MODELLO ORGANIZZATIVO PRIVACY

Data: giovedì 2 maggio 2024
Versione: 1.0

Società della Salute Amiata Senese e Val d'Orcia Valdichiana Senese
Piazza Grande, 1 - 53045 Montepulciano (SI) - Italia

Sommario

1. OBIETTIVI E DEFINIZIONI 3
2. AMBITO DI APPLICAZIONE 4
3. SICUREZZA DELLE INFORMAZIONI 5
4. RISERVATEZZA DELLE INFORMAZIONI 7
5. ATTUAZIONE DELLA POLICY 7
6. MONITORAGGIO DEL SISTEMA GESTIONE PRIVACY 8
7. INFORMAZIONE E FORMAZIONE 8
8. IMPEGNO DEGLI ORGANI DI GOVERNO 9
9. ORGANIGRAMMA, SISTEMA DI NOMINE E RESPONSABILITA' 10
9.1. Titolare del Trattamento 10
9.2. Responsabile del Trattamento 11
9.3. Referente esecutivo per la protezione dei dati personali o Data Protection Manager (DPM) 12
9.4. Referenti privacy 13
9.5. Persone autorizzate al trattamento 14
9.6. Amministratore di Sistema 15
10. MISURE DI SICUREZZA GENERALI 16
10.1. La gestione della sicurezza: ruoli e responsabilità 16
10.2. Misure per garantire la protezione dei dati 16
10.3. Scrivania sgombra e schermo inattivo (clean desk & clear screen Policy) 17
10.4. Livelli di sicurezza 17

1. OBIETTIVI E DEFINIZIONI

Società della Salute Amiata Senese e Val d'Orcia Valdichiana Senese (di seguito anche denominata "società") intende dotarsi di linee guida che consentano di affrontare in maniera organica gli obblighi normativi in materia di protezione dei dati personali, così da conseguire i migliori risultati nel proteggere le informazioni e i dati gestiti nell'ambito delle proprie attività da tutte le minacce interne o esterne, intenzionali o accidentali, secondo le disposizioni previste dalla normativa comunitaria e nazionale.

Obiettivo del presente documento e di quelli ad esso collegati è definire il **Modello Organizzativo Privacy** (Policy Privacy), ovvero individuare strategia, linee guida generali e disposizioni operative interne volte a disciplinare il trattamento dei dati personali effettuato dalla società, ai sensi del D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" (Codice della Privacy), come modificato dal D.Lgs. 10 agosto 2018, n. 101 e del Regolamento (UE) del Parlamento Europeo e del Consiglio del 27 aprile 2016, n. 679 (GDPR – General Data Protection Regulation), nonché ulteriori provvedimenti in materia di fonte normativa secondaria in vigore al momento dell'approvazione della seguente policy. In essa sono quindi disciplinati i ruoli e le responsabilità nonché gli adempimenti da seguire in materia di protezione dei Dati Personali ai sensi del "Codice della Privacy" e del "GDPR", anche con riferimento alle decisioni e ai provvedimenti emessi dal Garante Europeo della Protezione dei Dati (GEPD) e dall'Autorità Garante Nazionale per la protezione dei dati personali.

Ai fini del presente Modello Organizzativo Privacy si applicano le seguenti definizioni, coerenti con quanto previsto dalla normativa di settore:

- Regolamento: Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE (GDPR - Regolamento Generale sulla Protezione dei Dati);
- Normativa: D.Lgs. 2003/196 (come modificato dal D.Lgs. 2018/101) e Regolamento (UE) 2016/679, nonché ulteriori provvedimenti in materia di fonte normativa secondaria in vigore al momento dell'approvazione del presente Modello Organizzativo Privacy.
- Codice Privacy: Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" come modificato dal Decreto Legislativo 10 agosto 2018, n. 101;
- Società: Società della Salute Amiata Senese e Val d'Orcia Valdichiana Senese
- Affiliate: società controllate da o collegate con Società della Salute Amiata Senese e Val d'Orcia Valdichiana Senese stabilite nel territorio dello Stato italiano o in un luogo comunque soggetto alla sovranità dello Stato italiano;
- Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- Dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

- Dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- Interessato: la persona fisica cui si riferiscono i dati personali;
- Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
- Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- Referente esecutivo per la protezione dei dati personali (DPM - Data Protection Manager): la persona fisica preposta alla sorveglianza sull'applicazione e il rispetto delle disposizioni in materia di trattamento di dati impartite dal Titolare del trattamento e, per quanto di sua competenza se nominato da quest'ultimo, dal DPO;
- Referente privacy: le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile con compiti di coordinamento di più persone autorizzate (definite anche soggetti designati);
- Autorizzato: le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare del trattamento o dal Responsabile del trattamento (definite anche soggetti designati);
- Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare del trattamento o del responsabile del trattamento;
- Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- Trattamento transfrontaliero: a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente inciderebbe in modo sostanziale sugli interessati in più di uno Stato membro.
- Paesi terzi: paesi non appartenenti all'UE o allo spazio Economico Europeo (Norvegia, Islanda, Liechtenstein);

2. AMBITO DI APPLICAZIONE

La **politica della privacy (policy)** che discende dal presente Modello Organizzativo Privacy si applica all'azienda nella sua interezza, a tutti gli organi e alle strutture di qualsiasi livello organizzativo o funzionale.

La sua attuazione è obbligatoria per tutto il personale e deve essere inserita come parte integrante nella regolamentazione di qualsiasi accordo con tutti i soggetti esterni coinvolti con il trattamento di informazioni che rientrano nel campo del **Sistema di Gestione della Privacy (SGP)**.

