Sistema Gestione Privacy

REDAZIONE A CURA DI

Dott. Rosario Guerra

1° EMISSIONE

Dicembre 2022

Indice

1.

Obiettivi

Siamo consapevoli dell'importanza della tutela dei dati personali, in linea con le normative vigenti: per questo abbiamo definito questa Privacy Policy, espressione dell'approccio complessivo che intendiamo adottare per essere pienamente compliant ai requisiti normativi del GDPR.

Il presente documento ha l'obiettivo di rappresentare l'approccio complessivo adottato dalla Salerno Mobilità Spa al fine di garantire un adeguato livello di tutela dei dati personali di cui effettua un trattamento nel rispetto della normativa di riferimento, in particolare del Regolamento Generale sulla Protezione dei Dati (Regolamento UE 2016/679). Tale norma ha introdotto significativi cambiamenti nel contesto della gestione dei dati personali inducendo l'azienda a rinnovare le proprie politiche, procedure e prassi al fine di allinearsi al quadro normativo vigente e ad armonizzarlo con le normative nazionali per le specifiche peculiarità.

In particolare, il presente documento, che è parte integrante del Modello di Governance Privacy dell'Azienda, illustra i principi, i processi, le metodologie, i ruoli e responsabilità e le attività di monitoraggio che costituiscono nel complesso il "Sistema di Gestione Privacy", a cui la società deve conformarsi per rispondere in modo adeguato alla gestione dei dati personali di cui effettua un trattamento.

Il **Sistema di Gestione Privacy** adottato viene concretamente applicato facendo ricorso alla metodologia Plan-Do-Check-Act in ottica di miglioramento continuo e ponendo particolare attenzione alla fase di "analisi del rischio" permettendo all'organizzazione di determinare preventivamente i fattori che potrebbero rendere inefficace il Sistema di Gestione e di porre in atto i controlli necessari ad assicurare che questo non accada.

La struttura di riferimento del presente documento è inoltre ispirata alla High Level Structure ("HLS") delle norme ISO, ovvero all'insieme delle clausole che compongono le norme emanate dall'ente di standardizzazione internazionale. Tale scelta è dettata dai vantaggi offerti dall'adozione di un approccio riconosciuto a livello internazionale ed allineato a quello degli altri sistemi di gestione.

1.2 Ambito di applicazione e modalità di recepimento

Il presente documento si applica all'Azienda Salerno Mobilità Spa.
La Privacy Policy ha come campo di applicazione tutte le finalità di trattamento di dati personali comprese nel perimetro complessivo dei processi operativi della Società.

1.3 Riferimenti normativi esterni

È di seguito riportato un elenco, non esaustivo, dei riferimenti normativi a cui il Sistema di Gestione Privacy si attiene. Nell'ambito delle numerose linee guida emesse dal gruppo europeo del Working Party 29 (ora European Data Protection Board – EDPB), sono state considerate, ai fini della redazione del presente documento, solo quelle direttamente applicabili al contesto:

- 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 e che abroga la direttiva 95/46/CE (**Regolamento Generale sulla Protezione dei Dati**).
- Standard ISO/IEC 29134:2017 - Guidelines for Privacy Impact Assessment.
- Linee Guida sul Data Protection Impact Assessment emanate dal Working Party 29 (comitato delle Autorità UE Garanti per la protezione dei dati personali).
- Linee sul Data Protection Officer emanate dal Working Party 29 (comitato delle Guida Autorità UE Garanti per la protezione dei dati personali).
- Linee Guida sul Data Breach Notification emanate dal Working Party 29 (comitato delle Autorità UE Garanti per la protezione dei dati personali).
- Linee Guida sulla Trasparenza ai sensi del Regolamento 2016/679 emanate dal Working Party 29 (comitato delle Autorità UE Garanti per la protezione dei dati personali).
- Linee Guida sul Consenso ai sensi del Regolamento (UE) 2016/679 emanate dal Working Party 29 (comitato delle Autorità UE Garanti per la protezione dei dati personali).
- Handbook on Security of Personal Data Processing dell'ENISA (European Union Agency for Network and Information Security).

Sebbene il Regolamento UE 2016/679 sia di diretto recepimento da parte degli Stati membri e miri ad una completa armonizzazione tra le normative nazionali, contiene molte norme (le c.d. "disposizioni flessibili" o "clausole di specificazione") che rimandano alla legislazione degli Stati membri la disciplina più particolareggiata di alcune materie entro il quadro complessivamente offerto dal Regolamento.

Pertanto, nell'applicazione del presente **Sistema di Gestione Privacy** (di seguito anche Privacy Policy) oltre alle norme di cui sopra, l'Azienda deve tenere in considerazione anche la normativa nazionale sulla Data Protection in vigore in Italia a seguito della introduzione del GDPR.

1.4 Definizioni, abbreviazioni e acronimi

Ai fini della presente Policy si applicano le seguenti definizioni, coerenti con quanto previsto dalla normativa di settore:

TERMINE	DEFINIZIONE
Amministratore di Sistema (Ads)	Figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise Resource Planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.
Autorità di Controllo Nazionale	L'autorità pubblica indipendente istituita dai singoli Stati membri, ai sensi dell'art. 51 del GDPR.
Consenso dell'Interessato	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

TERMINE	DEFINIZIONE
Dato Giudiziario	Sono i dati personali che rivelano l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (quali, ad es., i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione). Rientrano in questa categoria anche la qualità di imputato o di indagato.
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.
Dato Personale Particolare	Sono i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Delegati del trattamento	I dipendenti della Salerno Mobilità Spa che hanno la responsabilità di garantire l'applicazione delle disposizioni privacy impartite dal Titolare, nonché l'osservanza delle prescrizioni in materia di misure adeguate di sicurezza. Promuovono, nelle strutture assegnate, l'adozione di prassi conformi al GDPR e alle correlate norme interne di attuazione.
Destinatario	La persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari. Esempi di destinatari: organismi sanitari, enti previdenziali ed assistenziali, ecc.
DPIA	Data Protection Impact Assessment (o Valutazione d'Impatto sulla Protezione dei Dati). Processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando tali rischi e determinando le misure per affrontarli.
DPO	Persona fisica o giuridica che informa e consiglia il Titolare o il Responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal GDPR e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati. Inoltre, sorveglia sull'osservanza del GDPR e di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali.

