "il trattamento è necessario per motivi di* ***interesse pubblico rilevante*** *sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato*", nei casi individuati dall'art. 2- sexies del Codice della Privacy;
- **lett. h)**, *applicabile a questa Azienda qualora il trattamento sia necessario per 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, 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* (par. 3 del Regolamento e considerando n. 53, art. 75 del Codice della Privacy);
- **lett. i**), applicabile a questa Azienda qualora il trattamento sia necessario *per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, 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* (es. emergenze sanitarie conseguenti a sismi e sicurezza alimentare).

Ciò non esclude che a seconda dello specifico trattamento effettuato, non possa ritenersi applicabile al caso concreto una delle altre deroghe previste dall'art. 9 del Regolamento.

Si precisa che i trattamenti per "**finalità di cura**", sulla base **dell'art. 9, par. 2, lett. h) e par. 3** del Regolamento, 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.
Per quanto riguarda l'ambito oggettivo, si precisa che i trattamenti di cui all'art. 9, par. 2, lett. h) sono solo quelli "necessari" al perseguimento delle specifiche "**finalità di cura**" previste dalla norma, cioè quelli essenziali per il raggiungimento di una o più finalità determinate ed esplicitamente connesse alla cura della salute (cfr. considerando 53 del Regolamento).
Gli eventuali trattamenti attinenti, solo in senso lato, alla cura, ma non strettamente necessari, richiedono, quindi, anche se effettuati da professionisti della sanità, una distinta base giuridica da individuarsi, eventualmente, nel consenso dell'interessato o in un altro presupposto di liceità (artt. 6 e 9, par. 2, lett. a, del Regolamento).
Il consenso espresso dell'interessato (art. 9 par. 2 lett. a), in base alle disposizioni normative ed alle indicazioni dell'Autorità di Controllo (Garante della Privacy) vigenti al momento dell'adozione del presente Regolamento aziendale, è ancora richiesto quale legittima base giuridica, tra gli altri casi, per i seguenti trattamenti:
- a) referto on line;
- b) fascicolo sanitario elettronico;
- c) dossier sanitario elettronico.

ARTICOLO 12) TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI (EX DATI GIUDIZIARI)
Come stabilito dall'articolo 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."*
Il Codice novellato ha demandato al Ministero della Giustizia con apposito decreto la previsione di tutti i

casi in cui il trattamento di dati giudiziari, ai sensi del predetto art. 10 Regolamento (UE) 2016/679, possa ritenersi legittimato, fatta eccezione per le ipotesi nelle quali lo stesso non sia già ammesso da norme di legge o norme regolamentari e non avvenga sotto il controllo dell'autorità pubblica.
Per quanto qui interessa, ed in particolare con riferimento all'attività dell'ASST della Valcamonica, l'art. 2- octies del Codice della Privacy, consente il trattamento dei dati giudiziari dell'interessato nell'ambito delle garanzie individuate dal predetto decreto ministeriale, per i trattamenti riguardanti in particolare:
a) l'adempimento di obblighi e l'esercizio di diritti da parte del titolare o dell'interessato in materia di diritto del lavoro o comunque nell'ambito dei rapporti di lavoro;
b) l'adempimento degli obblighi previsti da disposizioni di legge o di regolamento in materia di mediazione finalizzata alla conciliazione delle controversie civili e commerciali;
c) la verifica o l'accertamento dei requisiti di onorabilità, requisiti soggettivi e presupposti interdittivi nei casi previsti dalle leggi o dai regolamenti;
d) l'accertamento di responsabilità in relazione a sinistri o eventi attinenti alla vita umana, nonché la prevenzione, l'accertamento e il contrasto di frodi o situazioni di concreto rischio per il corretto esercizio dell'attività assicurativa, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;
e) l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
f) l'esercizio del diritto di accesso ai dati e ai documenti amministrativi, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;
g) l'esecuzione di investigazioni o le ricerche o la raccolta di informazioni per conto di terzi;
h) l'adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di pericolosità sociale, nei casi previsti da leggi o da regolamenti, o per la produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto;
i) l'accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, in adempimento di quanto previsto dalle vigenti normative in materia di appalti;
j) l'attuazione della disciplina in materia di attribuzione del rating di legalità delle imprese;
k) l'adempimento degli obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.
Nelle more dell'emissione del Decreto del Ministero della Giustizia, il trattamento dei dati giudiziari è lecito qualora avvenga secondo le prescrizioni indicate dall'Autorità Garante nel documento "*Autorizzazione generale n. 7- 2016 - Autorizzazione al trattamento dei dati giudiziari da parte di privati, di enti pubblici economici e di soggetti pubblici - 15 dicembre 2016*".

PARTE TERZA - DIRITTI DELL'INTERESSATO

ARTICOLO 13) INFORMATIVA SUL TRATTAMENTO DEI DATI (TRASPARENZA)

Come stabilito dall'articolo 13 del Regolamento Europeo n. 2016/679, in caso di raccolta presso l'interessato di dati che lo riguardano, il Titolare del trattamento deve fornire allo stesso, nel momento in cui i dati personali sono ottenuti, un'informativa che illustri, con linguaggio semplice e chiaro, modalità e finalità del trattamento.
L'informativa rappresenta lo strumento che rende esplicita e trasparente la gestione delle informazioni di carattere personale e particolare degli interessati, al fine di consentire agli stessi soggetti di prendere parte attiva alla difesa dei propri diritti nell'ambito della protezione dei dati personali.
L'informativa dovrà contenere 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 o DPO);
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
e) 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.

ARTICOLO 13.A) L'INFORMATIVA PRIVACY NELL'ASST DELLA VALCAMONICA
L'ASST della Valcamonica, quale Titolare del trattamento, adempie all'obbligo di rendere l'informativa attraverso le seguenti modalità:
- consegnandola direttamente all'interessato;
- rendendola disponibile presso le sale accettazioni, sale d'attesa, e ingresso reparti;
- messaggi preregistrati (CUP);
- pubblicazione sul sito aziendale.