La società consente la comunicazione e la diffusione delle informazioni di tipo procedurale e organizzativo verso l'esterno esclusivamente per il corretto svolgimento delle attività aziendali che avvengono nel rispetto delle regole e delle norme vigenti.

La presente policy è di applicazione immediata per la società e dovrà essere recepita dalle sue componenti tempestivamente e comunque non oltre 30 giorni dalla sua emissione, tramite le opportune deliberazioni degli organi di controllo preposti o gli altri atti necessari.

La società si impegna a garantire e dimostrare che il trattamento dei dati personali avviene in maniera conforme a quanto previsto dalla normativa e, secondo i seguenti principi di liceità, questi sono:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- esatti e, se necessario, aggiornati; a tal proposito sono state adottate misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- 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;
- 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.

Le presenti indicazioni sono valide, oltre che per i trattamenti dei dati personali di cui la società è Titolare, anche per tutti quei trattamenti di cui la società è nominata Responsabile del trattamento da altri Titolari del trattamento, salvo la presenza di misure più restrittive in materia di protezione dei dati personali contenute nei documenti che regolano i rapporti con il Titolare del trattamento.

Poiché analoghe garanzie di protezione e l'adozione di adeguate misure di sicurezza sono richieste ai soggetti terzi ai quali la società affida l'incarico di Responsabile del trattamento, la policy in oggetto è resa disponibile presso tali Responsabili del trattamento.

3. SICUREZZA DELLE INFORMAZIONI

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni trattate nell'espletamento delle procedure aziendali, rispetto alle quali la società assicura l'integrità e la protezione e consente l'accesso esclusivamente ai ruoli e alle funzioni necessarie e preventivamente autorizzate.

La mancanza di adeguati livelli di sicurezza può infatti comportare il danneggiamento dell'immagine aziendale, la mancata soddisfazione della clientela, il rischio di incorrere in sanzioni legate alla violazione delle leggi vigenti nonché altri danni di natura economica e finanziaria.

Per conseguire sempre l'allineamento normativo e aumentare la capacità di controllo, la società ha istituito e mantiene aggiornato un registro delle attività di trattamento.

La società identifica, quando ritenuto necessario a seguito delle risultanze dell'analisi dei rischi connessi al trattamento dei dati personali, le ulteriori esigenze di sicurezza tramite la valutazione di impatto sulla protezione

dei dati che consente di acquisire un livello aggiuntivo di consapevolezza sul livello di esposizione alle minacce dei propri sistemi di gestione dei dati.

La valutazione del rischio, eseguita su tutti i trattamenti in essere o previsti, permette di valutare le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione delle misure di sicurezza al sistema informativo e in generale all'intera organizzazione oltre a indicare quale sia la probabilità che le minacce identificate trovino reale materializzazione. I risultati di questa valutazione determinano le azioni necessarie per individuare le corrette e adeguate misure di sicurezza e i meccanismi per garantire la protezione dei dati personali.

La gestione della sicurezza delle informazioni è fondata su alcuni imprescindibili principi generali, di seguito enunciati:

- Esiste un catalogo costantemente aggiornato degli asset aziendali rilevanti ai fini della gestione delle informazioni e per ciascuno di essi è individuato un responsabile;
- Le informazioni sono classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza, integrità e disponibilità coerenti e appropriati;
- Gli accessi ai sistemi informativi sono sottoposti a una procedura di identificazione e autenticazione. Inoltre, le autorizzazioni di accesso alle informazioni sono differenziate in base al ruolo e agli incarichi ricoperti dai singoli individui, in modo che ogni utente possa accedere alle sole informazioni di cui necessita, e tali autorizzazioni sono periodicamente sottoposte a revisione (come previsto dal Regolamento Informatico);
- Sono definite le procedure per l'utilizzo sicuro dei beni (luoghi, mezzi di trasporto, strumenti) e delle informazioni aziendali;
- È incoraggiata la piena consapevolezza da parte del personale delle problematiche relative alla sicurezza delle informazioni;
- Per poter prevenire o almeno gestire in modo tempestivo gli incidenti, tutti sono chiamati a rendersi partecipi del sistema di sicurezza aziendale e pertanto devono notificare qualsiasi problema relativo alla sicurezza di cui sono a conoscenza;
- È necessario prevenire l'accesso non autorizzato ai locali e alle apparecchiature dove sono gestite le informazioni;
- È assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti;
- È predisposto un piano di continuità che permette all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale. Gli aspetti di sicurezza sono inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici;
- Sono garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

4. RISERVATEZZA DELLE INFORMAZIONI

La società si impegna a garantire la riservatezza e la confidenzialità delle informazioni e dei dati degli interessati acquisiti nel corso della propria attività in conformità alle procedure interne previste, coerenti con il presente Modello Organizzativo Privacy.

Il trattamento dei dati può essere effettuato attraverso strumenti manuali, informatici e telematici atti a memorizzare, elaborare, gestire e trasmettere i dati stessi nel rispetto delle misure di sicurezza previste. Tutti i soggetti in qualsiasi modo coinvolti nel trattamento dei dati personali, indipendentemente dal rispetto degli obblighi derivanti dal codice deontologico relativo alla professione regolamentata eventualmente esercitata nell'espletamento delle proprie mansioni, sono tenuti al segreto previsto dall'art. 2407 del codice civile.