TERMINE	DEFINIZIONE
Consulente Privacy	Soggetto esterno che svolge un ruolo di supporto per le tematiche Privacy all'interno della Società, gestisce l'integrazione e il coordinamento tra i diversi attori coinvolti in ambito Privacy.
Informativa all'interessato	Documento contenente tutte le informazioni fornite all'Interessato al momento della raccolta dei suoi dati personali (sia che i dati siano raccolti presso l'Interessato che presso terzi.
Interessato	Persona fisica identificata o identificabile per mezzo di un trattamento dei suoi dati personali effettuato dalla Salerno Mobilità Spa.
Persona Autorizzata al trattamento o Incaricata al trattamento	Persone fisiche che sono state autorizzate dal Titolare o dal Responsabile all'esecuzione di trattamenti di dati personali.
Paesi Terzi	Paesi non appartenenti all'UE o allo Spazio Economico Europeo.
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 (c.d. GDPR - Regolamento Generale sulla Protezione dei Dati).

Responsabile Esterno 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 sulla base di un contratto o altro atto giuridico a norma del diritto dell'Unione o degli Stati membri (cfr. GDPR-artt. 4, 28).
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 e mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento sia effettuato conformemente alle normative vigenti (cfr. GDPR-artt. 4, 24).
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.
WP29	Working Party 29. Comitato delle Autorità UE Garanti per la protezione dei dati personali. Sostituito dallo European Data Protection Board (EDPB).

2.

Contesto

Questo documento illustra principi, processi, metodologie, ruoli e responsabilità, attività di monitoraggio: elementi che costituiscono nel complesso il "Sistema di Gestione Privacy", a cui la Salerno Mobilità Spa deve conformarsi per gestire in modo adeguato i dati personali di cui effettua un trattamento.

2.1 Comprendere l'organizzazione ed il suo contesto

La Salerno mobilità Spa, nell'adottare il proprio Modello di Governance Privacy, tiene conto sia dei fattori esterni quali, ad esempio, nuove normative o standard sulla protezione dei dati, che di quelli interni come, ad esempio, nuovi processi di trattamento, modifiche all'organizzazione, etc., che possono influenzare la capacità di conseguire i risultati attesi dal Sistema di Gestione, nell'ottica di perseguire il miglioramento continuo.

- gli Interessati, siano essi esterni (es. clienti, fornitori, etc.) che interni (dipendenti) a cui l'Azienda vuole garantire un trattamento dei relativi dati personali orientato ai principi di correttezza, liceità e trasparenza, in conformità con le normative vigenti in materia di dati personali, bilanciando le necessità di entrambe le parti, ovvero da un lato la tutela dei diritti dell'interessato, dall'altro il perseguimento delle finalità organizzative.
- il Management della Società Salerno Mobilità Spa che riveste un ruolo attivo nel Modello di Governance Privacy definito (in particolare il Titolare) **a cui si vuole fornire evidenza della presenza di un Sistema di Gestione** orientato a garantire la conformità alle normative applicabili in materia di privacy, in maniera efficace ed efficiente, secondo un approccio di miglioramento continuo;
- Il Personale Autorizzato al Trattamento (Incaricato al trattamento), a cui si vuole garantire il necessario supporto in termini di formazione, istruzioni e procedure, riferimenti organizzativi e strumenti per svolgere i propri compiti nel contesto dei trattamenti dei dati personali in maniera consapevole delle possibili conseguenze derivanti da comportamenti a rischio e con la tranquillità della presenza di processi strutturati in grado di garantire la conformità ai requisiti privacy applicabili.

3.

Leadership

La diffusione della cultura e della sensibilità per la protezione dei dati personali al nostro interno è il primo passo per la compliance alla normativa: per questo poniamo con forza l'accento sulla "responsabilizzazione" (accountability) di tutti i ruoli organizzativi, delle Direzioni e delle Funzioni che concorrono, ognuna in ragione delle specifiche competenze, alla definizione e/o mantenimento del modello di Governance della Privacy.

3.1 Politica

La Salerno Mobilità Spa, consapevole dell'importanza dell'attenzione alla tutela dei dati personali ed in accordo alle normative vigenti, ha emesso la presente Privacy Policy, che è resa disponibile a tutti i dipendenti della Società e su richiesta, ad ogni aggiornamento ed emissione, a tutte le parti esterne che concorrono alla gestione dei processi di trattamento dei dati personali (Fornitori, Clienti, Partner).

La Società si impegna a garantire e dimostrare che il trattamento dei dati avviene in maniera conforme a quanto previsto dalla normativa e secondo i seguenti principi applicabili al trattamento dei dati personali, ai sensi anche dell'Art. 5 UE 679/2016:

- **Liceità, correttezza e trasparenza**: i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- **Limitazione della finalità**: raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- **Minimizzazione dei dati**: adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- **Esattezza**: 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;
- **Limitazione della conservazione**: 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;
- **Integrità e riservatezza**: 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.

La stessa garanzia di protezione e di adozione di adeguate misure di sicurezza è richiesta altresì a quei soggetti terzi ai quali la società ha affidato l'incarico della gestione di alcuni trattamenti.

3.2 Ruoli, Responsabilità ed Autorità nell'organizzazione

Sulla base di quanto riportato in precedenza si illustrano di seguito i principali ruoli organizzativi previsti nel Modello di Governance Privacy dell'Azienda.

3.2.1 TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento è l'entità che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali. In particolare, la Salerno Mobilità Spa è il Titolare del trattamento che, in aderenza alle disposizioni di legge, esercita un potere decisionale autonomo sulle finalità e sulle modalità secondo le linee guida contenute nella presente policy. Al Titolare, in persona del suo rappresentante legale o delegato, sono affidate le responsabilità di:

- Adottare il sistema e le regole di indirizzo e di attuazione della normativa vigente ed assegnare di conseguenza i compiti alle diverse strutture in essa previste;
- Nominare il Responsabile Privacy;
- Nominare il DPO (Data Protection Officer)
- Nominare l'Amministratore di Sistema;
- Definire e fornire tramite, specifiche disposizioni, le finalità, le modalità, gli strumenti e le misure di sicurezza per il trattamento dei dati personali;
- Approvare il piano delle verifiche periodiche e disporre gli interventi necessari alla risoluzione delle anomalie riscontrate;
- Approvare le nomine dei Responsabili Esterni del Trattamento, vigilando sul rispetto delle istruzioni a questi impartite;
- Approvare il Registro dei trattamenti della Società;
- Garantire l'informazione e la formazione delle persone autorizzate al trattamento (incaricati) sulle tematiche relative alla protezione dei dati personali e sul Sistema di Gestione adottato;
- Garantire autonomia e indipendenza di giudizio alle figure che svolgono attività di controllo del rispetto ed attuazione del Regolamento UE.

