Sistema Socio Sanitario
Regione Lombardia
ASST Bergamo Est

Regolamento sul Modello Organizzativo in materia di Protezione dei dati personali (MOP) della Azienda Socio Sanitaria Territoriale Bergamo Est

Sommario

CAPO I - DISPOSIZIONI GENERALI

Art. 1 - Oggetto

1. Il presente Regolamento sul Modello Organizzativo in materia di Protezione dati personali (MOP) disciplina l'assetto di governo e le disposizioni procedimentali per l'adeguamento dell'Azienda Socio Sanitaria Territoriale Bergamo Est (ASST Bergamo Est) al Regolamento Generale Protezione Dati UE del 27 aprile 2016 n. 679 (RGPD o GDPR) ed al D. Lgs. n. 196 del 30 giugno 2003 ("Codice in materia di protezione dei dati personali" o "Codice Privacy") e successive modifiche ed integrazioni.
2. Nello specifico, il presente documento regolamenta:

- **Principi**: definisce norme e principi cui deve ispirarsi l'attività dell'Ente in materia di protezione dei dati personali;
- **Sistema di gestione**: delinea l'organizzazione attuativa di riferimento nello svolgimento delle attività aziendali al fine di prevenire eventi avversi in tema di trattamento di dati, in un'ottica di monitoraggio e miglioramento continuo dei processi e delle procedure;
- **Supervisione e vigilanza**: individua un organo indipendente cui compete la vigilanza sull'efficacia e sull'adeguatezza del Modello Organizzativo;
- **Formazione ed informazione interna**: definisce le linee di indirizzo per sensibilizzare il personale sui rischi in tema di trattamento di dati personali e sull'importanza di allineamento al Modello Organizzativo.

Art. 2 - Principi organizzativi

1. Il presente Regolamento si ispira alle linee guida e agli indirizzi standard di settore, tra i quali, a titolo di esempio, il **NIST** (*National Institute of Standard and Technologies*, USA) **Privacy Framework**, il quale organizza le attività di gestione della privacy e dei rischi correlati in cinque funzioni principali, implementate all'interno di un processo di monitoraggio e miglioramento continuo:

1. **Identifica e censisci**: individuare attori, oggetti e situazioni di rischio, anche potenziale, per la sicurezza dei dati personali.
2. **Governa**: stabilire una strategia di governo del rischio, definendo ruoli, responsabilità e obiettivi.
3. **Controlla**: valutare la situazione ed implementare adeguate misure di controllo.
4. **Comunica e diffondi**: comunicare, in modo trasparente e proattivo, con gli Interessati e i soggetti coinvolti nella tutela dei dati personali a livello aziendale.
5. **Proteggi**: attuare le adeguate misure tecniche ed organizzative al fine di garantire che il trattamento dei dati personali sia effettuato in conformità con la normativa vigente e non comporti rischi per la salvaguardia dei dati stessi.

In particolare, nella distribuzione interna di ruoli e responsabilità relative al trattamento dei dati, si deve tenere conto di:

1. **Corretta separazione dei ruoli**, al fine di evitare la sovrapposizione tra funzioni di controllo e funzioni attuative, e partizionare il dominio di gestione operativa in ambiti coerenti (copertura e specificità).
2. **Mappatura delle competenze e degli ambiti di gestione**.
3. **Ciclo di vita della gestione**, articolata nelle seguenti fasi:
   a. **Mappatura** degli attori e degli oggetti (asset aziendali, trattamenti, situazioni di rischio, ecc.);

b. **Pianificazione** delle azioni;
c. **Valutazione** degli effetti;
d. **Ritorno** al punto a.

CAPO II - MODELLO ORGANIZZATIVO

Art. 3 - Inquadramento preliminare

1. Al fine di conseguire un'effettiva conformità al dettato normativo del GDPR, il Titolare del trattamento è tenuto a definire, con chiarezza, i ruoli e le specifiche responsabilità dei soggetti coinvolti ai vari livelli gestionali, di controllo e operativi, nelle diverse fasi del processo di trattamento dei dati personali, dalla loro raccolta ed elaborazione sino alla successiva dismissione (cancellazione e/o anonimizzazione).

Pertanto, in attuazione dei principi di specificità, pertinenza, e adeguatezza, il Modello Organizzativo in materia di Protezione dei dati personali dell'ASST Bergamo Est, individua, a copertura del perimetro di ambito, i seguenti soggetti:

- Titolare del trattamento;
- Responsabile della Protezione dei Dati personali;
- Responsabili delle Funzioni di Produzione;
- Responsabili delle Funzioni Tecnologiche e di Servizio;
- Referenti Privacy;
- Responsabile esterno del trattamento;
- Autorizzati al trattamento;
- Settore Privacy.

