Modello Organizzativo

Data Protection

REDAZIONE Data 24/09/2020	Avv. G. Cannella DPO	F.to
PRE-VERIFICA Data 20/11/2020	C. Paganoni UOC Qualità e Risk Management	F.to
VERIFICA Data 20/11/2020	S. Benedetti UOC Legale, Giuridico e Affari Generali A. Rossodivita-Direttore UOC Programmazione Strategica – ad interim UOC Qualità e Risk Management A. Panese- Direttore UOC Sistemi Informativi Aziendali Avv.G. Cannella DPO	F.to F.to F.to F.to
APPROVAZIONE Data 20/11/2020	A. De Vitis Direttore Amministrativo G. Ardemagni Direttore Sanitario P. Formigoni Direttore Sociosanitario	F.to F.to F.to

INDICE

PREMESSA

ASST della Valtellina e dell'Alto Lario (di seguito, anche, "ASST" o "Azienda") ha da sempre prestato particolare attenzione alla gestione dei dati personali trattati per l'esecuzione delle attività aziendali.
L'Azienda, sensibile all'esigenza di assicurare la piena liceità e correttezza nei trattamenti eseguiti - a supporto del processo di identificazione, misurazione, gestione e monitoraggio dei principali rischi che impattano sul corretto svolgimento delle attività aziendali - ha deciso di dare forma, con il presente documento al proprio Modello Organizzativo Data Protection ("MODP"), fondato su procedure e controlli atti a garantire il buon governo del trattamento di dati personali eseguiti.

Il documento si compone di una Parte Generale, in cui sono brevemente esposti i principi che regolano le attività di trattamento di dati personali eseguite dall'Azienda, le misure organizzative e tecniche adottate per garantire un corretto governo dei trattamenti eseguiti, le articolazioni della struttura *privacy* istituita e le rispettive competenze e responsabilità, e di più Parti Speciali costituite da più allegati, continuativamente oggetto di revisione ed aggiornamento, in cui trovano analitica descrizione i trattamenti eseguiti da ciascuna unità/servizio e le procedure applicate.

Il presente MODP è soggetto ad aggiornamento periodico, al fine di perseguire costantemente la piena conformità alla normativa vigente, alle pronunce giurisprudenziali ed ai provvedimenti adottati dalle autorità locali competenti in materia.

PARTE GENERALE

1. RIFERIMENTI NORMATIVI E DOCUMENTALI E AMBITO DI APPLICAZIONE

Il Modello Organizzativo Data Protection di ASST della Valtellina e dell'Alto Lario è stato redatto in attuazione delle seguenti disposizioni:

- Regolamento Europeo in materia di protezione dei dati personali n. 679/2016;
- Linee Guida adottate dal Gruppo WP29 in relazione alla corretta applicazione del Regolamento UE/679/2016;
- Determinazioni e linee guida del Comitato Europeo per la protezione dei dati personali;
- Codice in materia di protezione dei dati personali, il Decreto legislativo 30 giugno 2003, n. 196, come modificato dal D.Lgs. 101/2018 (anche, di seguito, Codice *Privacy*);
- Provvedimenti e linee guida emanati dal Garante per la protezione dei dati personali.

Il presente documento trova applicazione nei confronti di tutto il personale dell'Azienda, indipendentemente dalla tipologia del rapporto, e delle Terze Parti che, nell'ambito delle proprie mansioni o delle attività professionali svolte per conto dell'ASST, compiano operazioni di trattamento su dati personali sotto la responsabilità delle stesse.
Le misure di protezione e sicurezza di seguito descritte trovano applicazione su tutti i trattamenti di dati relativi a persone fisiche, indipendentemente dalla nazionalità o dal luogo di residenza.

2. PRINCIPI CHE REGOLANO IL TRATTAMENTO DEI DATI

Nello svolgimento di ogni attività di trattamento dei dati, l'ASST opera in conformità ai principi sanciti dalla normativa nazionale e comunitaria.

- **Liceità, correttezza e trasparenza**

Articolo 5, par. 1, lett. a) Reg. UE/679/2016

❖ Cfr. Considerando 39, 40, 44 Reg. UE/679/2016

"I dati personali sono … trattati in modo lecito, corretto e trasparente nei confronti dell'interessato".

L'Azienda si impegna ad eseguire esclusivamente trattamenti leciti ai sensi della normativa nazionale ed europea. Pertanto, la stessa tratta dati personali esclusivamente previa raccolta del consenso da parte dell'Interessato del trattamento, se necessario, o della diversa base giuridica rilevante ai sensi dell'art. 6 GDPR o dell'art. 9 GDPR, per i cd. dati particolari, e dell'art. 10 GDPR, per i dati giudiziari.
L'Azienda assicura, inoltre, la trasparenza dei trattamenti eseguiti, con particolare riferimento alle finalità e modalità del trattamento, attraverso la diffusione di informative facilmente accessibili, comprensibili e redatte con linguaggio chiaro e semplice.

- **Limitazione della finalità**

Articolo 5, paragrafo 1, lett. b), Reg. UE/679/2016

❖ Cfr. Considerando 28, 39, 50 e articolo 6, par. 1, lett. b) Reg. UE/679/2016

"I dati personali sono … 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, considerato incompatibile con le finalità iniziali".

L'Azienda pre-definisce le finalità di ogni trattamento eseguito e le esplicita fin dal momento della raccolta del dato, all'interno dell'informativa consegnata all'Interessato e nella sezione dedicata del Registro. In ogni caso, il Titolare raccoglie dati personali solo se strettamente necessari al perseguimento di tali finalità.
Inoltre, nel caso di nuova finalità, l'Azienda valuta in modo sostanziale e non meramente formale la compatibilità del fine ulteriore rispetto a quello per cui i dati sono stati raccolti, sulla base di parametri quali i) la ragionevole aspettativa dell'Interessato rispetto ai trattamenti futuri, anche considerando la relazione tra questo ed il Titolare, ii) la sede di raccolta dei dati, iii) le garanzie disponibili al fine di ridurre l'impatto dell'ulteriore trattamento sulla sfera privata dell'Interessato.

- **Minimizzazione dei dati**

Articolo 5, paragrafo 1, lett. c), Reg. UE/679/2016

❖ Cfr. articolo 25, paragrafo 2, Reg. UE/679/2016

"I dati personali sono … adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati".

L'Azienda raccoglie i dati funzionali ed essenziali al perseguimento delle finalità per cui il dato è trattato. Il trattamento non è eseguito in tutti i casi in cui le medesime finalità siano realizzabili mediante dati anonimi o altre modalità che rendano non determinabile l'identità dell'Interessato. Inoltre, l'Azienda ha definito e formalizzato diversi livelli autorizzativi per ogni soggetto coinvolto nel trattamento dei dati. Pertanto, ogni soggetto formalmente Incaricato al trattamento può accedere esclusivamente alle categorie di dati essenziali per lo svolgimento della propria mansione lavorativa.

- **Esattezza dei dati**

Articolo 5, paragrafo 1, lett. d), Reg. UE/679/2016

"I dati personali sono … 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".

L'Azienda effettua specifiche verifiche atte ad accertare l'esattezza dei dati personali trattati, dalla raccolta del dato fino alla sua cancellazione, e riconosce ad ogni Interessato la possibilità di esercitare in modo immediato il proprio diritto di rettifica ed aggiornamento.
L'Azienda adotta tutte le misure ragionevoli affinché i dati personali inesatti siano rettificati; di più, nel caso in cui il loro aggiornamento si configuri come impossibile l'ASST provvede alla tempestiva cancellazione.