La società si impegna a garantire adeguati livelli minimi di sicurezza delle informazioni rese disponibili da terzi con la medesima diligenza e livello di protezione utilizzati per la sicurezza e la riservatezza dei propri dati.

5. ATTUAZIONE DELLA POLICY

L'osservanza e l'attuazione della politica della privacy (policy) che discende dal presente Modello Organizzativo Privacy sono responsabilità di:

- tutto il personale che, a qualsiasi titolo, collabora con l'azienda ed è in qualche modo coinvolto con il trattamento di dati e informazioni che rientrano nel campo di applicazione del Sistema di Gestione della Privacy (SGP). Il personale è infatti responsabile, ciascuno per quanto di propria competenza, della segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza;
- tutti i soggetti esterni che intrattengono rapporti e collaborano con l'azienda e che devono garantire il rispetto dei requisiti contenuti nella politica della privacy (policy);
- il soggetto nominato Referente esecutivo per la protezione dei dati personali (DPM - Data Protection Manager) quale responsabile del Sistema di Gestione della Privacy (SGP). Questi, in collaborazione diretta con il Titolare del trattamento, deve:
  - condurre l'analisi dei rischi con le opportune metodologie e adottare le misure per la gestione del rischio;
  - stabilire le norme di comportamento necessarie alla conduzione sicura delle attività aziendali;
  - verificare le violazioni alla sicurezza, adottare le contromisure necessarie e controllare l'esposizione dell'azienda alle principali minacce e rischi;
  - organizzare la formazione e promuovere la consapevolezza del personale per tutto ciò che concerne la qualità, la sicurezza e la sicurezza delle informazioni;
  - verificare periodicamente l'efficacia e l'efficienza del Sistema di Gestione della Privacy (SGP).

Il personale dell'azienda che, in modo intenzionale o riconducibile a negligenza, disattenda le regole di sicurezza stabilite e in tal modo provochi un danno, potrà essere perseguito nelle opportune sedi, nel pieno rispetto dei vincoli di legge e contrattuali.

6. MONITORAGGIO DEL SISTEMA GESTIONE PRIVACY

La direzione aziendale verifica almeno una volta all'anno l'efficacia e l'efficienza del Sistema di Gestione della Privacy (SGP), in modo di assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e di favorire l'attivazione di un processo di aggiornamento continuo.

Il Referente esecutivo per la protezione dei dati personali (DPM - Data Protection Manager), quale responsabile del Sistema di Gestione della Privacy (SGP), ha il compito di condurre operativamente la revisione di questa politica. Questi dovrà utilizzare opportuna modulistica, predisposta in modo da garantire omogeneità del confronto e facilitare il controllo dei risultati nel corso del tempo. I risultati della revisione periodica sono da sottoporre ai livelli decisionali superiori per le opportune deliberazioni.

La revisione deve verificare lo stato delle azioni preventive e correttive e l'aderenza alla politica privacy delle procedure in atto così come di quelle previste e non ancora applicate.

Deve inoltre tenere conto di tutti i cambiamenti che possono influenzare l'approccio alla gestione della sicurezza delle informazioni, includendo i cambiamenti organizzativi, l'ambiente tecnico, la disponibilità di risorse, le condizioni legali, regolamentari o contrattuali e dei risultati dei precedenti riesami.

Il risultato dell'intero processo di revisione periodica include tutte le decisioni prese e le azioni adottate in merito al miglioramento del Sistema di Gestione della Privacy (SGP).

7. INFORMAZIONE E FORMAZIONE

L'obiettivo di garantire un corretto trattamento dei dati, conforme ai requisiti previsti dalla normativa[1], viene raggiunto dalla società anche e soprattutto grazie alla particolare attenzione risposta nei confronti della formazione del proprio personale.

A tale scopo il Modello Organizzativo Privacy è divulgato presso il personale già in servizio e, nel caso di nuove risorse umane inserite in organico, fin dal momento del loro ingresso nella compagine della società. Per gli stessi fini di conoscenza eventuali aggiornamenti sono diffusi con gli strumenti ritenuti di volta in volta più efficaci.

Allo scopo creare un ecosistema favorevole nell'ambiente di lavoro e formare con particolare cura i soggetti che per il ruolo ricoperto risultano inseriti nel Sistema di Gestione della Privacy (SGP), la società:

- adotta un piano formativo con l'obiettivo di alfabetizzazione iniziale in materia di protezione dei dati personali, destinato a tutto il personale della società;
- prevede l'erogazione di moduli specifici all'interno dei corsi di formazione per il ruolo ricoperto, sia in quelli organizzati all'immissione in servizio che al momento del cambio di mansione qualora sia di livello superiore o per ambito applicativo diverso;
- prevede un piano di formazione programmato con cadenza annuale sulla formazione erogata in ambito privacy a tutti i dipendenti della società;

1 Art. 29 Regolamento –"Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento" Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Art. 2 quaterdecies Codice Privacy – "Attribuzione di funzioni e compiti a soggetti designati" Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.

- conserva la documentazione distribuita e la modulistica attestante la partecipazione alle attività formative.

La formazione delle persone autorizzate al trattamento e, ove ritenuto necessario, delle altre figure chiave nel Sistema di Gestione della Privacy (SGP), riguarda in particolare:

- gli aspetti generali della disciplina di protezione dei dati personali;
- le minacce, le vulnerabilità, la probabilità di accadimento e di conseguenza i rischi che minacciano i dati trattati;
- le conseguenze derivanti dalla violazione dei dati personali (Data Breach);
- le procedure da seguire in caso di violazione dei dati personali;
- le misure di prevenzione per evitare o almeno ridurre la probabilità di accadimento delle violazioni e le misure di mitigazione del danno in caso si verifichino;
- gli aspetti specifici della normativa in materia di protezione dei dati personali nel settore di azione della società (con particolare attenzione per gli ambiti sanitario, TELCO, bancario, ecc.);
- l'addestramento specifico per aggiornare il personale sulle misure di sicurezza e protezione dei dati personali ritenute adeguate e adottate dal Titolare del trattamento.

