A.Se.R SpA
Via Martiri della Libertà, 4
Cf e P.Iva 04626760963

Politica generale sulla protezione dei dati personali

Revisione:	1
Data della revisione:	25/05/2018
Redatta da:	Direzione Operativa/Ufficio Affari legali
Approvata da:	Direzione Operativa - CDA (in prima emissione)

STATO DELLE REVISIONI

Rev.	Data	Descrizione delle modifiche	Approvazione
01	25/05/2018	Prima emissione	DO - CdA

Indice

1. Scopo, campo di applicazione e destinatari

A.Se.R SpA, da ora in poi definita come “Società”, si impegna a essere conforme alle leggi e ai regolamenti applicabili relativi alla protezione dei dati personali.

La presente procedura definisce i principi fondamentali secondo i quali la Società tratta i dati personali di clienti, fornitori, business partner, dipendenti ed altri individui, ed indica le responsabilità dei propri servizi e dei propri dipendenti nel trattamento dei dati personali.

I destinatari della presente procedura sono tutti i dipendenti, temporanei o permanenti, e tutti i collaboratori che operano per conto della Società.

2. Riferimenti normativi

- GDPR 2016/679 (Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche in materia di trattamento dei dati personali e alla libera circolazione di tali dati e che abroga la Direttiva 95/46 / CE)
- Leggi nazionali o regolamenti rilevanti per l’implementazione del Regolamento

3. Definizioni

Le definizioni utilizzate nel presente documento sono tratte dall’articolo 4 del Regolamento Europeo:

«**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 sensibili: dati personali che, per loro natura, sono particolarmente sensibili in relazione ai diritti e alle libertà fondamentali e meritano una protezione specifica in quanto il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali. Questi dati personali includono dati personali che rivelano origine razziale o etnica, opinioni politiche, credenze religiose o filosofiche, appartenenza sindacale, dati genetici, dati biometrici che identificano in modo univoco una persona fisica, dati sulla salute o dati relativi all’orientamento sessuale della persona.

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;

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;

Anonimizzazione: de- identificazione irreversibile dei dati personali in modo tale che la persona non può essere identificata tramite tecnologie e in tempi e costi ragionevoli né dal titolare né da altra persona. I principi di trattamento dei dati personali non si applicano ai dati anonimi in quanto questi non sono considerati dati personali.

Pseudonimizzazione: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile; la pseudonimizzazione riduce, ma non elimina del tutto, la possibilità di collegare un dato personale a un interessato. Tenendo conto che i dati che hanno subito il processo di pseudonimizzazione sono ancora dati personali, tale processo deve essere conforme ai principi di trattamento dei dati personali.

Trattamento transfrontaliero: 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 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 incide in modo sostanziale su interessati in più di uno Stato membro;

Autorità di controllo: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

Autorità di controllo principale: l'autorità di vigilanza con la responsabilità primaria di occuparsi di un'attività di trattamento di dati transfrontaliera, ad esempio quando un interessato presenta un reclamo in merito al trattamento dei propri dati personali; è responsabile, tra l'altro, di ricevere le notifiche di violazione dei dati, di essere informato sulle attività di trattamento rischiose e avrà piena autorità per quanto riguarda i suoi obblighi di garantire l'osservanza delle disposizioni del GDPR;

Ciascuna "**autorità di vigilanza locale**" manterrà comunque la sua attività nel proprio territorio e monitorerà qualsiasi trattamento di dati a livello locale che riguarda gli interessati o che viene effettuato da un titolare o un responsabile UE o non UE quando il loro trattamento si rivolge agli interessati che risiedono sul suo territorio. I loro compiti e poteri comprendono lo svolgimento di indagini e l'applicazione di misure amministrative e sanzioni,

la promozione a livello generale della consapevolezza dei rischi, delle norme, della sicurezza e dei diritti in relazione al trattamento dei dati personali, nonché l'accesso a qualsiasi sede del responsabile del titolare e del responsabile, compresi eventuali strumenti e mezzi per il trattamento dei dati.

