Regolamento del Comitato Privacy

ASST dei Sette Laghi

1. PREMESSA

Il "Comitato Privacy" (di seguito anche "Comitato") è stato costituito con deliberazione n. 1438 del 01.09.2005. Esso è un organismo aziendale previsto dal Piano di Organizzazione Aziendale Strategico (POAS) 2016-2018 che ne regola la collocazione gerarchico – funzionale nell'ambito dell'organizzazione aziendale, ne attribuisce il coordinamento e ne determina le principali funzioni.

Il Comitato è parte integrante del Modello di Organizzazione dell'ASST dei Sette Laghi per la gestione e la protezione dei dati personali (Modello Organizzativo "Data Protection" - MODP).

2. OGGETTO

Il presente Regolamento ha lo scopo di disciplinare il funzionamento del Comitato e, in particolare, definire i criteri per l'organizzazione e lo svolgimento dei lavori.

3. COMPOSIZIONE DEL COMITATO PRIVACY

Il Comitato alla data di approvazione del presente Regolamento è costituito da cinque componenti ovvero, in conformità alla deliberazione del Direttore Generale n. 263 del 21.05.2020, da:

- un Dirigente Medico di Direzione Medica;
- un Dirigente Avvocato della S.C. Affari Generali e Legali;
- il Direttore S.C. Sistemi Informativi Aziendali;
- un Dirigente Amministrativo assegnato in via esclusiva al Comitato;
- un Coadiutore Amministrativo assegnato in via esclusiva al Comitato con funzioni di segretario.

La composizione del Comitato è suscettibile di variazione mediante apposito provvedimento deliberativo della Direzione aziendale, nel rispetto del POAS vigente, senza implicare la necessità di aggiornare il presente regolamento.

4. COORDINAMENTO DEL COMITATO PRIVACY E INDIVIDUAZIONE DI UN REFERENTE

Il ruolo di Coordinatore del Comitato è riconosciuto dal Piano di Organizzazione Strategico Aziendale al Dirigente Medico di Direzione Medica.

Il ruolo di "Referente" del Comitato Privacy è attribuito al Dirigente Amministrativo, assegnato in via esclusiva al Comitato.

Il Dirigente Amministrativo ("Referente") insieme al Coadiutore amministrativo ("Segretario") compongono l"'Ufficio operativo" del Comitato Privacy.

5. PRINCIPI E CRITERI DI FUNZIONAMENTO DEL COMITATO PRIVACY

Il Comitato, in ossequio al POAS, supporta il Titolare/Datore di Lavoro nella *verifica dello stato di attuazione* del "Codice Privacy", nel *completamento degli adempimenti di legge* e nel *monitoraggio ed aggiornamento dello stato di attuazione e del livello di applicazione della normativa vigente in materia di protezione dei dati personali* (Regolamento n. 679/2016/UE e Codice Privacy n. 196/2003 e smi).

Il Comitato svolge le proprie funzioni con l'obiettivo di creare una sinergia diffusa tra tutti i soggetti del "sistema privacy" dell'ASST dei Sette Laghi, prevenire o evitare possibili conflitti organizzativi, e favorire in tal modo l'adeguamento continuo alla normativa sulla protezione dei dati personali delle persone fisiche. A tale scopo può interagire con tutti i soggetti del Modello organizzativo di trattamento dati adottato dall'ASST dei Sette Laghi ("Modello Organizzativo - Data Protection").

Nell'esercizio delle suddette funzioni il Comitato si raccorda in modo particolare, sistematico e trasparente, con il Responsabile per la Protezione dei Dati (R.D.P.) o Data Protection Officer (D.P.O) di cui all'art. 37 e ss del Regolamento n. 679/2016/UE.