La formazione deve essere:

- adeguata al proprio sistema di trattamento dei dati personali;
- efficace nella trasmissione delle informazioni in materia di protezione dei dati personali;
- efficiente nel fornire strumenti per l'esecuzione delle procedure previste dal Sistema di Gestione della Privacy (SGP);
- documentabile, in quanto la formazione è parte integrante della policy della società e l'articolazione e gli esiti di tale attività devono essere sempre disponibili.

8. IMPEGNO DEGLI ORGANI DI GOVERNO

La direzione della società sostiene attivamente le attività inerenti la gestione della privacy, o protezione dei dati personali, tramite indirizzi precisi, impegno evidente, incarichi espliciti e riconoscimento delle responsabilità specifiche relative alla sicurezza delle informazioni.

L'impegno della direzione si attua tramite un'adeguata struttura i cui compiti sono:

- garantire che siano identificati tutti gli obiettivi relativi alla sicurezza delle informazioni e che questi siano coerenti con la realtà della struttura a cui si riferiscono;
- stabilire i ruoli e relative responsabilità per lo sviluppo e il mantenimento del Sistema di Gestione della Privacy (SGP);
- fornire risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del Sistema di Gestione della Privacy (SGP);
- controllare che il Sistema di Gestione della Privacy (SGP) sia integrato in tutti i processi aziendali e che le conseguenti procedure e controlli siano sviluppati efficacemente;

- approvare e sostenere tutte le iniziative volte al miglioramento della sicurezza delle informazioni;
- attivare programmi per la diffusione della consapevolezza e della cultura della sicurezza delle informazioni.

La società riconosce la propria responsabilità che discende dalla normativa vigente e si impegna a proteggere i dati personali che gli utenti affidano ad essa da perdita, uso improprio o accesso non autorizzato. Per la protezione dei dati personali degli utenti, l'azienda si avvale di tecnologie e procedure aziendali di protezione secondo le migliori pratiche (best practices) di volta in volta disponibili.

9. ORGANIGRAMMA, SISTEMA DI NOMINE E RESPONSABILITA'

Al fine di garantire la tutela dei diritti delle persone fisiche relativamente al trattamento dei dati personali, la società garantisce sempre la precisa individuazione dei soggetti che ricoprono ruoli attivi nel trattamento. Ciò avviene con l'allestimento e il mantenimento efficiente nel tempo di un sistema tracciabile delle nomine e delle relative mansioni.

In questo modo risulta di immediata comprensione la conseguente ripartizione delle responsabilità di ogni soggetto, parametrate alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento, nonché ai rischi per i diritti e le libertà delle persone fisiche valutati ogni volta che sia ritenuto necessario.

Quanto descritto trova riscontro nell'organigramma privacy che viene aggiornato a cadenza periodica ritenuta più opportuna in relazione al settore di attività e all'articolazione della propria organizzazione oppure in occasione di qualsiasi variazione intervenuta.

In accordo con la normativa di riferimento e con la policy che discende dal presente Modello Organizzativo Privacy, costituiscono figure imprescindibili quelle di seguito descritte.

9.1. Titolare del Trattamento

Conformemente a quanto previsto dalla normativa la società è Titolare del trattamento e in tale ruolo si impegna a:

- adeguare il proprio assetto organizzativo per rendere il governo della privacy allineato ai dettami normativi;
- adottare le modalità operative necessarie alla corretta gestione degli adempimenti ai fini della protezione dei dati personali trattati;
- assumere le decisioni in ordine alle finalità, alle modalità del trattamento dei dati e agli strumenti utilizzati, ivi compreso il profilo della sicurezza, sia per i trattamenti svolti all'interno che all'esterno della propria organizzazione;
- individuare e designare i Responsabili del trattamento dei dati, impartendo loro le relative direttive e, se necessario, istruzioni specifiche;
- vigilare sulla puntuale osservanza delle disposizioni e istruzioni impartite a tutti i soggetti che hanno un ruolo attivo nel trattamento dei dati personali;
- garantire sempre il pieno controllo sulla piramide organizzativa di cui è al vertice, concedendo autorizzazioni generali o specifiche ai responsabili del trattamento secondo criteri di opportunità nelle diverse situazioni ed esprimendo o negando il gradimento nei confronti di sub-responsabili eventualmente proposti dai responsabili assumendo così un ruolo di effettivo controllo e indirizzo.

Inoltre, si impegna a garantire l'esercizio dei diritti degli interessati e a tal scopo individua e mette in pratica apposite procedure al fine di informare gli interessati e garantire a ciascuno di essi almeno il:

- diritto di accesso, cioè di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano e di averne accesso. In particolare l'interessato ha diritto di conoscere l'origine dei dati personali; le finalità e modalità del trattamento; la logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; gli estremi identificativi del titolare, dei responsabili e degli eventuali rappresentanti designati; l'elenco dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza a qualsiasi titolo in linea con la normativa e quello delle persone autorizzate al trattamento;
- diritto di rettifica, cioè di ottenere l'aggiornamento, la correzione ovvero, quando vi ha interesse, l'integrazione dei dati;
- diritto alla cancellazione (o diritto all'oblio), cioè di ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- diritto di opposizione, cioè di limitare od opporsi, per motivi legittimi, al trattamento, seguendo le modalità descritte dalle norme vigenti.