3.2.2 RESPONSABILE AL TRATTAMENTO

È la persona fisica (dipendente) aziendalmente identificata tramite uno specifico atto di nomina interno, per garantire l'applicazione delle disposizioni impartite dal Titolare nell'ambito della funzione di sua competenza, nonché l'osservanza delle prescrizioni in materia di misure adeguate di sicurezza.

Ha la responsabilità di:

- Nominare gli Incaricati al Trattamento;
- Attuare le prescrizioni impartite dal Titolare, con particolare riferimento ai controlli di primo livello sul rispetto delle policy e procedure aziendali;
- Informare tempestivamente il Titolare qualora identifichi o venga informato di una violazione di sicurezza sia essa intenzionale o accidentale (Data Breach) e collaborare nella gestione delle stesse e negli obblighi di notifica e informativa;
- Promuovere nelle strutture di cui ha la responsabilità, l'adozione di prassi conformi al "GDPR" e alle correlate norme interne di attuazione;
- Sottopone al Titolare adeguamenti o nuove attività formative da erogare all'interno delle strutture a lui assegnate;
- Svolgere attività di coordinamento e controllo sui trattamenti effettuati nell'ambito delle strutture assegnate, assicurandosi che i propri collaboratori abbiano accesso ai soli dati personali il cui trattamento sia strettamente necessario per adempiere ai compiti loro assegnati;
- Informare il Titolare di nuovi trattamenti di dati personali ovvero di modifiche ai trattamenti esistenti eseguendo la valutazione preliminare dei rischi ed eventuale

Valutazione d'Impatto Privacy prima di procedere al trattamento;

- Proporre al Titolare i nominativi delle società/enti/soggetti da designare a Responsabili del Trattamento per i trattamenti svolti all'esterno dell'organizzazione;
- Garantire la distruzione/cancellazione dei dati personali gestiti di cui è responsabile, al termine del loro trattamento.

3.2.3 DPO – Data Protection Officer

È la persona fisica o referente unico di Società/Ente con il compito di garantire che i diritti e le libertà degli interessati non siano pregiudicati dalle operazioni di trattamento effettuate dal Titolare. Ha le seguenti responsabilità:

- Verificare l'attuazione e l'applicazione del GDPR e delle altre disposizioni relative alla protezione dei dati, nonché delle politiche della Società adottate nel suo ruolo da Titolare o da Responsabile in materia di protezione dei dati personali;
- Fornire, se richiesto, pareri in merito al DPIA e assiste il Titolare nelle attività di esecuzione della DPIA a seguito di nuovi trattamenti o di modifiche ai trattamenti esistenti e sorvegliare i relativi adempimenti;
- Fungere da punto di contatto per gli Interessati, gestendo anche eventuali controversie e reclami, informando il Titolare nei casi ritenuti critici;
- Rappresentare il punto di contatto per il Garante oppure, eventualmente, consultare il Garante di propria iniziativa;
- Essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali;
- Essere coinvolto tempestivamente in caso di una violazione dei dati personali (Data Breach) al fine di supportare il Titolare nella valutazione del possibile impatto della violazione sulle libertà e i diritti degli interessati stessi e della necessità di notificare la violazione all'Autorità di Controllo e/o agli Interessati;
- Informare il Titolare dei cambiamenti e delle novità del Regolamento EU e della normativain materia di dati personali.

3.2.4 INCARICATO AL TRATTAMENTO

È la persona fisica, dipendente dell'Azienda, autorizzata dal Responsabile del trattamento, a compiere operazioni di trattamento dei dati attraverso uno specifico atto di nomina interno.

Ha la responsabilità di:

- Osservare le prescrizioni impartite dal Responsabile al trattamento;
- Trattare solo ed esclusivamente i dati personali strettamente necessari all'espletamento delle proprie mansioni;
- Conservare i dati personali, trattati per necessità lavorative, esclusivamente sulla risorsa di rete messa a disposizione della Funzione di appartenenza;
- Trattare i dati personali acquisiti nel rispetto delle norme e delle procedure aziendali; Assicurarsi, prima di inviare e/o consentire a colleghi e/o terzi l'accesso ai dati personali dei quali si ha l'autorizzazione al trattamento, che i destinatari abbiano titolo per riceverli, e viceversa;
- Informare tempestivamente il Responsabile del trattamento qualora identifichi o venga informato di una violazione di sicurezza sia essa intenzionale o accidentale (Data Breach);
- Rispettare le misure di sicurezza adottate dal Titolare per la protezione dei dati personali.

3.2.5 AMMINISTRATORE DI SISTEMA (ADS)

L'Amministratore di Sistema è una persona fisica, dipendente dell'azienda, che professionalmente opera nell'ambito dei sistemi informativi, intervenendo sulle componenti hardware e software con il compito di sovraintenderne l'utilizzo.

Tale figura è specificatamente richiesta dalla normativa italiana.
Ha la responsabilità di:

- Concorrere a mantenere gli adeguati livelli di sicurezza del trattamento dei dati;
- Essere parte attiva nella riduzione del rischio di comunicazioni non autorizzate di dati personali;
- Contribuire alla definizione delle policy aziendali di sicurezza, fornendo un feedback di quanto accade nell'operatività quotidiana;
- Adempiere alle altre attività operative previste nell'atto di designazione.

3.2.6 RESPONSABILE ESTERNO DEL TRATTAMENTO

È la persona fisica o giuridica, l'autorità pubblica, il servizio o ogni altro organismo che tratta dati personali per conto del Titolare del Trattamento.
Ha la responsabilità di:

- Trattare i dati personali solo su istruzione documentata del Titolare del Trattamento;
- Adottare tutte le misure di sicurezza previste dal GDPR e dall'atto di nomina del Titolare;
- Assistere il Titolare con misure tecniche e organizzative adeguate a proteggere i dati personali;
- Assistere il Titolare nel garantire il rispetto degli obblighi previsti dal GDPR;
- Garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- Collaborare alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da un altro soggetto da questi incaricato.