Il Comitato inoltre supporta la Direzione e/o le strutture competenti (SC Controllo di gestione o SS Politiche Sindacali) per definire e monitorare il raggiungimento degli obiettivi di budget finalizzati all'adeguamento continuo dell'Azienda al Regolamento generale Europeo n. 679/2016 sulla protezione delle persone fisiche con riguardo al trattamento di dati personali, ed alla normativa vigente in materia (c.d. "privacy");

6. APPROVAZIONE DI REGOLAMENTI, LINEE GUIDA, PROCEDURE O MODELLI AZIENDALI.

Nell'esercizio delle funzioni di supporto per l'applicazione del GDPR il Comitato, d'intesa con il DPO:

1. Verifica ed approva preliminarmente, sotto un profilo tecnico, la documentazione prevista dal Modello Organizzativo (MODP) e di modelli/procedure necessarie ad attuarlo. In via esemplificativa:
   - Modello di Organizzazione, gestione e protezione dei dati personali (Modello "Data Protection");
   - Modello aziendale dell'atto nomina dei Responsabili Interni da parte del Titolare;
   - Modello aziendale dell'atto di nomina dei Responsabili Esterni da parte del Titolare (o di soggetti delegati dal Titolare);
   - Modello aziendale di nomina dei soggetti autorizzati al trattamento dati (o "Incaricati"), da parte di ciascun Responsabile Interno;
   - Privacy policy del Sito Internet (inclusa Cookie policy);
   - Moduli standard di Informativa e/o di Consenso (ad esempio per degenze, prestazioni ambulatoriali, personale dipendente e collaboratori, fornitori, etc. etc.);
   - Procedura "Data Breach" (o "Data Breach policy");
   - Procedura "DPIA" ("Data Protection Impact Assessment");
   - Procedura "Audit policy";
   - Procedure riguardanti i registri "privacy" dell'ASST dei Sette Laghi.
2. Verifica ed approva preliminarmente inoltre, sotto un profilo tecnico e limitatamente ai soli aspetti concernenti il trattamento di dati personali, la documentazione predisposta dalle Strutture aziendali competenti per materia. In via esemplificativa Regolamenti/Linee guida o procedure:

- di natura informatica attinenti al trattamento dati (regolamenti o procedure ICT sull'utilizzo di strumenti informatici, nomina degli Amministratori di sistema, oscuramento o deoscuramento, assegnazione caselle di posta elettronica etc. etc.);
- riguardanti la videosorveglianza;
- riguardanti processi di erogazione di prestazioni sanitarie (in particolare procedure di telemedicina, nelle sue varie forme di televisita, teleconsulto, tele cooperazione, teleriabilitazione, tele monitoraggio a distanza, etc. etc.) o socio sanitarie;
- riguardanti la pubblicazione di documenti, informazioni e dati secondo la normativa vigente in materia di trasparenza o per motivi di pubblicità legale.

L'Ufficio operativo del Comitato provvede a curare l'istruttoria dei procedimenti finalizzati all'approvazione tecnica e/o all'espressione di parere preliminare da parte del Comitato.

La piena condivisione della documentazione tra Comitato Privacy ed Ufficio Operativo è assicurata anche mediante l'utilizzo della medesima casella di posta elettronica aziendale "comitato.privacy@asst-settelaghi.it".

7. COMPITI ULTERIORI DELL'UFFICIO OPERATIVO IN MATERIA DI APPROVAZIONE DI REGOLAMENTI, LINEE GUIDA, PROCEDURE O MODELLI AZIENDALI

L'Ufficio operativo cura i processi di predisposizione, verifica, approvazione, emissione e pubblicazione della documentazione di cui all'art. 6.1, privilegiando l'adozione di format aziendali. A tale scopo si raccorda con la S.C. Qualità, autorizzazione, accreditamento e rischio clinico e accreditamento (S.C. QAARC) per la verifica di conformità ai format aziendali e per la codificazione della citata documentazione.

L'Ufficio operativo inoltre supporta le Strutture aziendali che intendono predisporre Regolamenti/Linee guida o procedure che impattano sul trattamento dei dati personali. Le citate Strutture, pertanto, hanno l'onere di attivarsi sin dalla fase di progettazione e prima della approvazione/emissione dei documenti fornendo all'Ufficio ogni elemento utile o necessario a tale scopo (Privacy by design). Il raccordo tra le Strutture e l'Ufficio Operativo è favorito in particolare dalla S.C. QAARC, che coordina istituzionalmente le attività di miglioramento qualitativo anche per mezzo di procedure di certificazione.