- **Limitazione della conservazione**

Articolo 5, paragrafo 1, lett. e), Reg. UE/679/2016

❖ Cfr. Considerando 39 e articolo 89 Reg. UE/679/2016

"I dati personali sono … 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, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato".

L'Azienda ha definito i tempi di conservazione di ogni tipologia di dato personale trattato dandone specificazione all'interno di un'apposita sezione del Registro dei trattamenti adottato ai sensi dell'art. 30 GDPR.
I tempi di conservazione sono stati definiti in base alla finalità per cui il dato è trattato, tenendo conto degli obblighi normativi e regolamentari sussistenti in capo al Titolare del trattamento.

- **Integrità e riservatezza**

Articolo 5, paragrafo 1, lett. f), Reg. UE/679/2016

❖ Cfr. Considerando 39 Reg. UE/679/2016

"I dati personali sono … 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".

L'Azienda ha adottato tutte le misure, tecniche e organizzative, ritenute idonee a salvaguardare la correttezza del processo di raccolta e gestione dei dati, nonché la loro sicurezza e protezione in caso di intrusioni e alterazioni non autorizzate.

- **Principio di *Accountability***

Articolo 24, Reg. UE/679/2016

❖ Cfr. Considerando 74 Reg. UE/679/2016

"Il Titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento al Regolamento, compresa l'efficacia delle misure".

L'Azienda ha implementato un sistema di gestione del rischio *privacy*: individuando i rischi connessi al trattamento; valutando tali rischi in termini di origine, natura, probabilità e gravità; definendo le migliori prassi per attenuare il rischio connesso ad ogni trattamento eseguito.
L'adeguatezza delle misure adottate per ogni trattamento è valutata *ex ante*, secondo una prospettiva preventiva, ed *ex post*, a seguito di eventuali mutamenti del contesto di riferimento.
La predisposizione di tale sistema ed ogni successiva sua modifica o integrazione sono opportunamente tracciate e documentate, al fine di adempiere all'onere probatorio sussistente in capo al Titolare.

- ***Privacy by design e by default***

Articolo 25, Reg. UE/679/2016

❖ Cfr. Considerando 78 Reg. UE/679/2016

"Il Titolare del trattamento, al fine di dimostrare la conformità con il presente regolamento, dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default".

L'Azienda ha implementato un sistema di gestione *privacy* atto a perseguire la piena tutela dei dati trattati fin dal momento precedente all'avvio del trattamento.
A tal fine, l'ASST – al momento di definizione dei mezzi del trattamento – valuta lo stato dell'arte, i costi di attuazione, la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, i possibili rischi ad esso connessi e le correlate gravità e probabilità, nonché ogni altro elemento ritenuto utile, al fine di condurre un'analisi appropriata ed adottare scelte operative che siano idonee a garantire la tutela dei dati trattati.
Tali misure saranno aggiornate ogniqualvolta si renda necessario adottare un nuovo processo organizzativo o un nuovo sistema informatico nonché nel caso di utilizzo di nuove tecnologie.
Ancora, attraverso la loro applicazione ed il loro periodico aggiornamento, l'Azienda garantisce che per impostazione predefinita saranno oggetto di trattamento solo i dati personali necessari in relazione a ciascuna finalità specifica e che la quantità dei dati raccolti e la durata della loro conservazione non eccedano il minimo necessario per le finalità perseguite.

3. L'INTERESSATO E I SUOI DIRITTI

L'ASST, al fine di tutelare pienamente gli Interessati nell'ambito dei trattamenti eseguiti, ha individuato appositi canali – cartacei ed informatici – per la ricezione delle istanze relative all'esercizio dei diritti riconosciuti all'Interessato dal Regolamento UE.
Ad ogni Interessato è riconosciuta la possibilità di esercitare – nei limiti definiti dal Regolamento – i seguenti diritti:

- Diritto di Accesso (art. 15 GDPR): esercitando il proprio diritto di accesso, l'Interessato può i) avere conferma dell'esistenza di propri dati personali presso il Titolare, ii) accedere ai dati da questo trattati.
  A seguito della richiesta, il Titolare è tenuto a fornire gratuitamente una copia dei dati, in forma cartacea o elettronica, potendo addebitare il costo di eventuali ulteriori copie in capo all'Interessato.
  Nelle ipotesi in cui il trattamento comporti una notevole quantità di informazioni, l'Ufficio *privacy* potrà chiedere all'Interessato di specificare le informazioni a cui la richiesta si riferisce.

- Diritto di rettifica (art. 16 GDPR): ogni Interessato ha il diritto di ottenere la correzione di eventuali inesattezze nonché l'integrazione di informazioni non complete.
  L'inesattezza potrà in ogni caso essere inerente esclusivamente a dati di valore oggettivo.
  Di conseguenza, l'Interessato potrà chiedere la rettifica esclusivamente di dati fattuali e non invece di valutazioni soggettive e personali. Se non richiede uno sforzo sproporzionato, il Titolare comunica le richieste ricevute e le rettifiche/integrazioni effettuate ai soggetti cui i dati sono stati eventualmente comunicati.

- Diritto di cancellazione (diritto all'oblio) (art. 17 GDPR): nel caso di espressa richiesta dell'Interessato, il Titolare ha l'obbligo di cancellare i dati dell'Interessato, su qualsiasi supporto archiviati. Inoltre, se tali dati sono stati diffusi (es. pubblicazione su un sito web), il Titolare deve informare della richiesta di cancellazione gli altri Titolari che trattano i dati personali oggetto della richiesta di cancellazione, invitandoli a rimuovere ogni copia degli stessi.
  In ogni caso, si precisa che la richiesta di cancellazione deve essere accolta solo al ricorrere di una delle ipotesi previste dal Regolamento Europeo: a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) l'Interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento; c) l'Interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2; d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.
  In ogni caso, la richiesta sarà respinta in tutte le ipotesi in cui ricorra una delle fattispecie derogatorie previste dagli artt. 2-undecies e 2-duodecies del Codice Privacy.
  In forza dello specifico interesse connesso ai dati oggetto della richiesta, il Titolare del trattamento potrà optare per la loro cancellazione o anonimizzazione.
- Diritto di limitazione del trattamento (art. 18 GDPR): l'Interessato può chiedere al Titolare di limitare il trattamento dei propri dati solo con riferimento ad alcune specifiche finalità e solo al

ricorrere di una delle quattro ipotesi tassativamente elencate all'art. 18 del Regolamento, ovvero in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), nel caso in cui l'interessato chieda la rettifica dei dati (in attesa di tale rettifica da parte del titolare) o si opponga al loro trattamento ai sensi dell'art. 21 del Regolamento (in attesa della valutazione da parte del titolare), nelle ipotesi in cui i dati non siano più necessari al Titolare per il perseguimento delle proprie finalità ma divengano necessari per l'esercizio o la difesa di un diritto dell'interessato in sede giudiziaria.

Le tempistiche di limitazione sono strettamente connesse alla ragione posta a fondamento della richiesta. Infatti, nel caso in cui la limitazione sia richiesta per consentire la verifica della correttezza dei dati, per l'esercizio del diritto di opposizione o per l'esercizio di un diritto giudiziario dell'interessato i dati potranno essere nuovamente resi disponibili in seguito all'accertamento; nel caso di trattamento illegittimo e conseguente richiesta di limitazione dell'Interessato, la limitazione potrà proseguire fino alla cancellazione dei dati o, all'eventuale, richiesta di portabilità dell'Interessato.