3.2.7 INTERESSATO

La persona fisica identificata o identificabile, di cui la Salerno Mobilità Spa tratta i dati personali. Fornisce i propri dati per le finalità di trattamento operate dalla Società sulla base dei relativi criteri di liceità. Inoltre, ha facoltà di richiedere, l'esercizio dei propri diritti: accesso, rettifica, cancellazione ("oblio"), limitazione, portabilità, opposizione, processo decisionale automatizzato (cfr. artt. 15-22 del GDPR).

3.2.8 DESTINATARIO

La persona giuridica o l'ente pubblico o qualsiasi altro organismo che riceve dati personali dalle figure preposte all'interno della Società sulla base di un accordo lecito tra le parti (es. contratto, obblighi di legge, ecc.).

3.2.9 AUTORITÀ DI CONTROLLO

L'autorità pubblica indipendente istituita dai singoli Stati membri ai sensi dell'articolo 51 del Regolamento UE e incaricata di sorvegliare l'applicazione del Regolamento stesso al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione Europea. Con l'obiettivo di garantire il rispetto delle prescrizioni normative da parte dei Titolari e dei Responsabili del trattamento, inoltre, ha facoltà di effettuare ispezioni presso la Società Salerno Mobilità Spa, per verificare la conformità ai requisiti del GDPR e degli altri atti normativi afferenti al trattamento di dati personali.

4.

Pianificazione

Allo scopo di realizzare, attuare e migliorare costantemente il nostro Sistema di Gestione Privacy, ci siamo impegnati a definire e attuare processi operativi vincolanti, adattati allo specifico contesto della Società e coerenti con i principi espressi dal GDPR.

4.1 Soluzioni organizzative adottate per il rispetto dei Principi

Allo scopo di realizzare, attuare e migliorare costantemente il proprio Sistema di Gestione Privacy, finalizzato a tutelare le libertà e i diritti degli Interessati nel pieno rispetto del principio di accountability, la Salerno Mobilità Spa **si impegna a:**

- **diffondere la cultura della privacy nella Società diretta a tutto il personale,** coinvolgendo i dipendenti e facendo acquisire loro la consapevolezza dell'importanza delle attività lavorative che compiono in merito ad operazioni di trattamento dei dati e sensibilizzandoli al riconoscimento dei diritti degli Interessati e alla necessità di tutelare e garantire tali diritti;
- **definire ed implementare un Sistema di Gestione Privacy che preveda la definizione e l'attuazione di processi operativi vincolanti e coerenti con i requisiti del GDPR** e adattato allo specifico contesto della Società;
- **effettuare riesami periodici del Sistema di Gestione,** al fine di verificare che le operazioni di trattamento dati avvengano nel rispetto di quanto prescritto dal Sistema di Gestione Privacy e valutarne le prestazioni coerentemente con gli obiettivi prefissati;
- **garantire la disponibilità di adeguate risorse finanziarie e strumentali.**

Per conseguire tali risultati, la Società si è dotata di uno specifico assetto organizzativo, illustrato in precedenza, che definisce i ruoli e le responsabilità delle figure coinvolte a vario titolo nei trattamenti di dati personali effettuati.

4.2 Principi e Metodologie

4.2.1 PRINCIPI

4.2.1.1 *Accountability o Responsabilizzazione del Titolare*

La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'art. 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione Europea e l'art. 16, paragrafo 1, del trattato sul funzionamento dell'Unione Europea stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. **In tale contesto, la Salerno Mobilità Spa pone con forza l'accento sulla propria "responsabilizzazione" (accountability nell'accezione inglese) in qualità di Titolare, ossia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare la tutela degli Interessati** (cfr. in particolare artt. 23-25 e l'intero Capo IV del GDPR). Spetta al Titolare effettuare l'analisi dei rischi per gli interessati, derivanti dalla gestione del dato e determinare le contromisure tecniche ed organizzative opportune (es. valutazione di scenari alternativi, con approccio Risk Based), ecc.

Fondamentali sono le attività connesse alla gestione del rischio inerente al trattamento, da intendersi come rischio di impatti negativi sulle libertà e i diritti degli Interessati (cfr. Considerando 75-77); il Titolare dovrà valutare gli impatti sugli Interessati e, laddove decida di iniziare il trattamento, adottare adeguate contromisure per mitigarli. Da quanto illustrato consegue che le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (cfr. art. 32, paragrafo 1 del GDPR); pertanto, viene meno il concetto di misure "minime" di sicurezza (ex art. 33 Codice Privacy), poiché la valutazione di adeguatezza sarà rimessa, caso per caso, al Titolare in rapporto ai rischi specificamente individuati.

4.2.1.2 *Principio di Liceità del trattamento*

La Salerno Mobilità Spa garantisce che i dati personali siano trattati secondo i principi applicabili al trattamento di dati personali definiti dal GDPR (Art. 5), già menzionati (Cifrazione 5.1)
I fondamenti di liceità del trattamento, definiti nell'art. 6 del GDPR, sussistono solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

- l'Interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
- il trattamento è necessario all'esecuzione di un contratto di cui l'Interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'Interessato o di un'altra persona fisica;
- il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
- il trattamento è necessario per il perseguimento del legittimo interesse del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'Interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

4.2.1.3 *Approccio basato sul rischio*

La Salerno Mobilità Spa, tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche mette in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio.
Quando si parla di "rischio" nell'ambito della normativa privacy, si fa riferimento a due accezioni distinte:

a) Il rischio che incombe sui diritti e le libertà fondamentali delle persone fisiche a seguito del trattamento dei propri dati personali effettuato da un Titolare o da un Responsabile. Tale rischio può essere ulteriormente declinato in "rischio privacy" e "rischio di sicurezza": il primo viene valutato in termini di impatto potenziale sugli Interessati attraverso l'analisi del contesto in cui è effettuato il trattamento e dalla presenza di alcune caratteristiche dello stesso (es. valutazione o assegnazione di un punteggio, monitoraggio sistematico, ecc.); il secondo esprime invece il livello di esposizione alle minacce che incombono sugli asset attraverso cui viene effettuato il trattamento;

b) Il rischio, inteso come minaccia che impatta sulla privacy delle persone, preso in considerazione all'interno di una cultura basata sul rischio -"risk-based thinking"- che prevede la definizione ed implementazione di metodologie, soluzioni tecnico-organizzative, contromisure di sicurezza necessarie ad una corretta gestione degli adempimenti del Regolamento. Tale approccio è, peraltro, in linea con gli standard ISO, che pongono un'attenzione cruciale verso il risk-based thinking e la sua centralità nei processi previsti dalle diverse normative.