Art. 4 - Titolare del trattamento

1. L'Azienda Socio-Sanitaria Territoriale Bergamo Est rappresentato, ai fini previsti dal GDPR, dal Direttore Generale, è il Titolare del trattamento dei dati personali (d'ora in poi anche solo "Titolare") raccolti anche in banche dati, digitali o cartacee.
2. Il Titolare è responsabile del rispetto dei princìpi applicabili al trattamento di dati personali stabiliti dall'art. 5 GDPR:
   - liceità, correttezza e trasparenza;
   - limitazione della finalità e minimizzazione dei dati;
   - esattezza;
   - limitazione della conservazione;
   - integrità e riservatezza.

3. Il Titolare mette in atto le misure tecniche ed organizzative adeguate a garantire e a dimostrare che il trattamento di dati personali sia effettuato in modo conforme al GDPR.
4. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa e di bilancio mediante analisi della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.
5. Il Titolare provvede a:
   a) nominare il Responsabile per la Protezione dei Dati (RPD) o *Data Protection Officer* (d'ora in poi anche solo "DPO");

b) nominare i Responsabili delle Funzioni di Produzione ed i Responsabili delle Funzioni Tecnologiche e di Servizio, individuati nelle persone dei Dirigenti apicali delle singole Strutture in cui si articola l'organizzazione dell'Ente, quali soggetti attuatori degli adempimenti necessari per la conformità dei trattamenti dei dati personali effettuati dall'Ente e preposti al trattamento dei dati contenuti nelle banche dati di competenza delle articolazioni organizzative cui sono preposti;
c) garantire la formazione adeguata dei Responsabili delle Funzioni di Produzione e dei Responsabili delle Funzioni Tecnologiche e di Servizio in materia di trattamento dei dati personali;
d) assegnare compiti distinti a specifiche Strutture, in ragione delle peculiari competenze alle medesime attribuite dal POAS, al fine di avvalersi di particolari contributi ed apporti funzionali per il concreto e fattivo adeguamento dell'Ente al GDPR;
e) definire gli indirizzi per l'attribuzione di specifiche competenze al Settore Privacy al fine di supportare l'attività del DPO anche nel rapporto con le Strutture organizzative dell'Ente e fornire a queste ultime le necessarie indicazioni in materia di protezione dati sui trattamenti sviluppati dalle stesse;
f) definire gli indirizzi riguardo alla funzione di raccordo e di collaborazione con il Garante per la Protezione dei Dati Personali (d'ora in poi anche solo "Garante Privacy").

6. Il Titolare è Contitolare del trattamento, ai sensi dell'art. 26 del GDPR, nel caso di esercizio associato di funzioni e servizi, allorché due o più Titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento.

Art. 5 - Data Protection Officer (DPO)

1. Il *Data Protection Officer* è individuato nella figura unica di un professionista o di una società nel rispetto delle prescrizioni recate dal Codice degli appalti in materia di contratti di servizio, e deve possedere i requisiti specificati dagli artt. 37 e 38 del GDPR.
2. Il DPO è incaricato dei seguenti compiti:
a) informare e fornire consulenza all'Ente (in qualità di Titolare o di Responsabile esterno del trattamento), nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal GDPR e dalle altre normative relative alla protezione dei dati personali;
b) fornire, se richiesto, un parere in merito alla Valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento;
c) rendere una consulenza idonea, scritta od orale, anche nell'individuazione dei rapporti intercorrenti con soggetti terzi in materia di protezione dei dati;
d) cooperare con il Garante Privacy e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 GDPR, ed effettuare, se del caso, consultazioni relativamente ad ogni altra questione inerente al trattamento di dati personali;
e) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dall'Ente (in qualità di Titolare o di Responsabile esterno del trattamento);
f) altri compiti e funzioni a condizione che l'Ente (in qualità di Titolare o di Responsabile esterno del trattamento) si assicuri che non diano adito a un conflitto di interessi. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del DPO.

3. Il DPO dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente. L'ASST Bergamo Est (in qualità di Titolare o di Responsabile esterno del trattamento) fornisce al DPO le risorse necessarie per assolvere ai compiti attribuiti e per accedere ai dati personali ed ai trattamenti posti in essere.