L'Ufficio inoltre:

- cura la predisposizione delle proposte di deliberazione alla Direzione Generale per la formale adozione di Regolamenti "privacy", di carattere generale, preventivamente approvati in sede tecnica dal Comitato privacy;
- cura, interfacciandosi con l'URP, la pubblicazione sul sito internet ed intranet dell'ASST di documenti afferenti al MODP;
- favorisce il raccordo tra il DPO e le Strutture aziendali, inclusa la SS Anticorruzione, trasparenza ed Audit, per questioni riguardanti la pubblicazione di documenti, informazioni

e dati secondo la normativa vigente in materia di trasparenza o per motivi di pubblicità legale.

- svolge in generale una funzione di filtro e, nei casi più complessi, di facilitazione, anche favorendo i rapporti tra soggetti del modello organizzativo (ad esempio Responsabili Interni) ed il Comitato e/o il DPO.

8. COLLABORAZIONE CON IL DPO NELLE ATTIVITÀ DI VIGILANZA E DI VERIFICA

Il DPO può avvalersi della collaborazione del Comitato per pianificare la propria attività di vigilanza e verifica e per valutarne gli esiti. In relazione a tale attività di vigilanza il DPO può altresì avvalersi dell''Ufficio Operativo per attuare eventuali iniziative di AUDIT, siano esse iniziative sistematiche (pianificate preventivamente secondo criteri di priorità e frequenza) o iniziative contingenti o estemporanee su documentazione, flussi informativi, eventi, segnalazioni e/o richieste pervenute al Titolare.

Nell'esecuzione delle suddette attività potranno essere coinvolti il team di supporto del DPO ed in generale risorse qualificate, interne o esterne, che possano fornire indicazioni o informazioni utili in merito allo svolgimento degli audit;

In via esemplificativa la collaborazione può essere correlata:

1. alle attività di aggiornamento del Registro delle attività di trattamento;
2. alle analisi dei rischi e alle priorità di intervento individuate per la risoluzione delle problematiche relative ai trattamenti che presentino maggiori rischi tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo;
3. alle analisi di impatto sulla protezione dei dati (DPIA - Data Protection Impact Asessment");
4. All'esecuzione di Audit;
5. all'esame di istanze, particolarmente rilevanti o significative ai fini dell'applicazione del DGPR, prodotte dagli "Interessati".
6. Alle segnalazioni relative alla violazione dei dati personali

9. FORMAZIONE E COMUNICAZIONE

Il Comitato propone iniziative formative in materia di Protezione dei dati personali delle persone fisiche, raccordandosi tramite l'Ufficio operativo con le competenti strutture aziendali e, in particolare, con la SS Formazione del personale. Quest'ultima gestisce e conserva la documentazione delle iniziative formative dell'Azienda.
Il Comitato cura inoltre l'efficienza comunicativa interna, finalizzata ad una piena sensibilizzazione del personale autorizzato al trattamento di dati personali.

10. REGISTRI

In via ricognitoria i Registri obbligatori sono i seguenti:

- Registro delle Attività di Trattamento dati (gestito dal Titolare tramite i Responsabili Interni con il supporto del DPO e dell'Ufficio Operativo);
- Registro Data Breach (disciplinato da apposita procedura).

L'Azienda inoltre si è dotata di un:

- Registro degli Atti di nomina dei Responsabili Interni (tenuto a cura dell'Ufficio Operativo del Comitato);
- Registro delle Istanze degli Interessati (tenuto a cura del DPO).

Possono essere istituiti ulteriori registri senza modificare il presente Regolamento, previo parere del Comitato e d'intesa con il DPO (ad esempio in via ipotetica un Registro DPIA per le valutazioni di impatto effettuate prima dei trattamenti).