Al fine di esercitare i diritti sopra descritti, la società si impegna a rispondere senza ritardo alle richieste presentate da parte dell'interessato direttamente ad esso, ai Responsabili o ai soggetti autorizzati appositamente nominati, nelle forme e modalità nonché attraverso i mezzi ritenuti più idonei.

9.2. Responsabile del Trattamento

Il Responsabile del trattamento dei dati è il soggetto, persona fisica o giuridica, nominato dal Titolare al fine di garantire nelle operazioni di trattamento l'attuazione delle misure di sicurezza previste dalla normativa e dal presente Modello Organizzativo Privacy.

Il soggetto preposto allo svolgimento della funzione viene individuato tra quelli in possesso dei necessari requisiti e con adeguate garanzie. Tra le sue funzioni sono comprese quelle di:

- osservare le procedure in materia di protezione dei dati personali adottate dal Titolare;
- organizzare, gestire e supervisionare tutte le operazioni di trattamento dei dati personali affinché esse vengano effettuate nel rispetto delle disposizioni di legge e predisporre tutti i documenti nonché le misure tecniche organizzative richiesti dal Codice e dal Regolamento;
- adottare e verificare il rispetto delle misure di sicurezza indicate dal Codice e dal Regolamento e la conformità nel tempo dei sistemi e delle misure di sicurezza;
- redigere e aggiornare il registro delle attività di trattamento, qualora sia necessario;
- informare il Titolare del trattamento di tutte le misure adottate e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato al compito specifico;
- nominare le persone autorizzate che svolgono tali funzioni per suo conto, conservando i relativi estremi identificativi, definendo gli ambiti di operatività consentiti e verificando almeno annualmente il relativo operato per controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti il trattamento dei dati personali;

- nominare le persone autorizzate al trattamento dei dati nelle altre funzioni ritenute necessarie conferendo loro apposite istruzioni sulle norme e le procedure da osservare e provvedendo alla relativa formazione;
- controllare le operazioni di trattamento svolte dalle persone autorizzate sottoposte alla propria responsabilità e la conformità all'ambito di trattamento consentito;
- redigere e aggiornare la lista dei nominativi delle persone autorizzate sottoposte alla propria responsabilità e verificarne almeno annualmente l'ambito di trattamento consentito;
- proporre al Titolare del trattamento dei dati la nomina di soggetti per il ruolo di sub-Responsabile del trattamento dei dati in relazione all'affidamento agli stessi di determinate attività;
- attuare gli obblighi di informazione ed acquisizione del consenso, quando richiesto, nei confronti degli interessati;
- garantire all'interessato che ne faccia richiesta l'effettivo esercizio dei diritti previsti dalla normativa di settore inoltrando al Titolare del trattamento le richieste pervenute nel caso non possano essere evase autonomamente;
- distruggere i dati personali alla fine del trattamento nei casi previsti dal Regolamento, secondo le procedure atte a garantire la sicurezza degli stessi e provvedere alle formalità di legge e agli adempimenti necessari;
- comunicare immediatamente al titolare non oltre le 24 ore successive al loro ricevimento, ogni richiesta, ordine o attività di controllo da parte del Garante o dell'Autorità Giudiziaria;
- osservare le procedure in materia di protezione dei dati personali adottate dal Titolare del trattamento;

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il Titolare del trattamento può modificare la propria struttura per conseguire i migliori risultati di protezione variando opportunamente l'articolazione del proprio Sistema di Gestione Privacy (SGP).

9.3. Referente esecutivo per la protezione dei dati personali o Data Protection Manager (DPM)

Alla luce dell'analisi dei rischi aziendali in materia di trattamento dei dati personali, il Titolare ha ritenuto opportuno procedere alla nomina del **Referente esecutivo per la protezione dei dati personali o Data Protection Manager (DPM)**. A tal riguardo si precisa che le attività di trattamento di dati personali a monitoraggio regolare e sistematico non costituiscono l'attività principale della società.

I compiti affidati al Referente esecutivo per la protezione dei dati personali (Data Protection Manager – DPM), quale responsabile del Sistema di Gestione della Privacy (SGP), con espresso atto di designazione sono i seguenti:

- sorvegliare le politiche del Titolare del trattamento e del Responsabile della Protezione dei Dati (Data Protection Officer – DPO) circa l'osservanza della normativa in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale con ruoli attivi nel trattamento;
- vigilare sull'effettivo funzionamento delle prescrizioni adottate dalla società in materia di protezione dei dati personali;
- effettuare valutazioni indipendenti (audit) in materia di protezione dei dati personali e controllare l'applicazione dei principi fondamentali di privacy by design e privacy by default;