Le informative presenti in Azienda sono di due tipi: 1) Informative sintetiche; 2) Informative estese.

L'informativa sintetica (che rimanda a quella estesa), indicando il luogo dove trovarla, contiene almeno le seguenti informazioni:
a) L'identità del Titolare e i dati di contatto del Responsabile della protezione dei dati.
b) La finalità del trattamento per cui i dati vengono acquisiti.
c) Le misure di sicurezza, tecniche ed organizzative, che vengono utilizzate.
d) Le categorie dei destinatari cui i dati possono essere comunicati.
e) I diritti dell'interessato.

Tale informativa sintetica viene resa:
- In fase di prenotazione telefonica, (con voce preregistrata).
- Nelle aree video sorvegliate.

L'informativa estesa, invece, contiene tutte le informazioni richieste dall'art. 13 RGPD, sopra elencate.

L'informativa viene resa per l'insieme dei trattamenti che possono essere effettuati sui dati dall'ASST della Valcamonica e per le pluralità di prestazioni erogate da distinti Reparti ed Unità Operative di quest'Azienda.
Ciò comporta che l'informativa data all'inizio del trattamento (ad esempio all'atto dell'accettazione in fase di prericovero/ricovero o visita ambulatoriale), legittima l'insieme delle prestazioni e dei trattamenti correlati.
Le informative sono state elaborate nel modo più esaustivo possibile, in maniera trasparente, intellegibile e con linguaggio chiaro e semplice, tuttavia è dovere di ciascuno, per quanto a propria conoscenza, rispondere con delucidazioni orali ad eventuali richieste di chiarimenti da parte degli interessati. In caso di dubbi è necessario inoltrare le richieste al Responsabile della protezione dei dati (RPD).
Qualora l'Azienda intenda utilizzare i dati raccolti per una finalità diversa da quella per cui sono stati ottenuti, prima di tale ulteriore trattamento, deve fornire all'interessato informazioni in merito a tale diversa finalità.
Inoltre, qualora i dati non siano acquisiti dal diretto interessato ma da terzi (art. 14 RGPD), l'informativa deve anche indicare la fonte da cui sono stati acquisiti i dati personali e l'eventualità che i dati provengano da fonti accessibili al pubblico. In tal caso, il Titolare, fornisce l'informativa entro un termine

ragionevole dall'ottenimento dei dati, ma al più tardi entro un mese.

Dopo il raggiungimento della maggiore età le informazioni sono fornite all'interessato nel caso in cui non siano state fornite in precedenza.

L'Azienda ha redatto varie informative in relazione alle diverse finalità di trattamento:
l'elenco completo delle informative è reperibile alla directory \\storage.aslvc\fileserver\UUOOCertificate\Privacy\moduli\moduli_definitivi_in _uso

ARTICOLO 14) CONSERVAZIONE DEI DATI

Per quanto concerne il periodo di conservazione dei dati personali raccolti dall'ASST della Valcamonica, 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, l'ASST della Valcamonica fa rinvio, ove applicabile per analogia, ai termini di conservazione stabiliti nel Titolario e Massimario del Sistema Sociosanitario Lombardo, come meglio specificati nel Registro dei Trattamenti del Titolare, adottato dall'ASST della Valcamonica ai sensi dell'art. 30 del Regolamento Europeo n. 2016/679. Per quanto riguarda i dati personali inseriti nei sistemi informativi si rimanda ai principi di cui all'art. 5 Regolamento (UE) 2016/679, che prescrive la conservazione per un arco di tempo non superiore al conseguimento delle finalità, con specifico riguardo al principio di limitazione della conservazione di cui all'art. 5, lett. e) del Regolamento (UE) 2016/679.

ARTICOLO 15) DIRITTI DELL'INTERESSATO

Ogni interessato (paziente, dipendente, fornitore, ecc.) ha diritto di chiedere al Titolare del trattamento informazioni sui dati che lo riguardano e trattati dal Titolare.
Il Titolare del trattamento deve adottare tutte le misure appropriate per fornire all'interessato in maniera agevole riscontro alle richieste degli interessati.
Ai sensi degli artt. da 15 a 22 RGPD gli interessati possono esercitare i seguenti diritti:

- **Diritto di accesso**: per conoscere le finalità del trattamento, le categorie dei dati personali in questione, i destinatari o le categorie di destinatari a cui i dati personali sono o saranno comunicati, in particolare se in Paesi terzi o organizzazioni internazionali, quando è possibile, il periodo di conservazione dei dati personali previsto, oppure, i criteri utilizzati per determinare tale periodo; qualora i dati non siano raccolti presso l'interessato il diritto di avere tutte le informazioni disponibili sulla loro origine.
- **Diritto di rettifica**: l'interessato chiede la correzione dei dati inesatti, oppure, l'integrazione dei dati che sono incompleti, fornendo in tal caso una dichiarazione integrativa.
- **Diritto di cancellazione/diritto all'oblio**: l'interessato può richiedere la cancellazione dei dati che lo riguardano nel caso in cui sussistano uno dei seguenti motivi: i dati non sono più necessari rispetto alla finalità originaria, ha revocato il consenso su cui si basa il trattamento (art. 6, par. 1, lett. a) e art. 9, par. 2, lett. a) RGPD) e non sussiste altro fondamento giuridico per il trattamento, si oppone al trattamento (art. 21, par. 1, RGPD) e non sussiste motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento (art. 21, par. 2, RGPD), i dati personali sono stati trattati illecitamente, i dati personali devono essere cancellati per adempiere ad un obbligo legale.
- **Diritto alla limitazione al trattamento**: l'interessato contesta l'esattezza dei dati, per il periodo necessario alle verifiche, il trattamento è illecito, ma invece della cancellazione l'interessato chiede la limitazione, i dati sono necessari all'interessato per accertamento, esercizio o difesa di un diritto in sede giudiziaria, anche se il Titolare non ne abbia più bisogno, l'interessato si è opposto al trattamento (ai sensi dell'art. 21, par. 1, RGPD) in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.
- **Diritto di opposizione**: l'interessato ha il diritto di opporsi al trattamento dei suoi dati per motivi connessi alla sua situazione particolare, in tal caso quando il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento, oppure il trattamento è necessario per il perseguimento di interessi legittimi del Titolare o di terzi compresa la profilazione. Il Titolare sottoporrà a valutazione la richiesta dell'interessato per verificare entro che limiti possa essere soddisfatta.
- **Diritto alla portabilità dei dati**: l'interessato ha il diritto di ricevere i dati personali che lo riguardano, in