4. Ferma restando l'indipendenza nello svolgimento dei compiti allo stesso attribuiti, il DPO riferisce direttamente all'Ente (in qualità di Titolare o di Responsabile esterno del trattamento). Nel caso in cui siano rilevate dal DPO o sottoposte alla sua attenzione decisioni incompatibili con il GDPR e con le indicazioni fornite dallo stesso DPO, questo è tenuto a manifestare le proprie osservazioni e i propri rilievi comunicandoli all'Ente (in qualità di Titolare o di Responsabile esterno del trattamento),

Art. 6 - Responsabili delle Funzioni di Produzione

1. I Responsabili delle Funzioni di Produzione (RdP) sono individuati nei Dirigenti apicali delle Unità Operative, mediche e non mediche, che partecipano direttamente alle varie fasi del processo produttivo, incluse quelle preparatorie e seguenti agli atti medici.
2. Il Titolare formalizza tale incarico con apposito atto di nomina, nel quale vengono indicati gli specifici ambiti di attività o l'elenco dei trattamenti di dati personali cui è preposto ciascun Responsabile.
3. I Responsabili delle Funzioni di Produzione sono investiti delle seguenti responsabilità:
   a) vigilare sul corretto utilizzo delle risorse tecniche ed ambientali a propria disposizione, secondo le direttive impartite dai Responsabili delle Funzioni Tecnologiche e di Servizio;
   b) vigilare sul comportamento tenuto dal personale afferente alla propria Unità Operativa in relazione alla protezione dei dati personali;
   c) definire e attuare, su base almeno annuale, opportuni momenti di aggiornamento formativo e informativo per il personale della propria Unità Operativa;
   d) attuare un efficace sistema di comunicazione e allerta (escalation) in relazione a eventi avversi inerenti al proprio ambito di competenza;
   e) fornire il proprio contributo nella fase istruttoria conseguente alla presentazione di istanze da parte degli Interessati relativamente ai trattamenti di dati di competenza della propria Struttura organizzativa.
4. Gli stessi, inoltre, provvedono a:
   a) verificare la legittimità dei trattamenti di dati personali effettuati dalla Struttura di riferimento;
   b) documentare, in apposito registro, eventuali eventi avversi e non conformità in ambito privacy;
   c) individuare i soggetti Autorizzati al trattamento per la Struttura organizzativa di competenza e attribuire loro specifici compiti e attività di protezione dei dati;
   d) individuare ed incaricare, se ritenuto opportuno, i Referenti Privacy per la propria Struttura organizzativa;
   e) organizzare incontri periodici con i Responsabili delle Funzioni Tecnologiche e di Servizio al fine di valutare eventi e situazioni specifici del proprio ambito organizzativo;
   f) aggiornare i Registri delle attività di trattamento dei dati personali di cui all'art. 30 del GDPR;
   g) individuare e valutare eventuali rischi privacy connessi a soggetti e oggetti gestiti (personale, ambienti e relative dotazioni tecniche);
   h) rilevare e comunicare al Settore Privacy i casi di violazione dei dati personali (*Data Breach*) nell'ambito organizzativo di riferimento.

Art. 7 - Responsabili delle Funzioni Tecnologiche e di Servizio

1. I Responsabili delle Funzioni Tecnologiche e di Servizio (RdS) sono individuati nei Dirigenti apicali delle seguenti Strutture dell'Ente:
   - S.C. Sistemi Informativi Aziendali;
   - S.S. Ingegneria Clinica;
   - S.C. Gestione Tecnico Patrimoniale;
   - S.C. Gestione e Sviluppo delle Risorse Umane;
   - S.C. Qualità Risk Management e URP

2. Il Titolare formalizza tale incarico con apposito atto di nomina, nel quale vengono indicati gli specifici ambiti di attività o l'elenco dei trattamenti di dati personali cui è preposto ciascun Responsabile.
3. Ai Responsabili delle Funzioni Tecnologiche e di Servizio compete il governo (acquisizione e attivazione, configurazione, posizionamento e esercizio, gestione corrente ed evolutiva, cessazione e dismissione, ecc.) degli asset tecnici ed operativi impiegati nei processi produttivi (ICT, dispositivi medicali, ambienti e dotazioni relative, dotazioni cartacee, risorse umane), nonché la gestione del ciclo di vita delle dotazioni tecniche e tecnologiche dell'Azienda.
4. I Responsabili delle Funzioni Tecnologiche e di Servizio sono incaricati dei seguenti compiti:

a) individuare e valutare i rischi privacy connessi alla gestione del proprio ambito di competenza;
b) definire ed attuare le misure tecniche ed organizzative, preventive, correttive e di governo, per l'attenuazione del rischio privacy;
c) individuare i soggetti Autorizzati al trattamento per la Struttura organizzativa di competenza e attribuire loro specifici compiti e attività di protezione dei dati;
d) individuare ed incaricare, se ritenuto opportuno, i Referenti Privacy per la propria Struttura organizzativa;
e) definire e attuare, su base almeno annuale, opportuni momenti di aggiornamento formativo e informativo rivolti al personale della propria struttura organizzativa;
f) aggiornare i Registri delle attività di trattamento dei dati personali di cui all'art. 30 del GDPR;
g) gestire le Valutazioni di impatto sulla protezione dei dati ex art. 35 GDPR;
h) rilevare e comunicare al Settore Privacy i casi di violazione dei dati personali (*Data Breach*) nell'ambito organizzativo di riferimento.

Art. 8 - Referenti Privacy

1. I Referenti Privacy sono nominati dai Responsabili delle Funzioni di Produzione e dai Responsabili delle Funzioni Tecnologiche e di Servizio ai sensi degli artt. 6 e 7 del presente Regolamento, e sono incaricati della generale attività di supporto al Responsabile nello svolgimento e nello sviluppo dei compiti di responsabilità al medesimo attribuiti dal Titolare.
Nel compimento delle proprie attività il Referente è funzionalmente coordinato dal Settore Privacy.
2. In via principale, i compiti di supporto affidati al Referente riguardano:

a) l'attuazione, all'interno della propria Struttura organizzativa, delle procedure e le linee guida aziendali per la corretta gestione dei dati, assicurando che gli Interessati ricevano, ai sensi degli artt. 13 e 14 del GDPR, le opportune informazioni relativamente al trattamento dei dati personali;
b) la comunicazione delle modifiche intervenute nei trattamenti di competenza della propria Struttura organizzativa;
c) la verifica e il supporto all'attività svolta dagli Autorizzati;
d) la trasmissione, al Settore Privacy, delle istanze provenienti dagli Interessati;
e) gli adempimenti correlati con la rilevazione dei casi di violazione dei dati personali (*Data Breach*);
f) la raccolta e successiva rendicontazione verso il Responsabile dei bisogni formativi e informativi del personale della Struttura di appartenenza.

Art. 9 - Responsabile esterno del trattamento

1. Ai sensi dell'art. 28 del GDPR, il Responsabile esterno del trattamento è il soggetto, pubblico o privato, che tratta dati personali, anche particolari, per conto del Titolare e che presenta garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate, in modo che il trattamento soddisfi i requisiti previsti dal GDPR e garantisca la tutela dei dati dell'Interessato.

Il Titolare del trattamento formalizza il ruolo di Responsabile esterno mediante atto giuridico redatto in forma scritta, il quale specifica la finalità perseguita, la tipologia dei dati, la categoria degli Interessati, la durata del trattamento, gli obblighi e i diritti del Responsabile esterno e le modalità di trattamento. Tale atto può anche basarsi su clausole contrattuali tipo adottate dal Garante Privacy oppure dalla Commissione Europea.
2. Qualora l'Ente proceda alla nomina di Responsabili esterni dovrà prevedere, in sede di contratto di servizio, che questi ultimi:

- sviluppino il Registro dei trattamenti coordinandosi con l'Ente, comunicandone allo stesso contenuto e aggiornamenti;
- provvedano alla definizione, adozione e comunicazione all'Ente delle misure di sicurezza adeguate al livello di rischio sostenuto.

Art. 10 - Autorizzati

1. I Responsabili di cui agli artt. 6 e 7, individuano, nell'ambito della propria Struttura organizzativa di competenza, gli Autorizzati al trattamento quali persone fisiche ammesse al trattamento dei dati personali.
2. Nell'atto di individuazione, i Responsabili indicano, per ciascun Autorizzato, gli ambiti di attività e/o l'elenco dei trattamenti di competenza.