La richiesta è in ogni caso negata in tutte le ipotesi derogatorie di cui agli artt. 2-undecies e 2-duodecies del Codice Privacy.

- Diritto alla portabilità dei dati (art. 20 GDPR): il diritto alla portabilità dei dati consente all'Interessato a) di ottenere, su richiesta, la restituzione dei propri dati personali da parte del Titolare del trattamento e b) la loro trasmissione ad un nuovo Titolare.

  La richiesta di portabilità può essere accolta solo al ricorrere di determinati presupposti: 1) sono portabili solo i dati trattati con il consenso dell'Interessato o sulla base di un contratto stipulato con l'interessato e 2) solo i dati che siano stati "forniti" dall'Interessato al Titolare, inoltre 3) il diritto alla portabilità può essere soddisfatto solo se non lesivo di diritti e libertà altrui.

- Diritto di opposizione (art. 21 GDPR): l'Interessato può chiedere l'interruzione, in modo permanente, del trattamento dei suoi dati personali.

  La richiesta di opposizione sarà accolta esclusivamente al ricorrere delle ipotesi previste dall'art. 21 par. 1 Regolamento Europeo.

  Quando accolta, la richiesta di opposizione obbliga il Titolare ad interrompere il trattamento in modo definitivo e permanente.

- Diritto di reclamo (art. 77 GDPR): l'Interessato ha sempre il diritto di proporre reclamo al Garante della privacy qualora ritenga che i diritti di cui gode a norma della disciplina vigente siano stati violati a seguito di un trattamento.

Nelle informative rese agli Interessati al momento della raccolta dei dati, l'ASST comunica la possibilità di esercitare i diritti di cui al Regolamento, ovvero di chiedere: l'accesso ai dati personali; l'indicazione delle modalità, finalità e logiche del trattamento; la richiesta di limitazione, opposizione o portabilità dei dati; la rettifica e la cancellazione, nei limiti e nelle modalità indicate dal Regolamento; nonché, laddove il trattamento dei dati si basi sul consenso, il diritto di revocarlo in qualsiasi momento.

Da ultimo, le informative contengono esplicito riferimento alla possibilità per gli Interessati di proporre reclamo all'autorità di controllo, ovvero il Garante Privacy, ai sensi dell'art. 77 del Regolamento.

La gestione interna delle richieste pervenute e delle modalità e responsabilità di riscontro sono dettagliatamente disciplinate all'interno di specifica Procedura.

4. LE FIGURE DEL SISTEMA PRIVACY

Le figure coinvolte nel sistema di gestione del trattamento di dati personali dell'ASST della Valtellina e dell'Alto Lario sono quelle di seguito elencate:

- Titolare del Trattamento;
- Contitolare del trattamento;
- Comitato Privacy;
- Ufficio Privacy;
- Responsabili interni;
- Incaricati del trattamento;
- Data Protection Officer;
- Responsabile del Trattamento;
- Sub-Responsabile del Trattamento;
- Incaricati esterni del trattamento.

4.1 Il Titolare del Trattamento, il Delegato del Titolare ed il Contitolare

Il ***Titolare del trattamento*** è l'ASST – considerata nel suo complesso quale persona giuridica – che determina le finalità e i mezzi del trattamento dei dati personali ed è dotata di un potere decisionale in ordine alle misure tecniche ed organizzative da adottare con riferimento a tutte le operazioni di trattamento eseguite.
L'Azienda in quanto Titolare del trattamento provvede a:

i) definire le modalità e finalità dei trattamenti eseguiti e le categorie di dati trattati;
ii) adottare tutte le misure tecniche ed organizzative necessarie per garantire la sicurezza dei dati trattati;
iii) verificare ed aggiornare periodicamente le misure tecniche ed organizzative adottate;
iv) scegliere consapevolmente i soggetti coinvolti nel trattamento dei dati ed istruirli adeguatamente;
v) in caso di violazioni, porre in essere contro-misure tempestive ed effettive e effettuare le comunicazioni dovute ai sensi di legge.

L'Azienda ha conferito i poteri e le responsabilità connesse agli adempimenti sopra descritti al Direttore Generale dell'ASST, al quale compete la vigilanza sulla corretta ed effettiva applicazione di procedure, istruzioni e linee guida aziendali in materia *privacy*.
A tali fini, il Direttore Generale deve:

i) individuare all'interno dell'Azienda un *team*, cui affidare la gestione operativa degli adempimenti rilevanti in materia *privacy*, e nominare il DPO;
ii) garantire alle figure sopra indicate adeguate risorse economiche ed operative per lo svolgimento delle proprie mansioni;
iii) rapportarsi periodicamente con l'Ufficio Privacy e con il DPO;
iv) sovraintendere alle decisioni relative ai temi portati alla sua attenzione dall'Ufficio Privacy e dal DPO.

Con riferimento a specifici trattamenti, l'Azienda condivide la decisione in merito alle finalità e ai mezzi del trattamento con altri soggetti che operano quali autonomi Titolari del trattamento, assumendo cosi la posizione di ***Contitolari del trattamento***.

Tutte le situazioni di contitolarità sono formalmente disciplinate attraverso appositi accordi, in cui trovano puntuale esplicazione e definizione i ruoli reciproci e il riparto degli obblighi.
L'Azienda provvede ad informare gli Interessati sul contenuto di tale accordo: la dichiarazione del rapporto di contitolarità e le informazioni essenziali sullo stesso sono fornite con l'informativa resa al momento di avvio del trattamento; informazioni più approfondite sul contenuto dell'accordo sono rese su richiesta dell'Interessato.
In ogni caso, l'Azienda provvede ad informare tempestivamente l'Interessato nel caso di modifiche all'accordo che ne riguardino il contenuto essenziale o che incidano su aspetti della sfera giuridica dell'Interessato stesso.
L'elenco dei Contitolari e gli accordi di contitolarità stipulati sono conservati a cura di ciascun Responsabile interno.

4.2 Il Comitato Privacy

Al fine di definire l'opportuno e necessario coordinamento all'interno dell'Azienda, l'ASST ha istituito il Comitato Privacy.
Il Comitato è composto dai componenti dell'Ufficio Privacy, dai Responsabili Interni dell'Unità/dei Servizi strategici con riferimento alle tematiche *privacy* e dal DPO.
Il Comitato cura l'efficienza comunicativa interna, finalizzata ad una piena sensibilizzazione del personale autorizzato al trattamento di dati personali, esegue una valutazione complessiva dei rischi correlati ai trattamenti eseguiti e fornisce il proprio supporto nella risoluzione delle questioni di maggior impatto, indicando al Titolare le azioni più opportune da adottare al fine di perseguire la piena conformità normativa.

4.3 L'Ufficio Privacy

Al fine di dare piena attuazione alle scelte strategiche adottate dal Comitato Privacy, il Titolare individua tra il personale delle UOC afferenti all'Area Amministrativa le risorse dedicate alla gestione degli aspetti operativi in ambito privacy (cd. Ufficio Privacy).
Tale funzione, alla data di approvazione del presente Modello, è affidata al personale dell'UOC Legale Giuridico e Affari Generali, che vi provvede avvalendosi di un supporto professionale esterno.