un formato compatibile al comune uso e leggibile dai dispositivi comunemente in commercio e ha il diritto di trasmettere i suddetti dati ad altro Titolare del trattamento direttamente da parte del Titolare a cui è ricolta la richiesta.

– **Diritto di proporre reclamo ad un'autorità di controllo** quale il Garante per la protezione dei dati personali per lamentare una violazione della disciplina in materia e per richiedere una verifica dell'Autorità.

La completa illustrazione dei diritti dell'interessato e le modalità di esercizio degli stessi è disciplinata dalla specifica disposizione attuativa denominata "Istruzioni relative all'esercizio dei diritti in materia di protezione dei dati personali dell'interessato ai sensi degli artt. 12 - 22 del Regolamento (UE) 2016/679".

PARTE QUARTA – I SOGGETTI DEL TRATTAMENTO

ARTICOLO 16) 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 Regolamento Europeo e del Codice della Privacy, è l'Azienda Socio Sanitaria Territoriale della Valcamonica, nella persona del suo Direttore Generale pro tempore, in qualità di legale rappresentante dell'Azienda stessa, con sede in Breno, via Nissolina, 2.

Il Titolare, avvalendosi della supervisione e collaborazione del Responsabile della protezione dei dati (RPD) (c.d. DPO ***Data Protection Officer***) aziendale, oltre agli altri compiti previsti dal RGPD, provvede a:
a) nominare con contratto o altro atto giuridico i Responsabili esterni 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. 12 del Regolamento (UE), all'adozione delle misure di sicurezza per la conservazione, alla protezione e sicurezza dei dati;
b) nominare il Responsabile della protezione dei dati, come stabilito dall'articolo 37 del Regolamento (UE);
c) designare, attraverso i Responsabili privacy di area all'uopo nominati, gli incaricati autorizzati al trattamento dei dati, impartendo ad essi adeguate istruzioni in relazione all'espletamento delle proprie mansioni nei casi in cui, trattando dati sotto l'autorità del Titolare medesimo, utilizzino o vengano a conoscenza di dati relativi agli interessati, al fine di garantire il rispetto delle vigenti disposizioni in materia di trattamento, ivi compresa l'applicazione del Regolamento (UE) in materia di sicurezza dei dati, seguendo scrupolosamente le istruzioni contenute nei regolamenti aziendali;
d) disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;
e) ettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento dei dati sia effettuato conformemente al RGPD ed al presente Regolamento;
f) nel caso di violazione dei dati pone in essere misure effettive e tempestive e procede alla notifica al Garante per la protezione dei dati personali e alla comunicazione all'interessato;
g) fornire istruzioni ed a formare adeguatamente il personale autorizzato al trattamento dei dati.

Si ricorda, inoltre, 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 medesimo (si vedano artt. 23- 25, in particolare, e l'intero Capo IV del RGPD).
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 RGPD.

ARTICOLO 17) 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.

ARTICOLO 18) RESPONSABILI PRIVACY DI AREA (INTERNI)

Anche se il Regolamento Europeo (art. 28) disciplina i compiti del Responsabile "esterno" senza contemplare espressamente la figura ed i compiti del Responsabile "interno", ai sensi dell'art. 24 del medesimo RGPD, il Titolare del trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, mette in atto misure organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento medesimo (c.d. principio di "***accountability***").

Pertanto, l'ASST della Valcamonica, considerate la complessità e la molteplicità delle proprie funzioni istituzionali e la necessità di far divenire la protezione dei dati una parte integrante delle pratiche e dei valori condivisi dell'Azienda stessa garantendo, a tutti i livelli, la più efficace applicabilità dei precetti in materia di tutela dei dati personali, nonché per scongiurare conseguenze pregiudizievoli per i diritti e le libertà delle persone fisiche, ha reputato necessario individuare in ambito aziendale la figura dei Responsabili interni del trattamento dei dati personali, conferendo l'incarico a soggetti che presentino garanzie sufficienti a far sì che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'interessato.

In base all'organizzazione dell'ASST della Valcamonica, il Direttore Generale, con decreto, identifica nella propria organizzazione alcuni ruoli chiave all'interno di ciascun dipartimento aziendale, con il compito di istruire e sorvegliare i propri collaboratori nella gestione del trattamento dati.

Per coadiuvare il Titolare nella gestione delle politiche aziendali in materia di protezione dei dati personali, sono stati quindi individuati e designati i **Responsabili interni privacy di area**, identificati nei seguenti ruoli:

– Direttore Sanitario per tutti i Servizi/Uffici in staff alla Direzione Sanitaria in cui non sia stato nominato un Responsabile.
– Direttore Amministrativo per tutti i Servizi/Uffici in staff alla Direzione Amministrativa in cui non sia stato nominato un Responsabile.
– Direttore Socio Sanitario per tutti i Servizi/Uffici in staff alla Direzione Socio Sanitaria in cui non sia stato nominato un Responsabile.
– Direttori/Responsabili delle Unità Operative Ospedaliere, per quanto riguarda le Unità Operative/Servizi Sanitari (Strutture complesse e semplici).
– Direttori/Responsabili Amministrativi per quanto riguarda le Unità Operative/Uffici amministrativi (Strutture complesse e semplici).
– Responsabile Sicurezza IT: il responsabile del sistema informativo dell'Azienda.