La cura dei Registri è finalizzata a supportare il Titolare nella gestione documentale in materia di protezione dei dati personali delle persone fisiche anche ai fini della esibizione a terzi ed allo scopo di documentare le attività poste in essere dal Titolare (principio di "Accountability").

11. REPORTING E FLUSSI INFORMATIVI

Il Comitato riferisce direttamente al Titolare del trattamento in merito all'efficacia e osservanza del Modello Data Protection e di ogni altra procedura in materia di privacy, all'emersione di eventuali aspetti critici, alla necessità di interventi modificativi. A tal fine, il Comitato predispone con cadenza annuale, entro il 31 gennaio di ogni anno, una relazione informativa riepilogativa, relativa all'attività svolta, anche sulla base dei flussi informativi periodici del DPO, e propone un piano di attività annuale.

12. IL DPO

Il DPO partecipa al Comitato Privacy ed esercita una funzione di supporto e sorveglianza in accordo al disposto degli art. 37 e ss. GDPR.
Ai sensi della normativa vigente, il DPO provvede, tra l'altro, a:

- vigilare sull'osservanza del GDPR e delle disposizioni nazionali, nonché delle politiche dell'Azienda 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;
- informare il Comitato e, ove opportuno, direttamente il Titolare del trattamento, in merito agli obblighi derivanti dal GDPR e da altre disposizioni nazionali in materia di protezione dei dati personali;
- definire un Piano di verifica annuale e svolgere audit periodici al fine di verificare l'osservanza del GDPR e di altre disposizioni nazionali in materia;
- cooperare con il Garante italiano per la protezione dei dati personali per le questioni connesse al trattamento, tra cui la consultazione preventiva, il supporto nell'accesso da parte del Garante ai documenti e alle informazioni necessarie per l'adempimento dei suoi compiti, nonché ai fini dell'esercizio dei suoi poteri d'indagine, correttivi, autorizzativi e consultivi;
- operare come punto di contatto per gli Interessati in merito al trattamento dei loro dati personali, anche particolari, e all'esercizio dei diritti previsti dal GDPR;
- redigere, su richiesta, pareri in merito alla valutazione d'impatto sulla protezione dei dati condotta dell'ente.

Il DPO dell'ASST dei Sette Laghi svolge i suoi compiti sulla base di un appalto di servizi in coerenza con l'art. 37 del Regolamento Europeo n. 679/2016. I compiti e le funzioni del DPO e del suo team sono dettagliati nella documentazione contrattuale del citato appalto, aggiudicato con provvedimento deliberativo n. 1636 del 31.12.2018.

13. RIUNIONI

Il Comitato si riunisce di norma ogni 15 giorni, con la partecipazione del DPO. Il Comitato svolge le proprie funzioni in forma collegiale.

Ai fini dell'approvazione formale, in sede tecnica, di documenti, linee guida, procedure o atti riguardanti la protezione dei dati sono valide le riunioni con la presenza della maggioranza dei component (attualmente tre su cinque). Si intende validamente costituita anche la riunione alla quale, pur in assenza di formale convocazione, partecipino tutti i componenti.

Alle riunioni del Comitato possono essere invitati anche altri soggetti e alle stesse possono sempre partecipare, anche senza invito, il DPO ed i componenti della Direzione Strategica dell'ASST dei Sette Laghi.

Le riunioni sono coordinate dal Coordinatore. Il Segretario provvede alla convocazione. Le riunioni possono svolgersi sia presso la sede dell'ASST o anche altrove e/o anche mediante la partecipazione a distanza dei componenti e degli invitati, con sistemi audio e/o video collegati, a condizione che sia accertata l'identità degli intervenuti.

Ciascun componente ha diritto di fare iscrivere a verbale le proprie osservazioni in merito all'oggetto della discussione e i motivi del suo eventuale dissenso.

L'esecuzione delle determinazioni approvate dal Comitato è curata di norma dal Referente; tuttavia il Comitato può, in caso di specifiche necessità, delegare anche ad altro componente determinate attività, con obbligo di relazionare durante la successiva riunione.