Stabilimento principale: per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

Gruppo imprenditoriale: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

4. Principi base del trattamento dei dati personali

I principi sulla protezione dei dati delineano le responsabilità base per le organizzazioni che si occupano del trattamento dei dati personali. L'articolo 5, punto 2 del Regolamento stabilisce che "*il titolare del trattamento è responsabile e deve dimostrare la conformità a tali principi".*

4.1. Legalità, correttezza e trasparenza

I dati personali devono essere trattati in modo lecito, equo e trasparente in relazione all'interessato.

4.2. Limitazione dello scopo

I dati personali devono essere raccolti per scopi specifici, espliciti e legittimi e non ulteriormente trattati in modo incompatibile con tali scopi.

4.3. Minimizzazione dei dati

I dati personali devono essere adeguati, pertinenti e limitati a quanto necessario in relazione agli scopi per i quali sono trattati. Se possibile per ridurre i rischi per gli interessati la Società deve applicare l'anonimizzazione o la pseudonimizzazione ai dati personali.

4.4. Precisione

I dati personali sono accurati e, ove necessario, aggiornati; misure ragionevoli devono sono prese per garantire che i dati personali inaccurati, in relazione alle finalità per cui sono trattati, siano cancellati o rettificati in modo tempestivo.

4.5. Limitazione del periodo di conservazione

I dati personali sono conservati per un periodo non superiore a quello necessario agli scopi per i quali i dati personali sono trattati.

4.6. Integrità e confidenzialità

Tenendo conto dello stato della tecnologia e di altre misure di sicurezza disponibili, dei costi di implementazione e della probabilità e della gravità dei rischi dei dati personali, la Società utilizza misure tecniche o organizzative adeguate per trattare i dati personali in modo tale da garantire un'adeguata sicurezza dei dati personali, compresa la protezione contro la distruzione, la perdita, l'alternanza o la divulgazione accidentale o illecita o l'accesso non autorizzato.

4.7. Responsabilità

I responsabili del trattamento dei dati sono responsabili di dimostrare la conformità ai principi sopra descritti.

5. Integrare la protezione dei dati nelle attività commerciali

Al fine di dimostrare la conformità ai principi della protezione dei dati, l'organizzazione integra il sistema di protezione dei dati nei processi delle varie attività espletate.

5.1. Informativa agli interessati

(Vedi la sezione Linee Guida sul corretto trattamento)

5.2. Scelta e consenso dell'interessato

(Vedi la sezione Linee Guida sul corretto trattamento)

5.3. Raccolta

La Società raccoglie il minor numero possibile di dati personali. Se i dati personali sono raccolti da una terza parte, il Titolare si assicura che i dati personali siano raccolti secondo le previsioni di legge.

5.4. Utilizzo, conservazione e smaltimento

Gli scopi, i metodi, i limiti di archiviazione e il periodo di conservazione dei dati personali sono coerenti con le informazioni contenute nell'informativa sulla protezione dei dati generali.

La Società mantiene l'accuratezza, l'integrità, la riservatezza e la rilevanza dei dati personali in base allo scopo del trattamento. Utilizza adeguati meccanismi di sicurezza volti a proteggere i dati personali per impedire che vengano rubati o utilizzati in modo improprio e previene le violazioni dei dati personali. il Titolare è responsabile della conformità ai requisiti elencati in questa sezione.

5.5. Divulgazione a terzi

Ogni volta che la Società utilizza un fornitore di terza parte o un partner commerciale per trattare i dati personali per suo conto, garantisce che questo processore fornisca misure di sicurezza per salvaguardare i dati personali appropriate ai rischi associati.

La Società richiede contrattualmente al fornitore o al partner commerciale di fornire lo stesso livello di protezione dei dati. Il fornitore o il partner commerciale deve elaborare i dati

personali solo per adempiere ai propri obblighi contrattuali nei confronti della Società o dietro istruzioni della Società e non per altri scopi. Quando l'Azienda tratta i dati personali congiuntamente con una terza parte indipendente, la Società specifica esplicitamente le rispettive responsabilità e la terza parte nel rispettivo contratto o in qualsiasi altro documento legalmente vincolante, come il Contratto di trattamento dei dati del fornitore (Supplier Data Processing Agreement).

5.6. Trasferimento transfrontaliero dei dati personali

In caso la Società trasferisca i dati personali dallo Spazio economico europeo (SEE) devono essere utilizzate misure di salvaguardia adeguate, compresa la firma di un accordo sul trasferimento dei dati, come richiesto dall'Unione europea e, se necessario, ottenendo l'autorizzazione da parte della autorità di protezione dei dati. L'entità che riceve i dati personali deve rispettare i principi del trattamento dei dati personali stabiliti nella Procedura di trasferimento dei dati transfrontalieri.