Le nomine dei Responsabili privacy di area dell'Azienda, a firma del Direttore Generale, sono poste in essere per iscritto al momento dell'instaurarsi di un rapporto di lavoro dipendente e/o di collaborazione con l'Azienda.

L'atto di nomina viene conservato nel fascicolo del personale, ad opera dell'Ufficio Risorse Umane. Copia dell'incarico viene trasmesso all'ufficio URP, che provvede l'aggiornamento dell'elenco dei Responsabili privacy di area.

Il Titolare del trattamento dei dati all'atto del conferimento dell'incarico, deve informare ciascun

Responsabile interno del trattamento dei dati, così come individuato dal presente Regolamento, delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative vigenti.

I Responsabili interni del trattamento rispondono al Titolare di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente, pur rimanendo il Titolare unico responsabile verso gli interessati, gli altri Titolari o i Responsabili esterni.
Il Responsabile interno del trattamento deve:
a) Garantire che il trattamento dei dati personali e particolari avvenga secondo le istruzioni impartite dal Titolare del trattamento nel pieno rispetto delle vigenti disposizioni in materia e del presente Regolamento.
b) Garantire che ogni dato, venga trattato per le sole finalità per le quali è stato raccolto, nonchè la correttezza, l'esattezza e la completezza di dati personali oggetto di trattamento.
c) Garantire che in fase di progettazione di nuovi trattamenti, ove necessaria, venga richiesta una valutazione di impatto e di rischio, conforme alle direttive stabilite nel presente Regolamento informandone il Titolare del trattamento e il Responsabile della protezione dei dati (RPD).
d) Garantire che nel caso in cui si verifichi una violazione di dati personali, oltre agli specifici adempimenti previsti dalle relative Disposizioni Attuative ed istruzioni operative, informi tempestivamente il RPD, che a sua volta provvederà ad informare il Titolare.
e) Per conto del titolare, individuare e nominare i propri collaboratori "Incaricati del trattamento" con atto di designazione scritto (secondo l'apposito modello), archiviare e provvedere al costante aggiornamento delle stesse sulla base della dotazione organica: l'incarico deve essere aggiornato in occasione del mutamento delle mansioni o del profilo funzionale dell'incaricato anche in seguito di trasferimento all'interno dell'Azienda.
f) Aggiornare in caso di modifiche di procedure, ruoli e funzioni, gli ambiti di trattamento consentiti e comunicarli agli incaricati.
g) Garantire che il personale incaricato del trattamento operi in conformità alle disposizioni di legge e regolamenti loro impartiti.
h) Garantire che i documenti contenenti dati personali e particolari vengano custoditi in modo da non essere accessibili a persone non incaricate del trattamento.
i) Garantire che i dati personali e particolari vengano comunicati nel rispetto delle prescrizioni impartite. I documenti contenenti dati personali e particolari non devono essere condivisi, comunicati o inviati a persone non autorizzate.
j) Garantire che l'informativa di cui all'art. 13 RGPD venga effettivamente resa.
k) Garantire che gli incaricati, deputati alla raccolta del consenso (nei casi previsti dalla legge) lo acquisiscano secondo le indicazioni impartite.
l) Garantire che i dati personali e particolari raccolti su supporti cartacei ed informatici vengano trattati nel rispetto delle misure minime di sicurezza di cui all'art. 32 RGPD.
m) Osservare e verificare che, presso la propria struttura, le persone incaricate (autorizzate) al trattamento dei dati personali assolvano ad un adeguato livello di riservatezza.
n) Proporre l'adozione di idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi presso la propria struttura, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente.
o) Tenendo conto della natura del trattamento, assistere il Titolare del trattamento con misure tecniche ed organizzative adeguate, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato secondo quanto previsto nella normativa vigente.
p) Contribuire alle attività di verifica del rispetto del Regolamento, comprese le ispezioni, realizzate dal Titolare del trattamento o da altro soggetto da questi incaricato.

Il Responsabile interno privacy di area, nell'espletamento della sua funzione, deve inoltre collaborare con il Responsabile della protezione dei dati (RPD), al fine di:
a) comunicare al RPD, quando questi ne faccia richiesta, ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 del Regolamento (UE) 2016/679 riguardanti: l'adozione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio; la notificazione di una violazione dei dati personali al Garante privacy; la comunicazione di una violazione dei dati personali all'interessato, la predisposizione del Registro dei trattamenti;
b) utilizzare i modelli aziendali di Informativa e Consenso (quest'ultimo ove richiesto), verificandone il

rispetto e fornendo al RPD, quando questi ne faccia richiesta, le informazioni utili per l'aggiornamento del registro dei trattamenti;
c) attenersi alle specifiche Disposizioni Attuative per quanto concerne le istanze degli interessati, volte a facilitare l'esercizio del diritto di accesso dell'interessato e la valutazione del bilanciamento degli interessi in gioco;
d) contribuire a far sì che tutte le misure di sicurezza riguardanti i dati dell'Azienda siano applicate all'interno dell'Azienda stessa ed all'esterno, qualora agli stessi vi sia accesso da parte di soggetti terzi;
e) informare il Titolare del trattamento, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali.

Tutte le misure sopra elencate sono riesaminate e riaggiornate, qualora necessario, in base ad eventuali revisioni dell'organizzazione aziendale e puntualmente riportate nell'atto di nomina.