Il livello di rischio è stimato in termini di impatto e probabilità:

- l'impatto rappresenta l'entità dei potenziali effetti di un rischio per l'interessato;
- la probabilità che si verifichi un rischio dipende dal livello delle vulnerabilità degli asset di supporto che devono far fronte alle minacce e dal livello di capacità delle fonti di rischio di sfruttarle.

La probabilità è pertanto modulabile con i controlli implementati, mentre gli impatti dipendono esclusivamente dalle caratteristiche del trattamento effettuato.

4.2.1.4 *Principio di Privacy by Design e Privacy by Default*

La Salerno Mobilità Spa rispetta i principi di "privacy by design" e di "privacy by default" (cfr. art. 25 del GDPR), ovvero la "protezione dei dati fin dalla progettazione" e la "protezione dei dati per impostazione predefinita".

Per rispettare il principio di "privacy by design", è necessario identificare la presenza di eventuali trattamenti di dati personali nelle iniziative aziendali di competenza delle Direzioni/ Funzioni, quali a titolo esemplificativo:

- avvio di nuovi progetti;
- introduzione di nuovi processi o re-ingegnerizzazione di processi esistenti; implementazione di nuovi applicativi;
- prevenzione di incidenti di sicurezza o in generale in ambito IT.

Tutte le strutture aziendali sono sensibilizzate, tramite sessioni formative e specifiche comunicazioni, a considerare gli impatti privacy derivanti dalle proprie attività.

Anche la definizione, formalizzazione ed attuazione del Sistema di Gestione Privacy rientra tra le misure preventive che contribuiscono a progettare ed effettuare "by design" i trattamenti di dati personali in conformità con i requisiti del GDPR.

Per rispettare il principio di privacy by design, le strutture aziendali per le nuove attività di trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, tengono conto:

- dello stato dell'arte e dei costi di attuazione;
- della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento;
- dei rischi aventi probabilità e impatto diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento.

Valutati gli aspetti sopra, la Salerno Mobilità Spa pone in atto misure tecniche e organizzative adeguate. Nel paragrafo successivo relativo alle misure di sicurezza si descrivono quelle adottate dalla Salerno Mobilità Spa per la protezione dei dati personali.
Il rispetto del principio di privacy by design impone inoltre di considerare tale principio in tutti i processi in cui è previsto un trattamento di dati personali che sia impattato da cambiamenti di tipo organizzativo, tecnologico e/o di processo.
Il rispetto del principio di "privacy by default" è garantito dalla progettazione ed implementazione dei trattamenti di dati personali con l'obiettivo di raggiungere il principio di minimizzazione dei dati, ossia la raccolta, la conservazione e l'utilizzo dei soli dati personali necessari per raggiungere la specifica finalità di trattamento considerata, questo anche secondo il principio di limitazione della finalità. Il rispetto del principio di "privacy by default" è inoltre garantito dalla implementazione di misure tecniche e organizzative adeguate affinché sia garantita, per impostazione predefinita, la protezione dei dati personali.

4.2.2 METODOLOGIE

4.2.2.1 *Registro delle Attività di Trattamento*

L'art. 30 del Regolamento (EU) n. 679/2016 prevede tra gli adempimenti principali del Titolare e del trattamento la tenuta del registro delle attività di trattamento.
Il Registro dei Trattamenti costituisce uno dei principali elementi di accountability del Titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività. Non rappresenta soltanto un adempimento normativo ma un vero e proprio strumento di gestione, comprensione e auto valutazione e da molti punti di vista può essere interpretato come una componente centrale e cardine di tutto il Sistema di Gestione Privacy.
La Salerno Mobilità Spa ha realizzato il Registro dei Trattamenti su di una piattaforma elettronica che consente di soddisfare i principali requisiti di compliance e sicurezza delle informazioni, nonché requisiti circa le modalità di conservazione e aggiornamento dello stesso.
In ottica di compliance al GDPR, il portale adottato consente infatti di:

- effettuare accessi sicuri al registro: ogni utente accede ai documenti a seconda del livello di autorizzazione impostato, permettendo così l'accesso anche a personale esterno al gruppo, garantendo comunque la riservatezza dei dati in esso contenuti.
- gestire gli aggiornamenti del registro;
- favorire la collaborazione e il contributo di tutte le figure coinvolte nell'organizzazione privacy alla gestione e aggiornamento del Registro dei trattamenti, contribuendo all'accountability del Titolare, ognuno per le proprie competenze e responsabilità;
- dotare la Società di un'unica struttura di archiviazione dei trattamenti operati sulle singole realtà aziendali, rendendo omogeneo il patrimonio informativo sulla data protection.

La struttura del Registro è stata predisposta alla luce dell'art. 30 del GDPR, e contiene le seguenti informazioni:

- Registro del Titolare:
  - il nome e i dati di contatto del Titolare del trattamento;
  - le finalità del trattamento;
  - una descrizione delle categorie di interessati e delle categorie di dati personali;
  - le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
  - ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale;
  - ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
  - ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art. 32, paragrafo 1.

Il processo di corretta tenuta del Registro delle attività di trattamento, in termini di gestione, aggiornamento e monitoraggio dello stesso, è parte integrante del Sistema di Gestione Privacy.

4.2.2.2 *Diritti degli Interessati*

La tutela degli Interessati è centrale nel Sistema di Gestione Privacy della Salerno Mobilità Spa. Gli Interessati sono, di fatto, i proprietari dei dati personali oggetto di trattamento per l'esecuzione delle finalità concordate, nel rispetto dei diritti e delle libertà fondamentali.
Gli Interessati hanno diritto alla protezione dei propri dati personali.
Tale tutela deve essere garantita dal Titolare anche in caso di dati personali non ottenuti presso l'Interessato.
In tale scenario, la Società garantisce agli Interessati l'esercizio dei seguenti diritti:

- **Accesso** - L'Interessato ha il diritto di ottenere dal Titolare la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle relative informazioni;
- **Rettifica** - L'Interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo;
- **Cancellazione** - L'Interessato ha il diritto di ottenere dal Titolare la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo, nei casi previsti dalla norma;
- **Limitazione del trattamento** - L'Interessato ha il diritto di ottenere dal Titolare la limitazione del trattamento, se sussistono le condizioni previste dal Regolamento;
- **Portabilità** - L'Interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti al Titolare e ha il diritto di trasmettere tali dati a un altro Titolare senza impedimenti;
- **Opposizione** - L'Interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, compresa la profilazione;
- **Revoca del consenso** - L'Interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca;
- **Esenzione da trattamenti automatizzati**, compresa la profilazione, che producano effetti giuridici che riguardano gli Interessati o che incidano in modo analogo significativamente sulle loro persone.