5.7. Diritti di accesso degli interessati

Quando agisce come titolare del trattamento dei dati, la Società fornisce agli interessati un ragionevole meccanismo di accesso che consenta loro di accedere ai propri dati personali e di aggiornare, correggere, cancellare o trasmettere i propri dati personali, alle condizioni stabilite dalla legge.

5.8. Portabilità dei dati

Gli interessati hanno il diritto di ricevere, su richiesta, una copia dei dati che hanno fornito in un formato strutturato e di trasmettere gratuitamente tali dati a un altro titolare. il Titolare è responsabile di garantire che tali richieste vengano elaborate entro un mese, non siano eccessive e non pregiudichino i diritti sui dati personali di altre persone.

5.9. Diritto all’oblio

Sussistendo le condizioni previste dall’art. 17 del GDPR 2016/679 (Regolamento (UE) 2016/679, l’interessato, su richiesta, ha il diritto di ottenere dalla società la cancellazione dei suoi dati personali. Quando la Società agisce in qualità di titolare del trattamento, intraprende le azioni necessarie (comprese le misure tecniche) per informare le terze parti che usano o trattano quei dati di adeguarsi alla richiesta.

6. Linee guida sul corretto trattamento

I dati personali sono trattati legittimamente quando ricorrono le condizioni di cui all’art. 6 del GDPR 2016/679 (Regolamento (UE), qualora il trattamento sia basato sul consenso, il trattamento avviene solo se esplicitamente autorizzati dal titolare.

La Società effettua una valutazione di impatto sulla protezione dei dati per ogni attività di trattamento dei dati secondo quanto definito dalle Linee guida sulla valutazione dell’impatto sulla protezione dei dati personali. Data Protection Impact Assessment Guidelines.

6.1. Informativa agli interessati

Al momento della raccolta o prima della raccolta di dati personali per qualsiasi tipo di attività di trattamento, il Titolare è responsabile di informare adeguatamente gli interessati di quanto segue: la tipologia di dati personali raccolti, le finalità del trattamento, i metodi di trattamento, i diritti degli interessati in relazione ai loro dati personali, il periodo di conservazione, i potenziali trasferimenti internazionali di dati, se i dati saranno condivisi con terzi e le misure di sicurezza della Società per proteggere i dati personali. Queste informazioni sono fornite tramite un'informativa generale sulla protezione dei dati.

L'azienda sviluppa comunicazione differenziate in relazione alle molteplici attività di trattamento dei dati, i alle differenti caratteristiche del trattamento e delle categorie di dati personali raccolti.

Laddove i dati personali siano condivisi con terzi, il Titolare garantisce che gli interessati siano informati di ciò tramite un'informativa generale sulla protezione dei dati

Laddove i dati personali siano trasferiti in un paese terzo in base alla politica di trasferimento dei dati transfrontalieri, ciò è specificato nell'informativa generale sulla protezione dei dati, indicando chiaramente dove e a quale entità vengono trasferiti i dati personali.

Nel caso in cui vengano raccolti dati personali sensibili, il Responsabile della Protezione dei Dati assicura che l'informativa generale sulla protezione dei dati chiarisca espressamente lo scopo per il quale tali dati sensibili vengono raccolti.

6.2. Ottenimento dei consensi

Ogni qualvolta il trattamento dei dati personali è basato sul consenso dell'interessato, o su altri motivi legittimi, il Titolare è responsabile di conservare una registrazione di tale consenso. Il Titolare è responsabile di presentare alle persone interessate le diverse opzioni per fornire il consenso e deve informare e garantire che il loro consenso (ogni volta che viene utilizzato come base legale per il trattamento) possa essere revocato in qualsiasi momento.

Quando viene richiesto di correggere, modificare o distruggere registrazioni di dati personali, la Società garantisce che tali richieste siano gestite entro un ragionevole lasso di tempo. Le stesse sono registrate.