- informare e fornire consulenza al Titolare del trattamento nonché ai soggetti che eseguono il trattamento in merito agli obblighi derivanti dalla normativa di settore;
- promuovere la cultura della protezione dei dati all'interno della società e contribuire all'attuazione degli elementi essenziali del Regolamento (UE) 2016/679, ad esempio circa principi fondamentali del trattamento, diritti degli interessati, concetti di privacy by design e privacy by default, registro delle attività di trattamento, sicurezza dei trattamenti e violazioni dei dati personali (data breach);
- conservare e aggiornare l'elenco dei Referenti e delle persone autorizzate al trattamento dei dati personali;
- ricevere e dare esecuzione alle istruzioni e alle prescrizioni impartite dal Responsabile della Protezione dei Dati (DPO) per la conformità della società al Regolamento (UE) 2016/679;
- riportare direttamente al Responsabile della Protezione dei Dati (DPO) le decisioni adottate dal Titolare in contrasto con la normativa specifica in materia di protezione dei dati personali o in dissenso alle indicazioni ricevute dal Responsabile della Protezione dei Dati (DPO);
- predisporre e attuare adeguati flussi di comunicazione da e verso il Responsabile della Protezione dei Dati (DPO), ivi inclusi gli allarmi (alert) e le violazioni (data breach) di sistema;
- fornire al Responsabile della Protezione dei Dati (DPO) accesso alle informazioni necessarie per lo svolgimento dei compiti a quest'ultimo attribuiti;
- fungere da punto di contatto tra i Referenti privacy o le persone autorizzate al trattamento dei dati personali e il Responsabile della Protezione dei Dati (DPO);
- fungere da punto di contatto per l'interessato relativamente a tutte le questioni inerenti il trattamento dei propri dati personali e all'esercizio dei relativi diritti;
- redigere una relazione annuale sulle proprie attività da sottoporre al Responsabile della Protezione dei Dati (DPO);
- gestire operativamente il Registro dei trattamenti del Titolare del trattamento;
- supportare il Responsabile della Protezione dei Dati (DPO) nella stima di impatto sulla protezione dei dati personali (Data Protection Impact Assessment – DPIA), fornendo pareri specifici e sorvegliarne il corretto svolgimento;
- coinvolgere il Responsabile della Protezione dei Dati (DPO) in questioni di particolare complessità o in caso di trattamenti dei dati personali che presentino caratteri del monitoraggio regolare e sistematico su larga scala;
- cooperare con l'autorità di controllo e fungere da punto di contatto per questioni connesse al trattamento, tra cui la consultazione preventiva;
- informare tempestivamente il Responsabile della Protezione dei Dati (DPO) in caso di violazione dei dati personali (data breach) e fornire aggiornamenti fino alla risoluzione dell'incidente;
- garantire riservatezza in merito all'adempimento dei propri compiti, in conformità con il diritto previsto dall'UE e dagli Stati Membri.

9.4. Referenti privacy

Il Titolare del trattamento provvede a nominare, presso le Unità Organizzative in cui vengono svolti i trattamenti, le persone autorizzate con compiti di Referenti privacy.

I compiti del Referente privacy, autorizzato con apposito atto, sono di seguito sintetizzati:

- individuare le persone da autorizzare al trattamento dei dati e promuoverne l'autorizzazione per area di competenza;
- segnalare al Referente esecutivo per la protezione dei dati personali (Data Protection Manager – DPM) eventuali casi di violazioni dei dati personali, segnalati da parte delle risorse umane ad esso sottoposte o autonomamente individuati;
- segnalare al Referente esecutivo per la protezione dei dati personali (Data Protection Manager – DPM) eventuali richieste ricevute da parte dell'interessato sull'esercizio dei relativi diritti, nonché attenersi alla procedura interna sull'esercizio di tali diritti;
- cooperare in caso di attività di controllo nell'ambito della protezione dei dati personali da parte di strutture interne o esterne, fornendo eventuale documentazione richiesta e garantendo l'accesso ai locali;
- informare il Referente esecutivo per la protezione dei dati personali (Data Protection Manager – DPM) dell'esistenza di ogni nuova proposta che impatta sulla protezione dei dati, in applicazione del principio di privacy by design e by default;
- informare il Referente esecutivo per la protezione dei dati personali (Data Protection Manager – DPM) dell'esistenza di ogni nuovo trattamento per cui risulta necessario aggiornare il registro delle attività di trattamento o modificarlo, in applicazione del principio di privacy by design e by default;
- informare il Referente esecutivo per la protezione dei dati personali (Data Protection Manager – DPM) della presenza di ogni nuova risorsa umana che tratta dati personali al fine di valutare la necessità di formazione in ambito privacy;
- controllare che le persone autorizzate al trattamento rispettino le indicazioni impartite dalla società;
- segnalare casi di mancato rispetto delle disposizioni in tema di protezione dei dati al Referente esecutivo per la protezione dei dati personali (Data Protection Manager – DPM).

9.5. Persone autorizzate al trattamento

Il Titolare del trattamento (o il Responsabile del Trattamento) nomina, presso le Unità Organizzative in cui vengono svolti i trattamenti, le persone autorizzate al trattamento dei dati (o soggetti designati).

La persona autorizzata effettua tutte le operazioni di trattamento dei dati personali attinenti l'attività lavorativa di competenza dell'area di appartenenza e opera sotto l'autorità del Titolare del Trattamento (o del Responsabile del Trattamento), attenendosi alle istruzioni dallo stesso impartite nonché alle specifiche procedure che regolamentano le modalità di utilizzo delle banche dati cui la persona autorizzata abbia accesso.