4.4 I Responsabili Interni

Il ruolo di Responsabile interno è attribuito ai Responsabili delle strutture complesse e ai Responsabili dei servizi con maggiore rilevanza nel trattamento dei dati.
I Responsabili interni sono dunque i soggetti dell'organizzazione aziendale a cui vengono affidati specifici compiti in materia di protezione dei dati personali, con alcuni margini di determinazione autonoma dell'organizzazione *privacy,* dell'unità di competenza e delle modalità del trattamento eseguite dalla stessa nei limiti stabiliti dal Titolare.
Internamente, ciascun Responsabile è tenuto a:

- nominare per conto del Titolare gli Incaricati al trattamento dei dati personali afferenti all'Unità organizzativa o al Servizio di sua competenza;
- fornire supporto ad ogni Incaricato al trattamento per l'analisi e la risoluzione di dubbi/difficoltà connesse al trattamento dei dati;
- verificare che le istruzioni impartite dal Titolare siano effettivamente conosciute ed applicate;
- verificare che tutte le misure tecniche e organizzative siano scrupolosamente osservate;

- provvedere alla compilazione del Registro dei trattamenti per le parti di sua competenza e al suo aggiornamento periodico con le modalità che saranno, di volta in volta, rese note dal Titolare.

Esternamente, il Responsabile interno è tenuto a:

- verificare quali trattamenti siano affidati a soggetti terzi e monitorarne il procedimento di nomina a responsabile esterno ai sensi dell'art. 28 GDPR;
- ricevere eventuali segnalazioni o reclami da parte degli Interessati e trasmetterli tempestivamente ai soggetti competenti in accordo con le vigenti procedure aziendali.

Il rispetto delle istruzioni impartite dal Titolare nella Lettera di nomina a Responsabile interno costituisce un'obbligazione contrattuale. Tale contratto deve specificare la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento.
La mancata o non corretta esecuzione integra un inadempimento contrattuale che espone il Responsabile interno alle sanzioni previste dal Contratto Collettivo Nazionale di Lavoro applicato.

L'elenco dei nominativi dei soggetti individuati quali Responsabili interni è costantemente aggiornato e conservato a cura della UOC Legale, Giuridico e Affari Generali.

I Responsabili interni sono in alcune specifiche ipotesi coadiuvati nell'espletamento del proprio ruolo da risorse operative afferenti all'Unità di appartenenza, le quali forniscono un supporto pratico nella gestione degli adempimenti *privacy*.

La responsabilità circa l'effettivo e corretto svolgimento dell'incarico permane in ogni caso in capo al Responsabile interno designato.

4.5 L'Incaricato al trattamento

Gli Incaricati al trattamento di dati personali sono coloro che, per lo svolgimento della propria attività lavorativa, hanno accesso a dati personali e che sono stati formalmente autorizzati e puntualmente istruiti dal Titolare con riferimento a tali specifiche attività di trattamento.
In quanto Incaricati al trattamento, i dipendenti del Titolare - nello svolgimento della propria attività lavorativa - devono rispettare il Modello Organizzativo *Data Protection,* nonché ogni altra istruzione impartita dallo stesso.

Nell'ambito dell'ASST della Valtellina e dell'Alto Lario tutti i dipendenti ed i collaboratori che nell'espletamento delle proprie mansioni trattano dati di cui l'Azienda è Titolare, sono autorizzati al trattamento degli stessi tramite apposita nomina ad Incaricato al trattamento, sottoscritta dal Responsabile interno dell'Unità di appartenenza, in cui sono ampiamente descritti il ruolo ed i compiti loro attribuiti nel trattamento nonché la tipologia di dati al cui accesso sono autorizzati.

Ogni Incaricato al trattamento ha l'obbligo di operare con la massima diligenza ed attenzione in tutte le fasi di trattamento, al fine di garantire l'esatta acquisizione dei dati, il loro costante aggiornamento, un'adeguata conservazione ed una tempestiva cancellazione o distruzione degli stessi.
Tra i doveri degli Incaricati vi sono:

- effettuare il trattamento dei dati in modo lecito, trasparente e corretto;
- trattare i dati solo per le finalità strettamente connesse all'esecuzione dell'incarico;
- non comunicare e/o diffondere all'esterno i dati personali in qualunque forma, se non previa autorizzazione del Titolare del trattamento dei dati;

- comunicare al Titolare, tramite il proprio Responsabile interno, qualsiasi circostanza idonea a determinare potenzialmente una violazione dei dati, secondo le modalità definite nelle procedure aziendali.

Il mancato rispetto delle istruzioni impartite dal Titolare nella nomina ad Incaricato, nonché di quanto previsto dalla normativa vigente in materia di *privacy*, costituisce un inadempimento contrattuale e, pertanto, l'Incaricato al trattamento potrà essere sottoposto a sanzione disciplinare, sino ad arrivare, nei casi più gravi, allo scioglimento del Contratto e, dunque, al licenziamento.

Tra gli Incaricati al trattamento, l'ASST ha poi individuato e specificamente nominato coloro che assumono specifiche mansioni, ovvero:

4.5.1 Amministratore di Sistema

L'Amministratore di Sistema è un Incaricato autorizzato alla gestione configurazione verifica e controllo delle abilitazioni su un determinato sistema informatico aziendale con cui sono effettuati trattamenti di dati personali.
L'elenco completo degli Amministratori di sistema è tenuto aggiornato e conservato a cura della UOC Sistemi Informativi Aziendali, a seguito di specifica individuazione da uno o più UOC.

4.6 Data Protection Officer

Il Data Protection Officer, di seguito anche "DPO", è colui a cui è affidato il compito di osservare, valutare e supportare il Titolare nella gestione del sistema *privacy*, affinché i dati personali siano trattati nel rispetto delle disposizioni europee e nazionali.
In particolare, il DPO ha il compito di:

1) informare e fornire consulenza al Titolare nonché ai dipendenti degli obblighi derivanti dal Regolamento;
2) sorvegliare l'osservanza del Regolamento, nonché delle altre disposizioni europee o di diritto interno in materia di protezione dati;
3) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e attività di controllo;
4) fornire pareri e sorvegliare sulla redazione del *Data Protection Impact Assessment* (c.d. DPIA e se del caso sulle relative comunicazioni all'Autorità Garante);
5) fungere da punto di contatto e collaborare con l'Autorità Garante per la protezione dei dati personali;
6) assicurarsi che le violazioni dei dati personali siano documentate, notificate e comunicate (c.d. *Data breach Notification Management*).

Il DPO nell'esercizio delle proprie mansioni effettua *audit* e *test* atti ad accertare l'effettiva applicazione delle istruzioni impartite dal Titolare.
Inoltre, lo stesso fornisce supporto al Titolare e ad ogni Incaricato al trattamento per l'analisi e per la risoluzione operativa di problematiche connesse al trattamento dei dati.

L'ASST si è dotata di un DPO esterno, l'avv. Giuseppe M. Cannella, il quale può essere contattato all'indirizzo e-mail: dpo@asst-val.it.

Ai sensi dell'art. 38 par. 3 GDPR, il DPO riferisce direttamente al Titolare del trattamento in merito all'efficacia e all'osservanza del MODP e di ogni altra procedura in materia *privacy*, all'emersione di eventuali aspetti critici, alla necessità di interventi modificativi.
A tal fine, il DPO predispone:

- ad evento, appositi verbali indicanti le attività eseguite e gli esiti delle stesse;
- con cadenza annuale, una relazione informativa relativa all'attività svolta nel corso del proprio mandato;
- immediatamente, appositi flussi email al verificarsi di violazioni di dati e al rilevarsi di carenze tecniche e/o organizzative.