I dati personali devono essere trattati solo per lo scopo per il quale sono stati originariamente raccolti. Nel caso in cui la Società desideri trattare i dati personali raccolti per un altro scopo, deve richiedere il consenso dei suoi interessati in forma scritta chiara e concisa. Qualsiasi richiesta di questo tipo deve includere lo scopo originale per cui sono stati raccolti i dati e anche gli scopi nuovi o aggiuntivi. La richiesta include anche il motivo del cambiamento di scopo / i. Il Data Protection Officer/Responsabile della Protezione dei Dati è responsabile del rispetto delle regole in questo paragrafo.

La Società garantisce la conformità alla legge, alle buone pratiche e agli standard industriali pertinenti, dei metodi di raccolta del consenso praticati.

La Società è responsabile della creazione e della manutenzione di un registro delle informative generali sulla protezione dei dati.

7. Organizzazione e responsabilità

La responsabilità di garantire un adeguato trattamento dei dati personali spetta a chiunque lavori all'interno della Società o per suo conto e abbia accesso ai dati personali da essa trattati.

Le principali aree di responsabilità per il trattamento dei dati personali sono riferibili ai seguenti ruoli organizzativi:

Il **Consiglio di Amministrazione,** che unitamente alla **Direzione Operativa** prende decisioni e approva le strategie generali della Società in materia di protezione dei dati personali.

La **Direzione Operativa**, è inoltre responsabile:

- della predisposizione e dell'aggiornamento del Registro dei trattamento e della Valutazione dei Rischi;
- della implementazione e della esecuzione delle strategia di protezione dei dati personali.
- di garantire la protezione end-to-end dei dati personali dei dipendenti. In particolare che i dati personali dei dipendenti vengano elaborati in base a finalità legittime e alle necessità aziendali del datore di lavoro.
- di trasmettere al Consiglio di Amministrazione tutte le comunicazione relative al sistema di gestione della protezione dei dati personali.
- approvare qualsiasi dichiarazione sulla protezione dei dati allegata a comunicazioni quali e-mail e lettere.
- affrontare qualsiasi quesito in merito alla protezione dei dati da parte di giornalisti o altri mezzi di informazione come giornali.
- ove necessario, collaborare con il Data Protection Officer per garantire che le iniziative intraprese dall'Azienda rispettino i principi di protezione dei dati.
- migliorare la consapevolezza di tutti i dipendenti sulla protezione dei dati personali degli utenti.
- organizzare per i dipendenti che lavorano con dati personali formazione per aumentare la competenza in materia di protezione dei dati personali e la consapevolezza.
- protezione end-to-end dei dati personali dei dipendenti. Deve garantire che i dati personali dei dipendenti vengano elaborati in base a finalità legittime e alle necessità aziendali del datore di lavoro.

Il **Data Protection Officer (DPO)** o Responsabile della Protezione dei Dati, è responsabile della gestione del programma di protezione dei dati personali e dello sviluppo e della promozione delle procedure end-to-end di protezione dei dati personali, come definito nella lettera d'incarico del Data Protection Officer;

Il **Responsabile dell'Ufficio Affari legali** (Referente Privacy) che unitamente al Data Protection Officer/Responsabile della Protezione dei Dati, monitora e analizza le leggi sui dati personali e le modifiche alle normative e assiste i reparti aziendali nel raggiungimento dei loro obiettivi relativi ai dati personali, si occupa inoltre di:

- migliorare la consapevolezza di tutti i dipendenti sulla protezione dei dati personali degli utenti.
- organizzare per i dipendenti che lavorano con dati personali formazione per aumentare la competenza in materia di protezione dei dati personali e la consapevolezza.
- organizzare i piani di Audit e svolgere le relative verifiche.

Amministratore di sistema (esterno) è responsabile di:

- garantire che tutti i sistemi, i servizi e le attrezzature utilizzate per l'archiviazione dei dati abbiano standard di sicurezza adeguati.
- effettuare controlli periodici ed esami per verificare il livello di sicurezza dell'hardware e il funzionamento corretto del software.

8. Autorità di controllo principale

Dato atto che la Società ha sedi solo nello Stato Italiano e le sue attività di trattamento riguardano solo le persone interessate in tale Stato membro, l'unica autorità competente sarà l'autorità di vigilanza nel paese in cui la Società ha sede legale.