ARTICOLO 19) RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI
Nell'ambito dell'ASST della Valcamonica, 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'Azienda, trattino dati di cui la stessa sia titolare e qualora siano in possesso dei requisiti previsti dall'articolo 28 del Regolamento Europeo (esperienza, capacità ed affidabilità).
In ottemperanza al nuovo **articolo 28 del Regolamento Europeo 2016/679**, i Responsabili esterni hanno l'obbligo di:
a) trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della vigente normativa (nazionale ed europea) in materia di privacy;
b) trattare i dati personali, anche di natura sensibile e giudiziaria, degli utenti (o di altri interessati) esclusivamente per le finalità previste dal contratto o dalla convenzione stipulata con l'ASST della Valcamonica e ottemperando ai principi generali di necessità, pertinenza e non eccedenza;
c) rispettare i principi in materia di sicurezza dettati dalla normativa vigente (nazionale ed europea) in materia di privacy, idonei a prevenire e/o evitare operazioni di comunicazione o diffusione dei dati non consentite, il rischio di distruzione o perdita, anche accidentale, il rischio di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;
d) adottare, secondo la propria organizzazione interna, misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio, nei termini di cui all'articolo 32 del Regolamento Europeo 2016/679 rubricato "Sicurezza del trattamento";
e) nominare, al loro interno, i soggetti autorizzati/incaricati del trattamento, impartendo loro tutte le necessarie istruzioni finalizzate a garantire, da parte degli stessi, un adeguato obbligo legale di riservatezza;
f) attenersi alle disposizioni impartite dal Titolare del trattamento, anche nell'eventuale caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, nei termini di cui all'articolo 28, comma 3, lettera a) del Regolamento Europeo;
g) specificare, su richiesta del Titolare, i luoghi dove fisicamente avviene il trattamento dei dati e su quali supporti e le misure minime di sicurezza adottate per garantire la riservatezza e la protezione dei dati personali trattati.
h) assistere, per quanto di competenza e nella misura in cui ciò sia possibile, il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento Europeo (*sicurezza del trattamento dei dati personali, notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione di impatto sulla protezione dei dati*), tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
i) su scelta del Titolare del trattamento, cancellare o restituire al medesimo tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o dello Stato membro preveda la conservazione dei dati;
j) mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'articolo 28 del RGPD e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato.

Nel caso di mancato rispetto delle predette disposizioni e in caso di mancata nomina dei soggetti

incaricati al trattamento dei dati ne risponde direttamente, verso l'Azienda, il Responsabile esterno del trattamento.

La designazione del Responsabile esterno viene effettuata mediante “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.
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 20) RESPONSABILE DELLA SICUREZZA INFORMATICA

Nell’ambito dell’implementazione delle misure organizzative volte a garantire l’applicazione del RGPD a mente del citato art. 24 RGPD, tra i Responsabili del trattamento nominati dal Titolare, particolare importanza riveste il Responsabile della sicurezza informatica.
Il Responsabile della sicurezza informatica è di prassi individuato nel Responsabile UOS Servizi Sistemi Informativi pro tempore, in virtù dell’esperienza, capacità ed affidabilità che garantiscono il rispetto delle vigenti disposizioni in materia di trattamento, ivi compresa l’applicazione del regolamento in materia di sicurezza dei dati.
Il Responsabile della sicurezza informatica, oltre ai compiti sopra indicati rivolti a tutti i responsabili interni, ha la responsabilità complessiva di tutto il sistema informativo aziendale, incluso coordinamento, sviluppo, mantenimento, e monitoraggio del programma di sicurezza delle informazioni aziendali, nonché il compito di garantire che le informazioni aziendali siano opportunamente protette, considerando sia gli aspetti di natura logica, sia organizzativa e normativa. In particolare si evidenziano i seguenti compiti:

a) di concerto con il Titolare e con l’Amministratore di Sistema, elabora e mantiene aggiornato il Piano Aziendale per la Sicurezza Informatica, definendo azioni e tempistiche che dovranno essere attuate congiuntamente ai singoli dipartimenti (ad es: programma audit interno, corsi di formazione, ecc.);

b) cura l’esecuzione e l’aggiornamento dell'analisi dei rischi di sicurezza, identificando le principali criticità a livello organizzativo, di processo e tecnologico;

c) provvede alla ricognizione delle banche dati informatiche presenti in Azienda con indicazione delle rispettive sedi e caratteristiche;

d) definisce le norme comportamentali, le soluzioni procedurali e i sistemi architetturali per garantire la riservatezza, l'integrità e la disponibilità delle informazioni (es. configurazione sicura dei sistemi, definizioni di norme per la gestione degli asset, gestione degli incidenti, ecc.);

e) supporta la progettazione e realizzazione dei progetti di sviluppo aziendali congiuntamente ai singoli dipartimenti, indirizzando tutti gli aspetti afferenti la sicurezza infotelematica. Provvede a monitorare il corretto funzionamento delle misure di protezione adottate;

f) fornisce al Responsabile della protezione dei dati (RPD) la necessaria assistenza informatica ed il supporto per tutti gli aspetti correlati alla sicurezza dei trattamenti effettuati con strumenti elettronici.

ARTICOLO 21) AMMINISTRATORE DI SISTEMA

In relazione al provvedimento del Garante per la protezione dei dati del 27 novembre 2008, in G.U. n. 300 del 24 dicembre 2008, il Titolare provvede a nominare l’“Amministratore di sistema”.
Gli Amministratori di sistema, sono individuati in ambito informatico, in quanto figure specializzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, quali gli amministratori di data base, gli amministratori di rete e di apparati di sicurezza e gli amministratori di sistemi software complessi.
Gli estremi identificativi delle persone fisiche Amministratori di sistema, con l’elenco delle funzioni ad essi attribuite, vengono riportati in un documento interno all’UOS Servizi Sistemi Informativi da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.
L’identità degli Amministratori di sistema che riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, sono resi noti in Azienda attraverso strumenti di comunicazione interna (es. intranet aziendale, ordini di servizio a circolazione interna o bollettini).