4.7 Il Responsabile della sicurezza delle informazioni

Il Responsabile della sicurezza delle informazioni (CISO) è una figura che non appartiene all'Organigramma Privacy ma che ricopre un ruolo fondamentale per la sicurezza aziendale soprattutto alla luce della nuova disciplina sul trattamento dei dati personali dettata dal GDPR.

Il CISO ha, infatti, il compito di definire le strategie corrette per proteggere al meglio gli asset aziendali, congiuntamente e di supporto ai Sistemi Informativi Aziendali al fine di mitigare i rischi informatici, limitando in tal modo l'accadere di un data breach.

A tal fine il CISO può svolgere attività di audit e controllo attraverso il supporto dei sistemi informativi aziendali.

4.8 I Responsabili ed i Sub-Responsabili del trattamento ex art. 28 GDPR

I Responsabili del trattamento, consulenti e fornitori, sono coloro che svolgono attività di trattamento per conto del Titolare, su istruzione documentata dello stesso.
L'Azienda qualora si avvalga di soggetti esterni per lo svolgimento di servizi nell'ambito dei quali sia necessario eseguire un trattamento di dati personali nomina il prescelto fornitore quale Responsabile del trattamento.
L'ASST quando intende avvalersi di soggetti terzi per l'esecuzione di attività di trattamento deve dunque avere piena conoscenza delle modalità di trattamento che il Responsabile adotterà in concreto nonché delle misure che applicherà per garantire che nella parte di trattamento a lui affidata sia assicurato un livello di protezione almeno pari a quello garantito dal Titolare.
Al fine di verificare l'idoneità dei Responsabili, l'ASST ha predisposto un questionario di pre-qualifica, che deve essere sottoposto al Responsabile nella fase pre-contrattuale oltre che inserito nei bandi di gara.
L'incarico è sempre affidato tramite contratto o altro atto giuridico vincolante contenente gli elementi elencati all'art. 28 GDPR.
L'elenco dei Responsabili del trattamento nominati è tenuto a cura di ciascun Responsabile interno.

L'ASST prevede, in conformità alla normativa vigente, la possibilità che ciascun Responsabile possa delegare l'esecuzione di determinate attività a soggetti terzi, i Sub-responsabili.
L'Impiego di un Sub-responsabile è sempre subordinato al consenso dell'ASST, il quale può essere espresso volta per volta in occasione delle singole nomine effettuate dal Responsabile esterno oppure attraverso un'autorizzazione generale concessa al momento della stipulazione del contratto con il Responsabile esterno.
Sul Sub-responsabile saranno posti gli stessi obblighi imposti in capo al Responsabile del trattamento attraverso il contratto stipulato con il Titolare. Tuttavia, nel caso in cui il Sub-responsabile ometta di

adempiere ai propri obblighi, l'intera responsabilità nei confronti del Titolare ricadrà in capo al Responsabile esterno.

4.9 Formazione del personale coinvolto nel trattamento dei dati personali

L'Azienda sostiene e promuove al suo interno, ogni strumento di sensibilizzazione che possa consolidare il pieno rispetto del diritto alla riservatezza.
A tal riguardo, uno degli strumenti di sensibilizzazione utilizzati è l'attività formativa erogata a beneficio dei dipendenti e collaboratori dell'ASST, al fine di diffondere una conoscenza capillare dei contenuti del Regolamento Europeo e della normativa nazionale vigente.

Al momento di avvio del rapporto contrattuale, ad ogni dipendente è data una specifica comunicazione contenente le indicazioni necessarie per poter acquisire il MODP dell'ASST ed ognuno di essi si impegna a prendere visione del Documento e ad attenersi alle sue prescrizioni.

Inoltre, quale misura di sicurezza, il Titolare del trattamento ha definito un programma formativo pluriennale rivolto a tutti i soggetti autorizzati al trattamento al fine di renderli edotti su:

- i rischi che incombono sui dati;
- le misure disponibili per prevenire possibili danni;
- le responsabilità che derivano da eventuali danni;
- le misure tecniche e organizzative di protezione adottate dal Titolare del trattamento.

Specificamente, il Titolare del trattamento organizza sessioni di formazione – a distanza e/o in presenza – in materia di protezione dei dati personali nei seguenti momenti:

- al momento dell'ingresso di nuovo personale;
- al cambio mansione;
- a seguito di modifiche organizzative interne o di modifiche normative che abbiano influenza sulla gestione e protezione dei dati personali.

5. FLUSSI INFORMATIVI

L'effettiva applicazione del Modello Organizzativo Data Protection si basa su costanti flussi di comunicazione tra le diverse figure organizzative, descritte nel precedente paragrafo.

Il Comitato Privacy deve fornire al Titolare le seguenti informazioni:

- informazione tempestiva in caso di gravi eventi di Data Breach o di particolari urgenze, ad esempio relative a provvedimenti e/o richieste dell'Autorità di Controllo;
- informazione periodica circa le attività di attuazione e verifica delle istruzioni e procedure privacy e sui flussi di comunicazione ricevuti dal DPO.

L'Ufficio Privacy ha il compito di agevolare la comunicazione interna attraverso diverse modalità, tra cui:

- organizzazione di incontri periodici con i Responsabili interni e con il DPO al fine di condividere i temi rilevanti in ambito di trattamento dati;
- utilizzo dei canali opportuni per comunicare a tutti gli Incaricati le novità in materia di trattamento dati personali;
- utilizzo di caselle email dedicate alla ricezione e invio di comunicazioni: ufficio.privacy@asst-val.it.

Il Responsabile interno deve garantire all'Ufficio Privacy ed al DPO i seguenti flussi di comunicazione:

- la necessità di effettuare trattamenti su dati personali diversi ed eccezionali rispetto a quelli normalmente eseguiti o per finalità diverse, prima di procedere;
- le variazioni apportate ai livelli di accesso alle informazioni contenenti dati personali consentiti, per ragioni di sicurezza;
- ogni eventuale difficoltà riscontrata nell'esercizio della propria mansione;
- ogni carenza e/o inadeguatezza delle misure di protezione adottate dal Titolare del trattamento nelle aree di propria competenza;
- le richieste di esercizio dei diritti formulate dagli Interessati;
- ogni comportamento od evento che possa determinare una violazione del Modello Data Protection o che, più in generale, sia rilevante ai fini della normativa in materia di protezione dei dati personali.

Ai sensi dell'art. 38 par. 3 GDPR, il DPO riferisce direttamente al Titolare del trattamento in merito all'efficacia e all'osservanza del MODP e di ogni altra procedura in materia di *privacy*, all'emersione di eventuali aspetti critici e alla necessità di interventi modificativi.
A tal fine, il DPO predispone:

- con cadenza annuale, una relazione informativa, relativa all'attività svolta;
- immediatamente, al verificarsi di violazioni di dati, una comunicazione relativa all'evento verificatosi.

6. RAPPORTO CON L'AUTORITÀ DI CONTROLLO

Ogni Stato membro istituisce una o più autorità pubbliche indipendenti con il compito di "sorvegliare l'applicazione del presente regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione" (art. 51 GPDR).