Tali istanze, come prevede il Regolamento UE, sono riscontrate entro un mese dalla ricezione della richiesta, estendibile fino a 3 mesi in casi di particolare complessità. La Società adotta misure appropriate per fornire all'Interessato le informazioni in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.
Il riscontro all'Interessato avviene in forma scritta anche attraverso strumenti elettronici.

4.2.2.3 *Informative agli interessati*

Il regolamento europeo prevede che, in base alla finalità del trattamento, il Titolare debba fornire agli Interessati una informativa ogni qual volta vi sia un trattamento di dati. Questa è una comunicazione rivolta all'interessato che ha lo scopo di informare lo stesso sulle finalità e le modalità dei trattamenti operati dal Titolare del trattamento, nonché di permettere che l'Interessato possa rendere un valido consenso, se richiesto come base giuridica del trattamento.
La Salerno Mobilità Spa attraverso l'informativa specifica la propria identità, le finalità del trattamento, i diritti degli Interessati, quali sono i destinatari dei dati, i dati di contatto del Titolare, la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti di garanzia. Inoltre, al fine di garantire un trattamento corretto e trasparente specifica il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'autorità di controllo competente.
In tutti i casi l'Informativa deve avere una forma concisa, trasparente, intelligibile per l'Interessato e facilmente accessibile che prevede l'utilizzo di un linguaggio chiaro e semplice.
L'obbligo di fornire agli interessati le informazioni e le comunicazioni in forma "concisa e trasparente" implica, così come raccomandato nella presente Policy, proponga all'Interessato le informazioni/comunicazioni in maniera efficace e succinta e distinte chiaramente da altre, quali ad esempio clausole contrattuali o condizioni generali d'uso.

Come previsto dagli Artt. 13 e 14 del GDPR la Salerno Mobilità Spa fornisce l'Informativa all'Interessato prima di effettuare la raccolta dei dati, se gli stessi sono raccolti direttamente presso l'Interessato. Se invece i dati non sono raccolti direttamente presso l'Interessato, l'Informativa è fornita dalla Società entro un termine ragionevole.

4.2.2.4 *Data Protection Impact Assessment*

Come espressamente richiesto dal GDPR, "il Titolare effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali (Data Protection Impact Assessment)", ove ritenuto necessario.
Un Data Protection Impact Assessment (DPIA) è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando tali rischi e determinando le misure per affrontarli.
Il DPIA è uno strumento indispensabile per dimostrare l'adozione di misure appropriate per garantire il rispetto del Regolamento. In altre parole, *una valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità*. La realizzazione di un DPIA

è obbligatoria ogni qualvolta il trattamento "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche".
Il processo di Data Protection Impact Assessment (DPIA) è attivato a seguito di:

- Introduzione di nuovi trattamenti nell'ambito di nuovi processi e/o nuove attività aziendali;
- Importanti revisioni del modello organizzativo, con effetti su processi e relativi trattamenti;
- Nuovi servizi informativi e/o modifica dei servizi informatici in essere a supporto di trattamenti esistenti;
- Variazioni significative a Trattamenti in essere.

Una volta attivato il processo è compito del Titolare determinare il rischio inerente al trattamento analizzando gli impatti potenziali sugli Interessati attraverso un apposito processo di valutazione che tenga conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il Titolare ritiene di dover adottare per mitigare tali rischi.
Una corretta esecuzione del processo di DPIA prevede le seguenti fasi:

- Descrizione sistematica del trattamento:
  - sono presi in considerazione la natura, l'ambito di applicazione, il contesto, i princìpi di liceità e le finalità del trattamento;
  - sono registrati i dati personali, i destinatari e il periodo di conservazione dei dati personali;
  - viene fornita una descrizione funzionale del trattamento;
  - sono individuate le risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea).

- Valutazione delle necessità e della proporzionalità del trattamento:
  - sono determinate le misure previste per garantire il rispetto del Regolamento.

- Gestione dei rischi per i diritti e le libertà degli interessati:
  - l'origine, la natura, la particolarità e la gravità dei rischi o, più in particolare, per ciascun rischio (accesso illegittimo, modifica indesiderata e perdita dei dati) vengono determinate dalla prospettiva degli Interessati, comprese le tutele circa il formato di Informative e Consensi e l'esercizio dei diritti da parte degli interessati;
  - sono determinate le misure previste per gestire tali rischi.

- Determinazione di eventuali azioni correttive e validazione del trattamento:
  - si identificano le azioni di miglioramento che si rendono necessarie per mitigare i possibili rischi per l'interessato e si effettua la validazione da parte del Titolare della DPIA.

Si tratta di un processo di miglioramento continuo, pertanto, può richiedere diverse iterazioni per ottenere un sistema accettabile di protezione. Richiede, inoltre, un monitoraggio periodico e aggiornamenti ogni qualvolta si verifichi un cambiamento significativo.
Ogni processo di DPIA, per essere accettabile, deve contenere alcune informazioni considerate come requisiti minimi; l'approccio adottato dalla Società coniuga la metodologia della CNIL (Commission Nationale de l'Informatique et des Libertés), l'Autorità francese per la protezione dei dati, con quanto indicato nell'Allegato 2 delle Linee Guida del WP29, al fine di avere un riferimento riconosciuto ed autorevole per garantire la conformità al Regolamento.

4.2.2.5 *Misure di sicurezza*

La Salerno Mobilità Spa implementa un insieme di misure di sicurezza tecniche ed organizzative che garantiscono un livello minimo di protezione per tutti i dati ed i trattamenti. Tali misure consistono, a titolo esemplificativo, in:

- impianto documentale (policy, procedure, istruzioni operative, ecc.);
- assetto organizzativo (ruoli e responsabilità formalizzati, gestione delle competenze delle risorse, ecc.);
- definizione ed attuazione di processi di business e di supporto strutturati;
- certificazione rispetto a diversi standard internazionali (qualità, sicurezza delle informazioni);
- definizione ed attuazione - in ambito IT - di processi ispirati alle leading practices nei principali ambiti operativi (gestione dei cambiamenti, gestione della sicurezza e degli accessi, gestione dell'esercizio);
- implementazione di soluzioni tecnologiche robuste a supporto della gestione della sicurezza dei dati (autenticazione tramite user e password per l'accesso ai sistemi, sistemi di sicurezza perimetrale, backup automatizzati, ecc.).