In particolare, i compiti a essa attribuiti sono così sintetizzati:

- segnalare al Referente privacy da cui dipende, o al Referente esecutivo per la protezione dei dati personali (Data Protection Manager – DPM) nel caso di dipendenza diretta, eventuali richieste ricevute da parte dell'interessato sull'esercizio dei relativi diritti, nonché attenersi alla procedura interna sull'esercizio di tali diritti;
- avvisare il Referente privacy da cui dipende, o il Referente esecutivo per la protezione dei dati personali (Data Protection Manager – DPM) nel caso di dipendenza diretta, se nello svolgimento di un'attività dovesse riscontrare il trattamento di nuovi dati o finalità per cui risultasse necessario aggiornare il registro dei

trattamenti ed eseguire almeno un'analisi dei rischi, in applicazione dei principi di privacy by design e privacy by default;

- informare immediatamente il Referente privacy da cui dipende, o il Referente esecutivo per la protezione dei dati personali (Data Protection Manager – DPM) nel caso di dipendenza diretta, qualora le istruzioni ricevute risultino non conformi alla normativa sulla protezione dai dati;
- segnalare al Referente privacy da cui dipende, o il Referente esecutivo per la protezione dei dati personali (Data Protection Manager – DPM) nel caso di dipendenza diretta, eventuali accessi non autorizzati;
- rilasciare all'interessato l'informativa e acquisire il consenso laddove necessario, secondo le istruzioni impartite dal Titolare del trattamento (o dal Responsabile del trattamento).

9.6. Amministratore di Sistema

La figura professionale che, in ambito informatico, mantiene, configura e gestisce un sistema di elaborazione dati o sue componenti, ivi inclusi sistemi software complessi (system administrator), ovvero una base dati (database administrator), ovvero reti e apparati di telecomunicazione di sicurezza (network administrator) è nominata persona autorizzata al trattamento dei dati personali con la qualifica specialistica di Amministratore di Sistema.

L'attribuzione delle funzioni di Amministratore di Sistema avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia, ivi compreso il profilo relativo alla sicurezza.

La nomina ad Amministratore di Sistema deve essere individuale, esplicitata in forma scritta, con l'indicazione analitica degli ambiti di applicazione di operatività consentiti in base al profilo di autorizzazione assegnato.

In generale, l'Amministratore di Sistema ha le seguenti responsabilità:

- sovraintendere alle risorse dei sistemi computerizzati al fine di consentirne una corretta ed efficiente utilizzazione;
- in accordo con il Referente esecutivo per la protezione dei dati personali (Data Protection Manager – DPM), fornire guida e supporto ai Referenti Privacy e ai soggetti autorizzati in merito al trattamento dei dati personali;
- amministrare e gestire la sicurezza informatica operando anche come gestore e custode delle password;
- nell'ambito delle responsabilità assegnate, effettuare periodici controlli e verifiche tecniche, in merito a quanto previsto dal Regolamento Informatico nel quadro del Sistema di Gestione della Privacy (SGP);
- individuare i soggetti a cui affidare l'incarico di manutentore del sistema stesso.

L'Amministratore di Sistema che provvede alla designazione dei soggetti incaricati alla manutenzione deve preventivamente informare il Titolare del Trattamento e deve formalizzare per iscritto l'attribuzione dell'incarico eventualmente specificando i limiti dell'intervento e le manutenzioni richieste. Per manutenzione s'intende non soltanto l'intervento tecnico diretto ad eliminare eventuali avarie hardware, ma anche gli interventi volti alla ricostruzione di archivi che dovessero in qualche modo risultare danneggiati o corrotti oltre all'intervento tecnico diretto ad eliminare eventuali avarie al software di sistema e all'applicativo utilizzato.

Per consentire all'Amministratore di Sistema di svolgere adeguatamente le proprie funzioni, allo stesso vengono concesse dal Titolare del trattamento le "Autorità di sistema", che consistono nell'assegnazione di

attributi, privilegi, o accessi che consentono la gestione delle "risorse critiche del sistema operativo", ovvero degli oggetti informatici necessari al funzionamento dei sistemi e del servizio di elaborazione dati.

L'elenco dei soggetti nominati Amministratori di Sistema è conservato adeguatamente e consegnato in copia per la custodia al Referente esecutivo per la protezione dei dati personali (Data Protection Manager – DPM).

10. MISURE DI SICUREZZA GENERALI

10.1. La gestione della sicurezza: ruoli e responsabilità

La responsabilità delle attività di impostazione e coordinamento dei sistemi che garantiscono la sicurezza e la tutela di tutti i dati oggetto di trattamento sono in carico ai relativi ruoli inseriti nell'organico della società. Tali sistemi possono essere sia logici che fisici e la responsabilità comprende la loro gestione diretta o tramite fornitori esterni.

In considerazione della complessità delle implicazioni relative alla sicurezza logica, nel quadro del Sistema di Gestione della Privacy (SGP) è redatto il Regolamento Informatico.

10.2. Misure per garantire la protezione dei dati

Le misure per garantire la protezione dei dati sono quelle misure di sicurezza volte a minimizzare i rischi che le informazioni siano rivelate o modificate senza autorizzazione, ovvero perse o alterate accidentalmente o intenzionalmente.

Queste comprendono un sistema di autenticazione per assicurare che la persona che accede al sistema nelle sue diverse articolazioni sia identificata con certezza, basato su codice identificativo e password individuale segreta, nonché un sistema di autorizzazione che prevede che a ciascuna persona che accede al sistema sia assegnato un profilo di accesso che definisce i dati ai quali l'utente è autorizzato ad accedere e, ove applicabile, le operazioni che per ciascun dato o gruppo di dati è autorizzato ad eseguire (consultazione, inserimento, modifica, cancellazione).

Ad eccezione degli Amministratori di Sistema definiti e nominati secondo le disposizioni del Modello Organizzativo Privacy, nessun dipendente della società è Amministratore di Sistema della propria macchina e tutti gli utenti che dispongono di una postazione informatica sono censiti.