Art. 11 - Settore Privacy

1. Il Settore Privacy collabora e supporta il DPO nel rapporto con tutte le Strutture organizzative in materia di adeguamento al GDPR.
2. Tale funzione compete alla S.C. Affari Generali e Legali, individuata dal POAS quale Struttura preposta al coordinamento dell'applicazione della normativa in materia di tutela dei dati personali, che vi provvede avvalendosi della collaborazione di figure professionali esterne.
3. Al Settore Privacy competono, in via principale, compiti di vigilanza attiva e proattiva che, nello specifico, si traducono nelle seguenti attività:

a) vigilare sugli adempimenti previsti nel presente Regolamento;
b) vigilare sull'attuazione dei provvedimenti emessi dal Garante Privacy;
c) collaborare con il DPO al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
d) programmare, dandone opportuna comunicazione al DPO, un calendario di audit da svolgere verso i soggetti attuativi previsti nel presento Regolamento;
e) promuovere la formazione del personale e dei collaboratori di cui si avvale l'Azienda;
f) trasmettere i pareri richiesti dalle Strutture organizzative dell'Ente al DPO;
g) coordinare funzionalmente i Referenti nominati dai Responsabili interni relativamente all'ambito organizzativo di propria competenza;
h) individuare modalità e procedure operative volte alla conservazione del Registro delle attività di trattamento;
i) supervisionare la gestione degli episodi di violazione dei dati personali (*Data Breach*);
j) verificare, redigere e aggiornare i testi delle informative privacy, dei consensi e degli incarichi in accordo con le funzioni competenti;
k) essere punto di ricezione e orchestrazione delle richieste degli Interessati in materia di accesso, rettifica, cancellazione, limitazione del trattamento e portabilità dei dati;
l) ricezione e risposta alle richieste degli Interessati inviate direttamente al Settore Privacy.

Art. 12 – Gruppo Privacy Aziendale

1. In considerazione della complessità della materia e della trasversalità delle competenze coinvolte, il settore Privacy, nell'espletamento delle funzioni di cui all'art. 11 del presente Regolamento, si avvale della collaborazione del Gruppo Privacy Aziendale.
2. Il Gruppo Privacy, quale organismo collegiale multidisciplinare, è composto obbligatoriamente dal Dirigente della S.C. Affari Generali e Legali, della S.C. Sistemi Informativi Aziendali e della S.S. Ingegneria Clinica, nonché da un Collaboratore Amministrativo con funzioni di Segretario. Tale composizione potrà essere di volta in volta integrata, in ragione delle esigenze e/o delle criticità rilevate, con la partecipazione di soggetti appartenenti a Strutture aziendali diverse da quelle precedentemente indicate.
3. Nello svolgimento delle proprie attività il Gruppo Privacy opera in sinergia diffusa con tutti i soggetti del "sistema privacy" dell'ASST Bergamo Est, al fine di prevenire o evitare possibili conflitti organizzativi e favorire, in tal modo, l'adeguamento continuo alla normativa sulla protezione dei dati personali.

Art. 13 - Documentazione a sostegno della dimostrazione di presa in carico ("*accountability*")

1. Il principio di *accountability*, inteso come responsabilizzazione e obbligo di rendicontazione, impone al Titolare del trattamento il rispetto delle prescrizioni normative ed esplicita la richiesta di documentare la conformità al GDPR.
2. Al fine di dare concreta attuazione al suddetto principio è dunque indispensabile che il Titolare del trattamento provveda alla regolare tenuta della documentazione di seguito indicata:

1. registri delle attività di trattamento svolte dall'Ente ai sensi dell'art. 30 del GDPR (registro dei trattamenti);
2. documentazione relativa alla valutazione del rischio, rivalutata periodicamente;
3. documentazione relativa alle misure di sicurezza in essere, pianificate o in corso di adozione, con il riferimento alle informazioni di supporto (documenti tecnici, procedure, istruzioni operative, LOG informatici dei sistemi di protezione, registri degli accessi, ecc.);
4. piano di attuazione delle misure di sicurezza;
5. registri delle violazioni (*Data Breach*) e le relative procedure;
6. documentazione relativa alle Valutazioni di impatto (DPIA) e le relative procedure;
7. documentazione relativa ai rapporti con gli Interessati (informative sul trattamento, procedure di gestione dell'esercizio dei diritti e di gestione dei consensi);
8. documentazione di supporto relativa a specifiche attività di trattamento (quali, a titolo di esempio, relazioni tecniche, valutazioni preliminari, autorizzazioni, riferite a sistemi di videosorveglianza, localizzazione satellitare, particolari dispositivi tecnologici, attività di profilazione, ecc.);
9. audit report e relazioni periodiche formalizzate dal DPO nel corso degli audit e delle verifiche di competenza;
10. indice, diario e scadenziario delle revisioni dei documenti di cui sopra.

Art. 14 – Sicurezza e protezione dei dati (Rinvio)

Per quanto attiene alla sicurezza e alla protezione dei dati personali si rinvia ai documenti aziendali in materia.