L'ASST della Valcamonica può affidare a un operatore esterno i servizi di Amministrazione di sistema. In tale ipotesi le prescrizioni e gli adempimenti di cui al Provvedimento del Garante per la Privacy del 27 novembre 2008 e ss.mm.ii., sono pertanto posti in capo al soggetto esterno individuato dall'Azienda quale Responsabile esterno del trattamento ai sensi dell'art 28 del Regolamento.
In tal caso l'Amministratore di sistema - Responsabile esterno, in particolare è tenuto a:
a) procedere all'attribuzione delle funzioni di Amministratore di sistema mediante designazione individuale previa valutazione dell'esperienza, capacità e affidabilità del soggetto designato;
b) precisare analiticamente per ciascun soggetto designato l'ambito di operatività consentito in base al profilo autorizzativo assegnato;
c) conservare ed aggiornare periodicamente gli estremi identificativi delle persone fisiche preposte quali Amministratori di sistema;
d) procedere alla verifica, almeno annuale, dell'operato degli Amministratori individuati;
e) adottare sistemi di registrazione degli accessi logici ai sistemi di elaborazione ed agli archivi elettronici da parte degli Amministratori.

Ogni qualvolta l'Azienda intendesse esternalizzare i servizi di Amministrazione di sistema, l'atto di nomina a Responsabile del trattamento dovrà essere integrato con l'esplicitazione delle puntuali prescrizioni di cui al punto precedente.

A titolo esemplificativo e non esaustivo si elencano i compiti propri dell'Amministratore di sistema:
a) classificare analiticamente le banche dati e impostare/organizzare un sistema complessivo di trattamento dei dati personali comuni e sensibili, predisponendo e curando ogni relativa fase applicativa nel rispetto della normativa vigente in materia di protezione dei dati personali;
b) individuare per iscritto il/i soggetto/i incaricato/i della custodia delle parole chiave per l'accesso al sistema informativo e vigilare sulla sua/loro attività;
c) individuare per iscritto gli altri soggetti, diversi dall'/dagli incaricato/i della custodia delle parole chiave, che possono avere accesso a informazioni che concernono le medesime;
d) impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici;
e) impostare e gestire un sistema di autorizzazione per gli incaricati dei trattamenti di dati personali effettuati con strumenti elettronici;
f) adottare un sistema idoneo alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici; le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità, adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Tali registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate ed essere conservate per un congruo periodo, non inferiore a sei mesi;
g) assicurare e gestire sistemi di salvataggio e di ripristino dei dati (backup/recovery) anche automatici, nonché approntare adeguate misure e/o sistemi software di salvaguardia per la protezione dei dati personali (antivirus, firewall, IDS ecc.);
h) impartire a tutti gli incaricati istruzioni organizzative e tecniche che prevedano le modalità di utilizzo dei sistemi di salvataggio dei dati con frequenza almeno settimanale;
i) adottare procedure per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi;
j) organizzare i flussi di rete, la gestione dei supporti di memorizzazione, la manutenzione hardware, nonché la verifica di eventuali tentativi di accessi non autorizzati al sistema provenienti da soggetti terzi, quali accesso abusivo al sistema informatico o telematico, frode, danneggiamento di informazioni, dati e programmi informatici, danneggiamento di sistemi informatici e telematici;
k) predisporre un piano di controlli periodici, da eseguire con cadenza almeno semestrale, atti a verificare l'efficacia delle misure di sicurezza adottate in azienda/studio professionale;
l) coadiuvare, se richiesto, il Titolare del trattamento nella predisposizione e/o nell'aggiornamento e/o nell'integrazione di tutti i documenti necessari per il rispetto del Regolamento Europeo in materia di privacy.

ARTICOLO 22) INCARICATO (AUTORIZZATO) DEL TRATTAMENTO DEI DATI

Il Regolamento Europeo non fornisce rilievo autonomo alla figura dell'incaricato al trattamento dei dati, seppure si soffermi sul fatto che chi tratta dati, ricevendo istruzioni e formazione da parte del Titolare del trattamento debba da questi essere "*autorizzato*" al trattamento (articoli 4 e 29 del RGPD): cosicché si rinvengono nell'**autorizzato** al trattamento significative sovrapposizioni con il soggetto cui sono attribuiti funzioni e compiti connessi al trattamento dei dati personali previsto dall'art. 2- quatordecies del D.lgs. n. 196/2003.

Come già stabilito all'articolo 7 del presente Regolamento, al momento dell'ingresso in servizio, ad ogni dipendente dell'Azienda, a tempo indeterminato o determinato, pieno o parziale, agli operatori in formazione o in aggiornamento, agli operatori di supporto preposto ad un determinato servizio che implichi il trattamento di dati personali (oltre che ad ogni collaboratore, consulente, tirocinante, volontario, ecc.) è fornita, a cura di ciascun Responsabile interno privacy di area una specifica comunicazione, con la quale detti soggetti (dipendenti e non dipendenti) sono nominati quali "**incaricati al trattamento dei dati**" ai sensi del D.lgs. 196/2003 e ss.mm.ii. e del Regolamento (UE) 2016/679, fatte salve debite eccezioni in relazione alla natura dell'incarico.
Le nomine, comprensive di istruzioni, individuano altresì l'ambito del trattamento consentito.
La nomina dell'incaricato viene posta in essere al momento della presa in carico del personale all'interno delle proprie strutture e vengono aggiornate in base alla dotazione organica.
Le lettere di nomina degli incaricati firmate per conto del Titolare dal Responsabile interno privacy di area, con le relative istruzioni operative e l'ambito di trattamento, vengono archiviate all'interno della struttura aziendale di appartenenza.
Agli stessi viene consegnata, anche a mezzo di post elettronica, o attraverso la rete intranet aziendale, una copia del presente Regolamento e delle relative Disposizioni Attuative adottate.