L'Autorità di Controllo in Italia è il Garante della protezione dei dati personali (anche, Garante *Privacy),* competente a conoscere eventuali violazioni di dati personali (*Data breach*) e ad accogliere, nonché decidere su eventuali reclami presentati dagli Interessati.
A norma del Regolamento UE/679/2016, il Garante *Privacy* è anche il soggetto a cui il Titolare del trattamento comunica il nominativo e i dati di contatti del DPO.

In caso di ispezioni in materia di protezione dei dati personali o di richieste di informazioni e documentazione da parte del Garante P*rivacy* o di altre Autorità, ogni soggetto Incaricato è tenuto a informare tempestivamente il DPO, che si coordina con il Titolare del trattamento.

7. REGISTRO DEI TRATTAMENTI

Il Registro dei trattamenti dell'ASST della Valtellina e dell'Alto Lario è un file Excel formato da molteplici cartelle di lavoro, ciascuna dedicata ad uno specifico trattamento come di seguito meglio specificato.
L'Azienda si è dotata di un proprio Registro dei trattamenti, non solo al fine di adempiere all'obbligo normativo previsto dall'art. 30 GDPR, ma anche e soprattutto al fine di dotarsi di uno strumento attraverso il quale svolgere un'analisi accurata dei dati trattati, una mappatura approfondita dei trattamenti ed una ricognizione puntuale delle finalità perseguite.

7.1 Criteri di compilazione e tempistiche di aggiornamento

Il Registro è costituito da più file Excel, uno per ciascuna unità/ciascun servizio coinvolto nel trattamento dei dati.
Il singolo file - scheda di censimento - è poi costituito da più fogli, uno per ogni trattamento eseguito.
Ogni foglio si compone infine di più sezioni, tra cui:

- Ruoli Data Protection, ovvero i) Titolare, ii) Responsabile interno competente, iii) Responsabile del trattamento ex art. 28 GDPR, iv) Co-Titolare, v) DPO;
  Il Responsabile di UOC/UOSD/Servizio è il soggetto individuato come Responsabile Interno dell'Unità cui la scheda riferisce.
  Il Responsabile del trattamento è il soggetto che materialmente provvede alla compilazione della scheda.
  I Co-titolari ed i Responsabili esterni sono invece i soggetti esterni all'Azienda che concorrono nell'esecuzione del trattamento oggetto di descrizione.

- Descrizione del trattamento, ovvero i) Denominazione del trattamento; ii) Base Giuridica; iii) Categorie di interessati, iv) Categorie di dati personali, v) Finalità del trattamento, vi) Ambito di comunicazione e diffusione.
  Nel campo Denominazione del trattamento deve essere indicato brevemente il trattamento cui la scheda si riferisce.
  Nel campo Base Giuridica deve essere indicato il presupposto giuridico in forza di cui il trattamento è eseguito, ad esempio un contratto, un obbligo normativo o un interesse pubblico rilevante.
  Nelle sezioni "Categorie di interessati" e "categorie di dati personali" dovranno essere specificate, attraverso l'apposizione del flag corrispondente alla categoria scelta, le tipologie di persone coinvolte dal trattamento e le tipologie di dati oggetto del medesimo.
  Nel caso in cui le categorie di interesse non figurano tra quelle già presenti, è sufficiente selezionare l'opzione «Altro» e specificare nella casella di testo corrispondente la tipologia di dati o di interessati coinvolti.
  La sezione "Finalità del trattamento" deve invece contenere una breve descrizione del fine perseguito dal trattamento, come ad esempio "ricezione delle prenotazioni e gestione delle stesse per la definizione dell'agenda dell'ambulatorio".
  Il campo "Ambito di comunicazione e diffusione" è invece dedicato all'elencazione dei soggetti esterni all'Azienda a cui i dati saranno comunicati.
  In esso andranno dunque riportati, anche semplicemente per categoria di appartenenza, gli altri Titolari o Responsabili esterni a cui i dati sono trasmessi, come ad esempio il fornitore del software di gestione dell'agenda o Regione Lombardia per l'erogazione delle prestazioni in regime sanitario pubblico.

Per ciascuno dei soggetti indicati dovranno poi essere definiti il motivo della comunicazione, le categorie di dati e di interessati coinvolti, se il soggetto destinatario si trova all'interno dell'Unione Europea o meno.

- Modalità di trattamento, ovvero modalità e tempistiche di conservazione e misure di protezione.
  Nella sezione dedicata alle "Modalità di conservazione" si dovranno indicare i luoghi in cui si conservano le copie cartacee dei documenti ed ogni applicativo utilizzato per il trattamento.
  Nel campo "Tempi di conservazione" dovrà essere indicato il tempo per cui i dati sono conservati, le ragioni della conservazione (ad esempio il rispetto delle previsioni del Massimario della Regione Lombardia) e le azioni poste in essere alla scadenza del tempo definito (ad esempio distruzione del documento o sua anonimizzazione).
  Nell'ultima sezione, denominata "Misure di sicurezza adottate", dovranno essere descritte le misure di sicurezza adottate a protezione dei dati oggetto del trattamento.
  Le misure possono essere descritte anche in forma sintetica, purché dalla descrizione fornita si possa trarre un quadro generale delle stesse integrandolo con il rinvio a documenti ulteriori e di carattere generale (es. procedure organizzative, *policy* IT, ecc.).

Nel caso in cui si determini la necessità di procedere all'aggiornamento di una o più parti del Registro, ciascun Responsabile interno provvede alla creazione di un nuovo foglio Excel, il quale sarà denominato con la data di redazione.
I fogli recanti le schede di censimento obsolete saranno conservati in formato pdf e non saranno più modificabili.
Il file di Registro sarà conservato a cura di ciascun Responsabile interno e sarà reso disponibile in formato elettronico ed in sola visione – tramite piattaforma di condivisione – al personale dell'Ufficio Privacy ed al DPO.

Ciascun Responsabile interno aggiorna il Registro:
(i) ogni volta che vengono modificate le aree di trattamento già registrate o vengono introdotte nuove aree di trattamento;
(ii) in ogni caso, almeno una volta all'anno.

7.1.1 Basi giuridiche del trattamento

Come specificato, l'ASST esegue il trattamento esclusivamente in forza di una delle basi giuridiche previste dall'art. 6 del GDPR o dall'art. 9 GDPR.

Con specifico riferimento al trattamento di dati personali comuni, il trattamento è eseguito esclusivamente in forza di uno dei seguenti presupposti:

i. consenso informato ed esplicito dell'Interessato;
ii. esecuzione di un contratto o di misure precontrattuali su richiesta dell'Interessato;
iii. obbligo legale al quale è soggetto il Titolare;
iv. salvaguardia di interessi vitali dell'Interessato o altra persona fisica;
v. esecuzione di un compito di interesse pubblico o esercizio di pubblici poteri;
vi. perseguimento di un legittimo interesse del Titolare o terzi a condizione che non prevalgano su interessi o diritti fondamentali dell'Interessato che richiedono protezione dei dati personali, soprattutto nel caso di Interessati minori di età.