9. Risposta agli incidenti di violazione dei dati personali

Quando la Società viene a conoscenza di una sospetta o reale violazione dei dati personali, conduce, tramite i referenti di funzione, un'indagine interna e prende appropriati provvedimenti in maniera tempestiva. Queste sono comunicate alla Direzione Operativa, al Referente Privacy e al Responsabili della Protezione dei Dati (DPO).

Se ci sono delle minacce ai diritti e alle libertà degli interessati, la Società procede nel rispetto di quanto disposto agli artt. 33 e 33 del Regolamento, notificando le violazioni alle autorità per la protezione dei dati senza alcun ritardo, e se possibile, entro 72 ore. Tale notifica deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Quando la violazione è suscettibile di presentare un rischio per i diritti e le libertà degli interessati, la Società provvede, senza ingiustificato ritardo, a comunicarla agli interessati alle condizioni e nei termini disciplinati all'art. 34 del Regolamento.

Il Titolare del trattamento, la Direzione Operativa e il Referente Privacy sono responsabili di effettuare le comunicazioni/notifiche di cui ai paragrafi precedete, che devono avvenire con mezzi idonei e comprovarne la ricezione da parte dei destinatari (es. raccomandata A/R, PEC). L'elenco delle violazioni è archiviato, unitamente alle inerenti comunicazioni, presso l'ufficio del Referente Privacy.

10. Audit e responsabilità

Il Referente Privacy, con il supporto del Responsabile della Protezione dei Dati , è responsabile di verificare con le cadenze stabilite nelle successive "Istruzioni operative", la corretta applicazione della presente procedura da parte delle aree aziendali.

La violazione della presente procedura comporterà l'applicazione di un'azione disciplinare, ferme restando le responsabilità civili o penali conseguenti alla violazione di leggi o regolamenti.

11. Conflitti di legge

Tale procedura intende essere conforme con le leggi ed i regolamenti vigenti nei paesi dove è ubicata e dove opera la Società. In caso di conflitto tra questa procedura e le leggi ed i regolamenti applicabili, prevalgono questi ultimi.

12. Gestione e validità del documento

Il responsabile del documento è il Direttore Operativo, che unitamente all'Ufficio Affari Legali ha il compito di controllarlo e, se necessario, aggiornarlo.

Allegati:

A. Istruzioni operative:
1) gestione dei responsabili esterni;
2) controllo interno (audit);
3) gestione dei sistemi di videosorveglianza;
4) gestione delle informative;
5) gestione della formazione.

B. Registro dei trattamenti ed annessi:
1) documento di Descrizione delle misure tecniche per la protezione degli strumenti informatici;
2) Linee guida.

C. Valutazione del rischio ed annessa:
1) Metodologia di valutazione.

D. Funzionigramma e Organigramma Privacy.

ISTRUZIONI OPERATIVE

1) GESTIONE DEI RESPONSABILI ESTERNI:

La mappatura dei soggetti incaricati dalla Società, quale Titolare del trattamento, di svolgere il ruolo di responsabili esterni del trattamento permette di individuare con più semplicità quali attività di trattamento sono state affidate in outsourcing.

Per ogni soggetto a cui viene affidato l'incarico di responsabile esterno del trattamento dei dati deve essere dimostrata la conformità ai requisiti del GDPR, conformità che può essere verificata dal titolare tramite la specifica checklist per la qualifica del fornitore.

L'incarico di responsabile esterno deve essere affidato tramite specifico accordo tra le parti che, una volta sottoscritto, deve essere archiviato e conservato, mediante la lettera di nomina a responsabili esterni del trattamento.

Tutti i soggetti che ricoprono il ruolo di responsabili esterni devono essere inseriti in specifico elenco.

Nel caso in cui l'ufficio incaricato della gestione dei fornitori identifica un soggetto come fornitore di una attività che comporta il trattamento di dati personali, deve avvertire il referente privacy che inserisce il soggetto all'interno dell'elenco dei responsabili esterni.

Nel caso in cui sia obbligatoria la nomina del Responsabile per la Protezione dei Dati, il Referente Privacy consegna al soggetto individuato la lettera di nomina del Responsabile della Protezione e ne ottiene copia firmata per accettazione.