Per ridurre i rischi di indisponibilità (parziale o totale) nell'accesso al sistema informatico della società sono previste una serie di attività, in particolare al momento dell'assunzione o della dimissione delle risorse umane con la procedura di allestimento o dismissione dell'utenza personale. Sempre al fine di controllo si procede a verificare con cadenza semestrale che la lista dei dipendenti cessati sia coerente con le utenze disabilitate.

Tutti i dispositivi della società concessi in dotazione ai dipendenti vengono formattati a seguito delle dimissioni degli stessi al fine di rimuovere tutti i dati personali contenuti al loro interno.

Tutti i dipendenti della società sono pertanto tenuti ad assicurarsi che venga correttamente eseguito il passaggio di consegne affinché venga assicurata la continuità dei servizi erogati e la conservazione dei documenti di lavoro.

10.3. Scrivania sgombra e schermo inattivo (clean desk & clear screen Policy)

La politica della scrivania sgombra (Clean Desk Policy) e dello schermo inattivo (Clear Screen Policy) è una delle migliori strategie da attuare per ridurre il rischio di violazioni della sicurezza della postazione di lavoro.

Lo scopo di tale politica è stabilire requisiti minimi per prevenire violazioni accidentali o dolose dei dati personali (Data Breach) e responsabilizzare i soggetti che nelle attività lavorative si trovano a loro contatto.

Di seguito sono elencati i comportamenti virtuosi da applicare:

- i dipendenti sono tenuti a garantire che tutte le informazioni sensibili o confidenziali in formato elettronico o cartaceo siano messe al sicuro nella propria postazione di lavoro, in particolare alla fine della giornata lavorativa e in caso di assenza prolungata;
- i computer devono essere bloccati quando le postazioni di lavoro non sono occupate;
- tutti i computer devono essere spenti alla fine della giornata lavorativa;
- qualsiasi informazione e/o dato particolare/sensibile deve essere rimosso dalla scrivania e chiuso a chiave in un cassetto quando la postazione di lavoro non è occupata e alla fine della giornata lavorativa;
- le cartelle contenenti informazioni riservate e/o sensibili e/o categorie particolari di dati personali devono essere tenute chiuse e bloccate quando non utilizzate;
- le chiavi utilizzate per accedere alle informazioni riservate e/o ai dati sensibili e/o alle categorie particolari di dati personali non devono essere lasciate su una scrivania non presidiata;
- i laptotp devono essere bloccati con un cavo di bloccaggio o conservati in un cassetto chiuso a chiave se non utilizzati;
- le password non possono essere lasciate su note adesive attaccate sopra, sotto o nei pressi di un computer, né possono essere lasciate per iscritto in posizione accessibile;
- le stampe contenenti informazioni riservate e/o dati particolari/sensibili devono essere immediatamente rimosse dalle stampanti;
- al momento dello smaltimento, i documenti riservati o contenenti informazioni riservate e/o sensibili e/o categorie particolari di dati personali devono essere distrutti e, ove presenti, triturati nei distruggidocumenti appositi;
- le lavagne contenenti informazioni riservate e/o sensibili e/o categorie particolari di dati personali devono essere pulite cancellando il contenuto scritto;
- i dispositivi portatili come laptop, smartphone o tablet non devono mai essere lasciati sbloccati e incustoditi;
- tutti i dispositivi di archiviazione di massa come CDROM, DVD o chiavi USB contenenti informazioni riservate e/o sensibili e/o categorie particolari di dati personali devono essere conservati in cassetti chiusi a chiave.

Il dipendente che viola queste norme di comportamento è soggetto alle azioni disciplinari previste, fino al licenziamento.

10.4. Livelli di sicurezza

L'amministrazione della sicurezza logica segue i criteri generali di seguito riportati:

- applicazione del principio “need to know” o del minimo privilegio, secondo cui la definizione dei profili standard da assegnare agli utenti, con le autorizzazioni necessarie all’espletamento delle rispettive mansioni (definite per ruoli e competenze), avviene alla luce delle effettive esigenze operative. A tal scopo viene limitato l’accesso logico a reti, sistemi e basi dati;
- la validità delle richieste di accesso alla rete è verificata automaticamente dal sistema stesso prima di consentire l’accesso ai dati, tramite un sistema di autenticazione costituito da User-ID e password;
- sono adottate delle indicazioni per la gestione delle password che stabiliscono la lunghezza, la complessità, la durata, la conservazione sicura richiesta nel caso di trattamenti dei dati effettuati con strumenti elettronici;
- sono previsti sistemi per la periodica validazione e il censimento delle utenze e delle abilitazioni;
- sono adottate tecniche e metodologie per la verifica continua dell’utilizzo dei sistemi applicativi e per il controllo del traffico di rete generato, al fine di garantire un pronto intervento in caso di attività anomale;
- sono previsti presidi rafforzati per l’accesso da remoto, in particolare nei confronti di utenti appartenenti a soggetti terzi;
- è prevista la revisione periodica delle misure di sicurezza, anche attraverso esercizi di penetration test, al fine di prevenire violazioni dei dati personali (Data Breach);
- sono organizzate sessioni di formazione dei dipendenti, nonché regolamenti e altre forme di documentazione interna, al fine di rendere gli stessi edotti dei rischi in materia di sicurezza delle informazioni e di protezione dei dati personali;
- sono previsti periodici controlli al fine di verificare l’adeguatezza, l’affidabilità complessiva e la tutela del sistema informativo.