ARTICOLO 23) AMBITO DI TRATTAMENTO

È stato definito, per tutto il personale sanitario e non sanitario operante presso i reparti di degenza (ambulatori, servizi sanitari) l'ambito di trattamento consentito sia su supporto cartaceo che informatizzato per i Responsabili privacy di area e gli autorizzati al trattamento. Nel modulo M AGR 040 l'Azienda ha individuato le figure che possono o no trattare i dati personali/e o particolari e sono definiti i trattamenti possibili sui dati.
Analogamente, per le UO amministrative è stato definito l'ambito di trattamento, e sono state individuate le figure che possono trattare i dati e le operazioni consentite.
La tabella deve essere portata a conoscenza, da parte del Responsabile privacy di area a tutto il personale incaricato.

ARTICOLO 24) RESPONSABILE AZIENDALE DELLA PROTEZIONE DEI DATI

Il Regolamento Europeo impone la nomina del Responsabile della protezione dei dati (in italiano: Responsabile della protezione dei dati o "RDP") o ***Data Protection Officer*** (DPO) nei termini di cui agli articoli 37, 38 e 39 del Regolamento medesimo.

La nomina del RDP è obbligatoria in tutte le organizzazioni, anche pubbliche, che trattano come **attività principali dati "particolari" su larga scala.**

Chi svolge la funzione di RPD, quindi, deve presentare caratteristiche di indipendenza ed autorevolezza. 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.
Il RPD svolge il proprio compito in piena autonomia e con un supporto adeguato in termini di risorse finanziarie, infrastrutture, e personale per svolgere in modo efficace i compiti cui è chiamato.
Valutate le dimensioni aziendali nonché la complessità dell'organismo sanitario, il RPD è supportato da un gruppo di lavoro, individuato nelle seguenti aree aziendali: UOC Controllo, Sistemi e Supporto Strategico, UOS Servizi Sistemi Informatici, Anticorruzione, Servizio Ingegneria Clinica, Direzione Medica di Presidio, Ufficio Qualità, URP.

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

- **sorvegliare l'osservanza del RGPD** e di altre disposizioni dell'Unione Europa o degli Stati membri relativi alla protezione dei dati nonché delle politiche decise dal Titolare del trattamento in materia di protezione dei dati personali, compresi: l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo, 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 derivanti dal RGPD, dal presente Regolamento nonché da ulteriori 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), la designazione del RPD deve avvenire sulla base delle competenze professionali e personali. In particolare 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;
- delle norme e procedure amministrative applicabili all'Azienda;
- delle tecnologie informatiche e misure di sicurezza dei dati;
- dello specifico settore di attività: sanitario;
- dell'organizzazione e dei processi aziendali.

Egli, inoltre, deve:
- 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;
- possedere capacità organizzative, relazionali e di conseguenza capacità di promuovere una cultura della protezione dei dati all'interno dell'Azienda.

Il Regolamento (UE) prevede 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.

Sia che il RDP sia interno che esterno, è necessario conferire allo stesso **incarico/contratto ad hoc**. Nel caso il cui il RDP sia un "esterno" (persona o società) tutte le clausole, oltre che il compenso per l'incarico, dovranno essere inserite in un apposito contratto, ove siano anche previste le risorse necessarie a far funzionare l'ufficio del RDP.

PARTE QUINTA - SICUREZZA DEI DATI PERSONALI MISURE DI CARATTERE ORGANIZZATIVO, INFORMATICO E TECNOLOGICO

ARTICOLO 25) PROTEZIONE DEI DATI FIN DALLA 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 medesimo 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.
I principali requisiti relativi alla **privacy by design** sono:
– **Approccio a misure proattive**: anticipare, identificare e prevenire gli incidenti potenzialmente invasivi prima che si verifichino.
– Stabilire e applicare **elevati standard di sicurezza privacy** in funzione dei dati da trattare e dei rischi impliciti.
– Generare un impegno responsabile alla privacy condiviso tra l'Azienda e gli interessati, in una cultura di **miglioramento continuo**.

Privacy by default: La protezione by default richiede che l'Azienda **garantisca che vengano trattati solo i dati personali necessari per raggiungere uno scopo specifico, chiaro e limitato**, secondo i principi di:
– Limitazione della finalità: i dati devono essere raccolti e registrati per finalità esplicite e legittime, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi.
– **Minimizzazione dei dati**: i dati personali oggetto di trattamento devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.
– **Esattezza**: i dati devono essere 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.
– **Limitazione della conservazione**: i dati personali oggetto di trattamento devono essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore al conseguimento delle finalità per i quali essi sono stati raccolti o successivamente trattati.
– **Integrità e riservatezza**: deve essere garantita 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.
– **Liceità, correttezza e trasparenza** nei confronti dell'interessato.

ARTICOLO 26) 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 (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 Socio Sanitaria Territoriale, non può che avere forma elettronica, verrà conservato dal Titolare e dal RPD 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 organizzato di corretta gestione dei dati personali.