Il Titolare del trattamento ricorre alla base giuridica di cui al punto vi., perseguimento di un legittimo interesse, solo in casi eccezionali e residuali. Inoltre, il Titolare si impegna - nel caso in cui si rilevasse la necessità di utilizzare tale base giuridica – a svolgere preventivamente un bilanciamento tra l'interesse proprio o di terzi ed interessi, diritti e libertà fondamentali dell'Interessato.
Tale bilanciamento sarà eseguito a cura dell'Ufficio Privacy, con il supporto del DPO.
Il bilanciamento dovrà dare evidenza delle ragioni a sostegno della prevalenza dell'Interesse legittimo del Titolare o dell'Interessato.
Nelle ipotesi in cui il bilanciamento attesti la prevalenza dell'interesse del Titolare o di terzi, il trattamento sarà legittimamente avviato e traccia scritta del bilanciamento con correlato esito saranno archiviati a cura del DPO.
Nei casi in cui emerga una prevalenza degli interessi, delle libertà e dei diritti dell'Interessato, il trattamento non sarà avviato per carenza di un'idonea base giuridica.

Con specifico riferimento al trattamento di dati cd. particolari, al pari di quanto appena descritto per i dati comuni, l'ASST esegue il trattamento dei dati solo ed esclusivamente dopo aver accertato la sussistenza di una delle basi giuridiche di cui all'art. 9 GDPR.
Nello specifico, alla luce delle attività di cura ed assistenza che sono proprie dell'ASST, l'ente ricorre tipicamente alla base giuridica del motivo di interesse pubblico rilevante di cui all'art. 9, par. 2, lett. f) GDPR nonché art. 2-sexies Codice della Privacy).

7.1.2 Tempi di conservazione

Il Titolare del trattamento ha definito i tempi di conservazione di ogni categoria di dati in base alla finalità di impiego dei medesimi.
In particolare, nel Registro dei trattamenti è indicato il termine massimo di conservazione oltre il quale il Titolare si impegna a cancellare i dati o ad adottare procedure che li anonimizzino.

I dati personali trattati dai soggetti che il Titolare ha nominato Responsabili esterni saranno cancellati oppure restituiti al Titolare al termine del rapporto contrattuale che ha legittimato l'utilizzo di tali dati da parte del Responsabile esterno.

7.1.3 Misure Tecniche ed Organizzative

Ai sensi dell'art. 32 GDPR, il Titolare del trattamento, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio.

Le **misure tecniche** adottate dall'Azienda per garantire un adeguato livello di rischio sono, tra le altre:

- controllo accessi (sistemi di autenticazione, sistemi di autorizzazione);
- utilizzo di password complesse;
- obbligo periodico sostituzione password;
- tracciabilità degli accessi ai vari sistemi software clinici e gestionali;
- protezione da malware;
- sistema di backup;
- antivirus;
- firewall;
- archiviazione e gestione dei Log degli amministratori di sistema.

Le **misure organizzative** adottate sono, tra le altre, le seguenti:

- creazione di un organigramma *privacy* e definizione di ruoli e responsabilità;
- adozione di istruzioni chiare e precise sui compiti e le responsabilità di ogni soggetto coinvolto nel trattamento di dati;
- organizzazione di corsi di formazione e di campagne di sensibilizzazione in materia di protezione dei dati personali;
- implementazione di un Modello Organizzativo Data Protection;
- definizione di procedure e *policy* di sicurezza logiche e fisiche;
- creazione di un sistema di separazione dei dati con utilizzo di cartelle dedicate ad accesso limitato ai soli soggetti autorizzati;
- individuazione dei soggetti terzi che hanno accesso ai dati del Titolare, nomina di tali soggetti quali Responsabili esterni e previsione di verifiche periodiche sul rispetto del Regolamento da parte di tali soggetti;
- minimizzazione dell'utilizzo dei dati personali.

8. DATA PROTECTION IMPACT ASSESSMENT

Ai sensi dell'art. 35 del Regolamento UE 2016/679 (di seguito anche "GDPR") il Titolare del trattamento, nel caso in cui tratti una tipologia di dati che, consideratane la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, è tenuto ad effettuare, prima di procedere al trattamento, una valutazione d'impatto *privacy* (di seguito DPIA).

La DPIA è pertanto obbligatoria solo per i trattamenti che presentano un rischio elevato per i diritti e le libertà delle persone fisiche (cfr. considerando 75 GDPR)

Il Regolamento Europeo (Considerando 75 e 76) precisa che il suddetto rischio deve essere misurato con criteri oggettivi che permettano di individuare trattamenti a rischio e a rischio elevato in termini di probabilità e gravità e che tali grandezze debbano essere determinate con attenzione a natura, ambito di applicazione, contesto e finalità di trattamento.

In assenza di ulteriori indicazioni inerenti alla metodologia attraverso cui l'adempimento deve essere condotto, l'ASST ha costruito un processo di valutazione e gestione del rischio privacy seguendo le indicazioni contenute nei Considerando del GDPR, nelle Linee Guida WP248rev.1 adottate in materia dal Gruppo WP29 e nell'Allegato 1 al provvedimento n. 467 dell'11 Ottobre 2018 del Garante privacy italiano.

In particolare il processo così costruito prevede che, al fine di adempiere alle prescrizioni normative, l'Azienda:

esegua un'analisi preliminare di ogni trattamento posto in essere, sulla base di quanto riportato nel Registro dei trattamenti, per verificare la sussistenza delle condizioni per procedere alla DPIA (valutazione rischio astratto);

solo per i trattamenti per cui risulta in essere un rischio astratto elevato, esegua una valutazione d'impatto (DPIA), verificando l'incidenza delle misure tecniche e organizzative nell'attenuazione e gestione del rischio (valutazione rischio residuo);

nei casi in cui la DPIA restituisce come esito un rischio elevato, proceda alla consultazione preventiva del Garante per la protezione dei dati personali ai sensi dell'art. 36 GDPR.

l'Azienda utilizza l'espressione "**rischio**" per indicare *uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità» per i diritti e le libertà* e l'espressione "**rischio astratto**" per indicare *il rischio associato al verificarsi di un possibile evento che possa comportare un impatto sui diritti e le libertà degli Interessati, senza tenere in considerazione le misure di sicurezza interne.*

Il rischio astratto è quindi identificato nel rischio intrinseco che l'Interessato corre nel momento in cui suoi dati sono oggetto di trattamento.

La fase di "Analisi Preliminare" si compone di due sotto-fasi: i) verifica della ricorrenza di una delle ipotesi indicate dall'Autorità Garante nell'Allegato 1 al provvedimento n. 467 dell'11 Ottobre 2018; ii) individuazione e misurazione del rischio astratto correlato ai trattamenti posti in essere.

Con riferimento al punto i), l'ASST confronta ogni trattamento effettuato con l'elenco delle 12 tipologie di trattamento da sottoporre a necessaria valutazione d'impatto pubblicato dall'Autorità Garante e nei casi di corrispondenza procede all'esecuzione della DPIA.

Con riferimento al punto ii), l'ASST sottopone a valutazione specifica del rischio astratto ogni trattamento che non trovi corrispondenza nell'elenco di cui sopra (stante la sua natura esemplificativa e non tassativa).

Nello specifico, il "Rischio astratto" è calcolato attraverso il rapporto tra la "probabilità" (P) che si verifichi un evento lesivo per gli Interessati nell'ambito del singolo trattamento e la "gravità" (G) potenziale di tale impatto.