Il Segretario del Comitato:

- cura le convocazioni trasmettendo l' Ordine del Giorno;
- cura le convocazioni alle riunioni del Comitato di eventuali invitati di volta in volta di interesse, secondo le determinazioni dello stesso Comitato e/o del Coordinatore e/o su richiesta del Titolare e/o del DPO;
- redige apposito verbale, sequenzialmente numerato, di ogni riunione;
- collabora con il Referente nell'esecuzione delle determinazioni assunte dal Comitato e nel monitoraggio dello stato di avanzamento dei lavori;
- cura l'archiviazione dei verbali delle riunioni del Comitato.

Il DPO ed il soggetto aggiudicatario di cui al successivo punto 15 possono partecipare da remoto o in presenza, al bisogno, anche ad ulteriori riunioni di tipo operativo con uno o più componenti del Comitato. Per tali riunioni di tipo operativo non è richiesta la partecipazione della maggioranza dei componenti del Comitato stesso e, di norma, non richiedono la redazione di specifico verbale.

14. ESCLUSIONI (Studi clinici/progetti di ricerca)

Esula dall'ambito di competenza del Comitato Privacy l'approvazione tecnica o l'espressione di pareri preliminari in materie specificamente attribuite dalla normativa vigente o da eventuali determinazioni aziendali ad altri soggetti (ad esempio studi clinici o progetti di ricerca comunque denominati soggetti al parere del Comitato Etico Interaziendale dell'Insubria).

Rimane ferma ed impregiudicata la disponibilità del Comitato su richiesta di soggetti del Modello organizzativo aziendale a favorire, anche tramite l'ufficio operativo, il raccordo collaborativo con il Responsabile della Protezione dei Dati (DPO) dell'ASST dei sette Laghi nel rispetto delle sfere di competenza di ciascuno.

15. ADEGUAMENTO CONTINUO AL GDPR n. 679/2016.

Alla luce della scelta strategica dell'Azienda di esternalizzare servizi di consulenza finalizzati a garantire l'adeguamernto continuo dell'Azienda Socio Sanitaria Territoriale dei Sette Laghi al Regolamento Europeo sulla protezione dei dati personali 679/2016 il Comitato Privacy, tenendo conto delle attività esternalizzate, esercita le proprie funzioni interagendo anche con il soggetto aggiudicatario dei servizi predetti.

16. COMITATO PRIVACY E CODICI DI COMPORTAMENTO - CERTIFICAZIONI DI QUALITÀ

Il Titolare può chiedere il parere del Comitato in ordine ad eventuali proposte di adesione dell'Azienda a Codici di condotta o a meccanismi di certificazione, ai sensi e per gli effetti di cui, rispettivamente, agli articoli 42 e 44 del Regolamento europeo n., 679/2016. Il Comitato si esprime unitamente il DPO e l'aggiudicatario dei servizi di consulenza dopo aver acquisto i pareri interni delle strutture maggiormente coinvolte (ad esempio S.C. Sistemi Informativi Aziendali, Direzioni Mediche, S.C. QAARC, RSPP, etc .etc.)

17. CONFIDENZIALITÀ E RISERVATEZZA

Il Comitato non ha rilevanza esterna ed i suoi componenti sono tenuti al segreto in ordine alle notizie ed informazioni acquisite nell'esercizio della funzione.

Il Comitato non comunica a terzi nessuna informazione acquisita nell'ambito della propria attività, salvo che tale obbligo o facoltà sia prevista dal Modello Organizzativo ("Data Protection") o sia richiesto dalla legge.

Il Comitato si astiene dal ricercare ed utilizzare informazioni riservate per ragioni personali o per scopi non conformi o estranei alle funzioni proprie.

18. RINVIO

Le disposizioni adottate con il presente atto si applicano nel rispetto della normativa e della regolamentazione, nazionale o regionale, in vigore tempo per tempo e compatibilmente con la stessa. Per tutto quanto non previsto dal presente regolamento si rinvia alla normativa vigente ed ai provvedimenti del Garante per la protezione dei dati personali.