L'art. 30 RGPD prevede che il registro elenchi le seguenti informazioni:
a. Il nome e i dati di contatto del Titolare del trattamento e, se nominati, del contitolare del trattamento, del rappresentante del Titolare del trattamento e del Responsabile della protezione dei dati (RPD).
b. Le finalità del trattamento, distinte per tipologie (es. trattamento dei dati dei dipendenti per la gestione del rapporto di lavoro; trattamento dei dati di contatto dei fornitori per la gestione degli ordini).
c. Una descrizione delle categorie di interessati (es. clienti, fornitori, dipendenti) e delle categorie dei dati personali (es. dati anagrafici, dati sanitari, dati biometrici, dati genetici, dati relativi a condanne penali o reati, ecc.) trattati.
d. I destinatari (anche solo per categoria di appartenenza) a cui i dati personali sono stati o saranno comunicati (compreso gli altri titolari, come gli enti previdenziali cui vanno trasmessi i dati dei dipendenti per adempiere agli obblighi contributivi, ma è opportuno indicare anche i Responsabili e Sub-

responsabili ai quali sono trasmessi i dati, come i soggetti ai quali il Titolare affidi il servizio di elaborazione delle buste paga dei dipendenti).

e. Ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui all'art. 49, par. 2, RGPD, la documentazione delle garanzie adeguate.

f. Dove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati.

g. Dove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art. 32, par. 1, RGPD:

- La pseudonimizzazione e la cifratura dei dati.
- La capacità di assicurare su base permanente la riservatezza, l'integrità la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.
- Una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

L'ASST della Valcamonica ha anche redatto il Registro dei trattamenti per tutti quei trattamenti che svolge in qualità di Responsabile ex art. 30, par. 2, RGPD (es. nell'ambito di alcune convenzioni).

ARTICOLO 27) 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)).

Per lo stesso motivo, secondo il Regolamento (UE) non potranno più sussistere dal 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza (come contemplava l'abrogato art. 33 del Codice della Privacy), poiché tale valutazione sarà rimessa, caso per caso, al Titolare e al Responsabile in rapporto ai rischi specificamente individuati come da art. 32 del RGPD.

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.

ARTICOLO 28) NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITÀ DI CONTROLLO

A partire dal 25 maggio 2018, tutti i Titolari dovranno **notificare all'Autorità di controllo le violazioni di dati personali** di cui vengano a conoscenza, entro 72 ore e comunque "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*.

Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

a. il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b. il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

c. detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

I contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli art. 33 e 34 del RGPD.

Il Titolare del trattamento, sentito il Responsabile della protezione dei dati (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 la gestione dei "Data Breach", l'ASST ha adottato apposite Disposizioni Attuative a cui si rimanda integralmente denominate "Istruzioni per la gestione della violazione dei dati personali (Data Breach)".

ARTICOLO 29) VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (DPIA- DATA PROTECTION IMPACT ASSESSMENT)

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

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.

La DPIA è lo strumento che, in termini di responsabilizzazione (***accountability***), aiuta il Titolare non soltanto a rispettare le prescrizioni del RGPD, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni. In altri termini, la DPIA permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali.

La DPIA è obbligatoria in tutti i casi in cui un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche: ad esempio se include dati particolati, quali quelli sanitari, ed è effettuato su larga scala, oppure dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, anziani, ecc.). La DPIA deve essere condotta prima di procedere al trattamento.

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.

ARTICOLO 30) TRASFERIMENTO DI DATI PERSONALI ALL'ESTERO

Mentre la circolazione dei dati all'intero dello Spazio Economico Europeo è libera, i trasferimenti al di fuori di tale Spazio sono generalmente vietati, a meno che non intervengano specifiche garanzie. L'art. 44 del RGPD è chiaro nello stabilire che i trasferimenti di dati personali al di fuori dello Spazio Economico Europeo sono ammessi solo in determinate circostanze. In deroga a tale divieto, il trasferimento verso Paesi terzi è consentito anche nei casi menzionati dall'articolo 26, comma 1, della Direttiva 95/46 (consenso della persona interessata, necessità del trasferimento ai fini di misure contrattuali/precontrattuali, interesse pubblico preminente, ecc.), nonché sulla base di strumenti contrattuali che offrano garanzie adeguate (articolo 26, comma 2, della Direttiva 95/46).

Si fa pertanto 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.

ARTICOLO 31) DISCIPLINA AZIENDALE SULL'UTILIZZO DEI MEZZI INFORMATICI E TELEMATICI

Come indicato all'art. 3) del presente Regolamento, l'Azienda disciplina l'utilizzo delle risorse info-telematiche con apposite Disposizioni Attuative a cui si rimanda integralmente.

PARTE SESTA – ENTRATA IN VIGORE ED ATTUAZIONE DEL REGOLAMENTO AZIENDALE

ARTICOLO 32) ENTRATA IN VIGORE E PUBBLICITÀ

Il presente Regolamento entrerà in vigore dalla data di adozione con decreto del Direttore Generale.

Il Regolamento verrà pubblicato sul sito *internet* dell'Azienda, nella Sezione Privacy, sulla rete intranet e/ o inviato alle caselle di posta elettronica di dipendenti e collaboratori

Il testo del presente Regolamento potrà essere aggiornato con decreto del Direttore Generale a seguito di eventuali modifiche che intervengano rispetto alla vigente normativa, nazionale che regionale, e alle indicazioni dell'Autorità di Controllo in materia di protezione dei dati personali.

ARTICOLO 33) DISPOSIZIONE FINALE RELATIVA ALLE DISPOSIZIONI ATTUATIVE

Quanto, invece, alle Disposizioni Attuative, poiché si tratta di "strumenti di lavoro quotidiano", essi saranno inevitabilmente oggetto di continue, quanto rapide integrazioni, modifiche e revisioni, in virtù sia delle necessità aziendali che delle esigenze imposte da una realtà normativa ed organizzativa tuttora in rapidissima evoluzione.

Le Disposizioni Attuative e gli eventuali aggiornamenti verranno distribuite secondo la procedura stabilita al successivo art. 34) e attraverso la rete intranet aziendale e/o inviate alle caselle di posta elettronica di dipendenti e collaboratori.

ARTICOLO 34) RINVIO

Per quanto non previsto dal presente Regolamento aziendale, trovano applicazione le disposizioni del Regolamento (UE) 2016/679, il Codice della Privacy di cui al D.lgs. n. 196/2003 e successive modificazioni e integrazioni, nonché i Provvedimenti del Garante per la Privacy.