La "probabilità" (P) è definita attraverso il prodotto di due parametri:
il tipo di trattamento (T): il cui valore è dato dal ricorrere di una o più delle attività indicate dalle citate Linee Guida del Gruppo WP29 come caratterizzate da un "rischio elevato" in quanto potenzialmente lesive dei diritti e delle libertà delle persone fisiche se ricorrenti congiuntamente.
Pertanto, il valore del fatto probabilità cresce al crescere delle ipotesi ricorrenti, seguendo il seguente schema:

Categoria	Descrizione	Valore attribuito
Trascurabile	Il dato non rientra in alcuna delle categorie	1
Basso	Il dato rientra in 1 categoria	2
Medio	Il dato rientra in 2 categorie	3
Elevato	Il dato rientra in più di 2 categorie	4

il numero di interessati coinvolti (Q): la cui incidenza è valutata sulla base dei seguenti 4 parametri:

Categoria	Quantità interessati	Valore attribuito
Trascurabile	Da 1 a 10	1
Basso	Da 11 a 100	2
Medio	Da 101 a 10.000	3
Elevato	Oltre 10.000	4

Correlando gli indicatori relativi al tipo di trattamento (T) e al numero di interessati coinvolti (Q), secondo la matrice $\boldsymbol{P = T \times Q}$, è definito il valore della Probabilità:

			Tipologia trattamento (T)			
			Trascurabile	Bassa	Media	Alta
			1	2	3	4
Quantità di interessati	Trascurabile	1	1	1	2	2
	Bassa	2	1	2	3	3
	Media	3	2	3	3	4
	Alta	4	2	3	4	4

L'attribuzione del valore della probabilità avviene secondo i seguenti 4 livelli:

Probabilità	Valore attribuito
Improbabile	1
Poco probabile	2
Mediamente probabile	3
Altamente probabile	4

Il fattore Gravità, ovvero gli effetti causati sui diritti e le libertà dell'Interessato da un determinato evento, è determinato in base all'incidenza sul dato in termini di disponibilità, integrità e riservatezza.

In particolare, la valutazione è effettuata con l'ausilio dei criteri riportati nella tabella sottostante:

Livello Gravità	Riservatezza (divulgazione e accesso illegittimo)	Integrità (alterazione illegittima)	Disponibilità (distruzione illegittima, indisponibilità, perdita dei dati)
1 - Trascurabile	La mancanza di riservatezza, di integrità o di disponibilità ha impatti lievi (es. fastidio) sulla vita sociale o personale degli interessati. Ad esempio, perdita di tempo nel dover ripetere le procedure o di aspettarle, riutilizzo dei dati da parte di terzi per scopi pubblicitari, senso di violazione della privacy senza danno reale.		
2 - Basso	La mancanza di riservatezza, integrità e disponibilità ha impatti, non critici e che creano piccole difficoltà (es. costi, paura, incomprensioni, stress, malanni minori) a causa degli effetti sulla vita sociale o personale degli interessati.		

3 - <u>Medio</u>	La mancanza di riservatezza, integrità e disponibilità ha un elevato impatto che può essere superato con difficoltà sulla vita sociale o personale degli interessati. Ad esempio fondi non disponibili, blocco da parte di enti economici, danni alla proprietà, perdita del posto di lavoro, denunce, peggioramento della salute, appropriazione indebita di denaro, guadagni persi, perdita di lavoro, vittima di ricatti, cyberbullismo, molestie morali.
4 - <u>Elevato</u>	La mancanza di riservatezza, integrità e disponibilità ha impatti non reversibili sulla vita sociale o personale, e comporta: - perdita di autonomia; - esclusione (p.e. inabilità a lavorare); - sanzioni penali e perdita di libertà; - danni fisici (p.e. danni fisici o mentali a lungo termine o morte); - impossibilità di azione legale; - squilibrio di potere; - perdita di fiducia; - perdita economica.

In base alle valutazioni condotte ad ogni trattamento è attribuito uno dei seguenti quattro livelli di gravità:

Entità/Gravità impatto	Valore attribuito
Trascurabile	1
Basso	2
Medio	3
Elevato	4

Il Rischio Astratto (RA) è pertanto calcolato secondo la seguente tabella:

			Entità e gravità dell'impatto			
			Trascurabile	***Bassa***	***Media***	***Alta***
			1	**2**	**3**	**4**
Probabilità	***Improbabile***	**1**	**1**	**2**	**3**	**4**
	poco	**2**	**2**	**4**	**6**	**8**

	Probabile	3	3	6	9	12
	altamente	4	4	8	12	16

Indice di Rischio	Descrizione
Trascurabile	$R \leq 2$
Basso	$2 < R \leq 4$
Medio	$4 < R \leq 6$
Alto	$6 < R \leq 9$
Elevato	$R > 9$

Per i soli trattamenti in cui il Rischio Astratto sia stato valutato elevato, l'Azienda esegue la valutazione d'impatto ai sensi dell'art. 35 GDPR ed individua il Rischio Residuo (RR), tenendo conto delle misure di sicurezza adottate che consentono, quindi, di arginare l'incidenza del rischio astratto.
Nello svolgimento di tale valutazione sono prese in considerazione le misure di sicurezza che si distinguono in:

- **in misure tecniche**:
  - Controllo accessi (Sistemi di autenticazione, sistemi di autorizzazione);
  - Data transfer;
  - Data storage;
  - Vulnerability management;
  - Protezione da malware;
  - Key management;
  - Archiviazione e gestione dei Log;
  - Continuity management: sistema di Disaster Recovery, sistema di backup;
  - Firewell;
  - Cifratura dei dati;
  - Intrusion detection;
  - Vulnerability assessment/penetration test;
  - Tracciamento operazioni.
- **in misure fisiche**:
  - vigilanza della sede;
  - sistemi di videosorveglianza;
  - ingresso controllato nei locali ove ha luogo il trattamento;
  - sistemi di allarme e/o di sorveglianza antintrusione;
  - registrazione degli accessi;
  - autenticazione degli accessi;
  - custodia in armadi blindati e/o ignifughi;
  - dispositivi antincendio;
  - continuità dell'alimentazione elettrica;

- controllo sull'operato degli addetti alla manutenzione;
- verifica della leggibilità dei supporti;
- monitoraggio parametri ambientali locali macchine.

- **in misure organizzative**:
  - creazione di un organigramma privacy e definizione di ruoli e responsabilità;
  - istruzioni;
  - formazione;
  - elaborazione di un Modello Organizzativo Privacy;
  - procedure e policy di sicurezza logiche e fisiche;
  - audit;
  - strumenti di controllo per gli interessati;
  - separazione dei dati;
  - controllo accessi amministratori;
  - misure di sicurezza per terze parti;
  - minimizzazione dei dati;
  - anonimizzazione dei dati;
  - conservazione adeguata.

La valutazione delle misure di sicurezza è effettuata sulla base dei criteri riportati nella tabella sottostante, i quali danno una corrispondenza in termini di 3 livelli di adeguatezza delle suddette misure:

Livello	Linee guida per la valutazione	Valutazione rischio residuo
1- Inadeguato	Il controllo non è previsto o è assente nella pratica.	Tale livello comporta il mantenimento della classe di rischio individuata per il rischio astratto.
2- Parzialmente adeguato	Le misure sono state adottate, tuttavia sono state rilevate delle mancanze che non ne garantiscono la totale efficacia oppure il controllo è stato implementato, ma è sporadicamente applicato.	Tale livello comporta il passaggio ad una classe di inferiore rischio.
3- Adeguato	Le misure di sicurezza sono adeguate e sistematicamente applicate.	Tale livello comporta il passaggio a due classi inferiori di rischio.

Se all'esito della valutazione d'impatto il rischio rimane elevato, l'Azienda procederà con la consultazione preventiva all'autorità Garante della Privacy ex art. 36 GDPR.