Allegati:

- MOD0201 - Lettera di nomina dei responsabili del trattamento esterni
- MOD0202 - Elenco responsabili esterni
- MOD0203 - Checklist per la qualifica dei responsabili esterni

2) CONTROLLO INTERNO (AUDIT):

Vengono di seguito definiti i tempi e i modi per monitorare, verificare e valutare l'efficacia delle misure tecniche organizzative impiegate dalla Società per garantire la sicurezza del trattamento dei dati.

Piano di audit interni

Il Referente Privacy definisce il programma annuale di audit. Gli audit interni vengono effettuati, con il supporto del DPO, con cadenza almeno annuale in base alla valutazione dei rischi e ai risultati degli audit precedenti.

Conduzione di un singolo audit interno

Gli aspetti che devono essere verificati e valutati durante l'audit interno sono i seguenti:

- Requisiti delle politiche, delle procedure di gestione dei dati personali della Società
- Risultati dei precedenti audit interni
- Risultati dell'analisi dei rischi, dei controlli, della valutazione di impatto della protezione dei dati.

Come risultato degli audit interni devono essere documentati i seguenti dati:

- L'auditor interno deve registrare tutte le evidenze nel report degli audit interni
- Se vengono riscontrate non conformità, l'auditor interno deve riportarle in forma scritta alla Direzione Operative che li riporta al Titolare del Trattamento.

Allegati:

- MOD0101 - Piano di audit
- MOD0102 - Verbale di audit
- MOD0103 - Checklist (lista di riscontro) audit interni

3) GESTIONE DEI SISTEMI DI VIDEOSORVEGLIANZA:

La videosorveglianza è un sistema che implica la raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini. Ciò configura un trattamento di dati personali pertanto deve essere gestito in maniera tale da tutelare i diritti e le libertà fondamentali degli interessati al trattamento dei dati personali.

Per ogni sistema di videosorveglianza installato, è necessario verificare:

- Presenza degli appositi cartelli informativi
- Numero delle telecamere installate
- Posizionamento delle telecamere
- Numero dei monitor
- Numero delle apparecchiature di registrazione

Allegati

- MOD0401 – Nomina responsabile videosorveglianza
- MOD0402 – Nomina rappresentante lavoratori videosorveglianza
- MOD0403 – Nomina manutentore impianto videosorveglianza
- MOD0404 – Informativa sistema di videosorveglianza
- MOD0405 – Informativa dipendente
- MOD0406 – Elenco sedi sottoposte a videosorveglianza

4) GESTIONE DELLE INFORMATIVE:

Quando i dati riguardanti altri individui sono raccolti e utilizzati non per uso strettamente personale ma per altre finalità, il trattamento dei dati personali deve rispettare alcune regole, in particolare l'obbligo di informazione dell'interessato. Di seguito vengono definite le modalità di gestione delle informative relative ai dati personali.

Per ogni attività di trattamento che comporti la raccolta di dati di soggetti terzi, siano essi dipendenti o clienti o utenti deve essere individuata:

- Tipo di informativa
- Modalità di presentazione dell'informativa agli utenti
- Tempistiche di presentazione dell'informativa
- Data di aggiornamento del testo dell'informativa

Tali informazioni sono conservate all'interno del registro delle informative.

Il referente privacy deve monitorare e approvare le informative presenti all'interno del registro e deve validare la conformità del testo rispetto a quanto richiesto dagli articoli 13 e 14.

Il referente privacy nella verifica delle informative deve assicurarsi che sia rispettata la richiesta dell'articolo 12 del Regolamento, in merito alla semplicità e trasparenza delle comunicazione.

Allegati

- MOD0701 – Registro delle informative
- MOD0702 – Privacy policy per il sito internet
- MOD0703 – Informativa per il personale dipendente

5) GESTIONE DELLA FORMAZIONE:

Tutto il personale che ha accesso permanente o regolare ai dati deve ricevere adeguata formazione e informazione sui requisiti del Regolamento e sulle procedure implementate dalla Società per garantire la conformità a tale normativa ed assicurare agli interessati il corretto trattamento dei loro dati e il rispetto dei loro diritti e libertà fondamentali.
La formazione viene svolta anche mediante una lettera di responsabilizzazione e di incarico al trattamento.
La formazione può essere svolta nella modalità giudicata più appropriata alle esigenze della Società e viene registrata in apposito registro, parte del Programma di addestramento aziendale.