Le misure di sicurezza rappresentano un presidio di sicurezza applicato, a supporto del principio di privacy by default, a tutti i dati trattati dalla Società, ivi inclusi quelli personali, e sono adeguate a tutelare i trattamenti che non presentano un elevato rischio per gli Interessati.

In accordo con l'approccio basato sul rischio e con le prescrizioni del GDPR, la Salerno Mobilità Spa ha identificato livelli di protezione specifici per i dati personali da applicare a ciascun tratta- mento in base alla relativa rischiosità. In particolare, sono stati identificati i seguenti livelli di protezione, suddivisi in Misure Organizzative e Tecniche:

Misure Organizzative

- *Politiche per la sicurezza e procedure per la protezione dei dati personali:* la Società adotta un impianto documentale e un Sistema di Gestione della Sicurezza delle Informazioni. Inoltre, sono presenti e sono seguite delle procedure operative per i più importanti processi di gestione ed erogazione dei sistemi informativi che tengono conto delle diverse strategie di sicurezza adottate.
- *Ruoli e responsabilità:* la Società definisce i ruoli e le responsabilità relativi alla sicurezza delle informazioni con particolare riguardo al trattamento dei dati personali;
- *Politica di controllo degli accessi:* per ciascun ruolo coinvolto nel trattamento di dati personali, sono identificati profili di autorizzazioni diversificati, in base al principio del minimo privilegio e necessità per il ruolo di accedere e conoscere i dati;
- *Gestione delle risorse e degli asset:* la Società censisce le risorse IT utilizzate per il trattamento dei dati personali all'interno di un registro degli asset informatici; le risorse IT sono riviste e aggiornate regolarmente;
- *Gestione degli incidenti e delle violazioni dei dati personali:* in materia di incidenti di sicurezza sui dati personali la Società realizza, e diffonde a tutti gli Incaricati del trattamento, le procedure operative per l'identificazione e la gestione degli eventuali "data breach".
- *Continuità operativa:* la Società adotta le procedure ed i controlli da eseguire per garantire il necessario livello di continuità e disponibilità del sistema IT su cui si effettuano i trattamenti di dati personali.
- *Riservatezza del personale:* la Società garantisce che tutte le persone autorizzate al tratta- mento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati persona- li oggetto del trattamento da essi svolto.

- *Formazione:* la Società assicura che tutti gli incaricati del trattamento siano adeguatamente formati e informati in merito ai requisiti e agli obblighi legali in materia di protezione dei dati attraverso regolari campagne di sensibilizzazione o iniziative di formazione specifica.
- *Sicurezza fisica:* la Società utilizza delle chiare politiche di accesso fisico e protezione delle risorse materiali dell'azienda.

Misure Tecniche

Gestione dei cambiamenti: la Società, tramite opportune procedure, assicura che tutte le modifiche al sistema IT siano registrate, classificate, valutate, autorizzate e pianificate anche tenendo conto degli standard di sicurezza adottati. Il monitoraggio di questo processo viene fatto regolarmente.

- *Raccolta di log e monitoraggio:* la Società assicura il controllo proattivo dell'implementazione della sicurezza tramite un adeguato livello di protezione dei dati personali e una rapida prevenzione, rilevazione e rendicontazione di attività inusuali e/o anormali;
- *Backup:* la Società definisce e documenta le procedure di backup e ripristino dei dati; il backup dei dati è realizzato regolarmente, coerentemente con quanto richiesto dai fabbisogni della Società;
- *Sicurezza dei server, dei database e delle postazioni di lavoro:* la Società assicura la protezione degli apparati mediante l'adozione di misure di sicurezza adeguate;
- *Sicurezza di reti e comunicazioni:* la Società utilizza tecniche e strumenti di sicurezza e le relative procedure di gestione (e.g. firewalls, dispositivi di sicurezza, segmentazione della rete e rilevazione delle intrusioni) per autorizzare l'accesso ed il controllo del flusso di informazioni da e per la rete aziendale, anche tramite canale cifrato (e.g. VPN) per gli accessi da remoto;
- *Cancellazione e dismissione dei dati:* la Società assicura che i documenti ed i supporti che contengono dati personali, al termine del periodo di retention definito, o sulla base delle richieste fatte dagli interessati devono essere "cancellati" o distrutti in maniera sicura, secondo la normativa vigente.

4.2.2.6 *Relazione con le terze parti*

All'interno della categoria "terze parti" rientra "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 o del responsabile."
Il Regolamento Europeo in particolare distingue tra:

- **Destinatario:** la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.
- **Contitolari del trattamento:** quando due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informative.
- **Responsabile Esterna del Trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o ogni altro organismo che tratta dati personali per conto di un Titolare del Trattamento.

Per quest'ultima categoria, la Società si impegna a nominare Responsabili del trattamento, ai sensi dell'art.28 del GDPR, tutte le società fornitrici che trattano dati personali per conto del Titolare, mediante un apposito contratto o atto giuridico scritto.

4.2.2.7 *Data Breach Notification*

Un Data Breach, o violazione dei dati personali, è un evento che provoca la perdita di riservatezza, integrità o disponibilità dei dati personali trattati dalla Salerno Mobilità Spa. Il GDPR lo definisce (cfr. art. 4) come "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati". Una violazione dei dati personali è tale anche se i suoi effetti sono temporanei e non permanenti.
I possibili impatti per gli Interessati derivanti da un Data Breach possono includere, tra gli altri, perdita di controllo sui propri dati personali, limitazione dei propri diritti, discriminazione, frode, furto di identità, perdite finanziarie, danni reputazionali, ecc.
Nell'ambito del Sistema di Gestione Privacy, la Salerno Mobilità Spa implementa adeguate misure tecniche ed organizzative per prevenire il verificarsi di Data Breach (cfr. par. Misure di sicurezza), nel rispetto dei principi di privacy by design e by default e, nel caso in cui una violazione venga rilevata, per reagire ad essa in modo tempestivo ed efficace.
In particolare, è stato definito un processo di gestione delle notifiche di violazioni di dati personali, atto a garantire la tempestiva comunicazione di un Data Breach al Garante e, ove necessario, anche agli Interessati, nonché l'attuazione delle attività richieste per contenere l'incidente e ripristinare le normali condizioni operative.
Il Data Breach va comunicato dal Titolare all'Autorità di Controllo entro 72 ore dalla rilevazione, e senza ingiustificato ritardo agli Interessati laddove comporti un elevato rischio per i diritti e le libertà degli stessi (cfr. artt. 33-34 del GDPR), eventuali ritardi saranno evidenziati con le relative motivazioni. L'attenzione è posta sulla pronta investigazione di ciascun incidente per determinare il possibile impatto sui dati personali e le appropriate azioni di remediation al fine di limitare i danni per gli Interessati. Per i trattamenti di cui la Salerno Mobilità Spa è Responsabile, l'Azienda notificherà la rilevazione di un Data Breach al Titolare, senza ingiustificato ritardo.
È opportuno notare che la valutazione del rischio svolta a seguito di un Data Breach ha un focus differente da quella effettuata nell'ambito di un DPIA:

- il DPIA considera sia il rischio che il trattamento non sia effettuato secondo le modalità previste che i rischi derivanti da una eventuale violazione. Quando si considera una potenziale violazione, si esamina in termini generali la probabilità che ciò si verifichi e i conseguenti impatti per gli Interessati. Si tratta quindi di una valutazione di un evento ipotetico;
- A seguito di un Data Breach, invece, l'evento si è già verificato realmente, e quindi l'attenzione è posta interamente sul rischio derivante dall'effettivo impatto della violazione sulle persone.

Nel rispetto del principio di accountability, la Salerno Mobilità Spa documenta tutti i Data Breach rilevati e le conseguenti attività di investigazione, valutazione del rischio, notifica e remediation, tramite apposito registro.

4.3 Formazione e Sensibilizzazione Privacy

Il principio di accountability impone alla Salerno Mobilità Spa anche l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che effettua i trattamenti e alle connesse attività di controllo. **La Società riconosce il valore della comunicazione quale strumento fondamentale al fine della diffusione ed attuazione delle buone pratiche, con particolare riferimento al trattamento dei dati personali. A tal fine, la Società realizza iniziative periodiche e strutturate di formazione e sensibilizzazione volte ad innalzare la cultura della privacy in azienda e ad aumentare il livello di consapevolezza del personale.**
I processi di diffusione, comunicazione e formazione sulla Normativa Privacy, avvengono tramite diversi canali, come ad esempio:

- Iniziative periodiche di formazione obbligatoria sulle tematiche privacy sia per gli aspetti normativi che per quelli operativi. Tali iniziative sono rivolte sia a tutta la popolazione aziendale, per una generale promozione e diffusione delle buone pratiche, sia al personale che partecipa direttamente ai trattamenti.

4.4 Informazioni documentate

Il Sistema di gestione Privacy rende disponibili, in formato elettronico e/o cartaceo, le informazioni utili al fine di:

- dare evidenza di come viene assicurato il raggiungimento degli obiettivi;
- garantire tutte le informazioni necessarie per la gestione ed il controllo dei processi;
- fornire al personale la documentazione necessaria per lo svolgimento dei compiti assegnati.

La documentazione aziendale rilevante ai fini della privacy e alla dimostrazione dell'"Accountability" del Titolare è la seguente:

- Manuale del Sistema di Gestione della Privacy
- Registro dei trattamenti del Titolare;
- Nomina del DPO;
- Nomina del Responsabile del trattamento;
- Nomine degli incaricati Privacy;
- Registro delle richieste relative all'esercizio dei diritti da parte degli Interessati;
- Registro dei Data Breach;
- Notifica dei Data Breach al Garante Privacy (eventuale);
- Notifica dei Data Breach agli Interessati (eventuale);ù
- Informative;

4.5 Pianificazione e Controlli Operativi

La Società Selamatic Spa pianifica, implementa e controlla i processi idonei a soddisfare i requisiti relativi al Sistema di Gestione della Privacy.
Il primo tipo di controllo si realizza attraverso un Audit per verificare l'applicazione dei Principi, Metodologie e Procedure predisposti tenendo, tra l'altro, in considerazione le Policy e le Linee Guida.
È in capo al Responsabile il compito di verificare che il personale della propria struttura incaricato del trattamento di dati personali svolga le attività nel rispetto dei presidi contenuti nei sopra menzionati documenti.

5.

Valutazione

Ci siamo dotati di un modello di monitoraggio che analizza la conformità della Policy. Monitoriamo gli obiettivi sistematicamente sulla base di un piano definito periodicamente dalle funzioni interessate; in base all'esito delle valutazioni definiamo opportune azioni correttive e/o di miglioramento.

5.1 Monitoraggio, misurazione, analisi e valutazione

La Società Salerno Mobilità Spa si accerta che l'organizzazione sia conforme al Regolamento Europeo e a tutta la normativa in materia di tutela dei dati personali.
Per raggiungere tali obiettivi **la Società si è dotato di un modello di monitoraggio che analizza la conformità tramite il Responsabile Privacy. Gli obiettivi sono monitorati sistematicamente sulla base di un piano definito periodicamente dalle funzioni interessate.**

In base all'esito delle valutazioni sul raggiungimento degli obiettivi, si definiscono opportune azioni correttive e/o di miglioramento, da sottoporre alla valutazione ed approvazione del CDA/AD. Per le azioni correttive pianificate sono identificate le responsabilità ed i tempi di attuazione.

5.1.1 MONITORAGGIO DELLA CONFORMITÀ

Il Responsabile Privacy ed il DPO effettuano un monitoraggio relativo al controllo della corretta applicazione della normativa interna implementata (linee guida, principi, metodologie, procedure, policy), della normativa europea e di quella nazionale, allo scopo di verificarne l'efficacia, mediante l'esecuzione delle attività di monitoraggio previste nel piano.
I controlli operativi oggetto della verifica da parte del Responsabile Privacy sono programmati e concordati con il Responsabile del Trattamento, anche per recuperare la documentazione di supporto utile alle attività di verifica. A seguito della verifica stessa, il Responsabile Privacy unitamente al DPO redigono un report di audit con gli esiti del monitoraggio che condivide con il Titolare del Trattamento.

5.2 Miglioramento continuo

5.2.1 RIESAME DELLA DIREZIONE

Periodicamente il Responsabile esamina il Sistema di Gestione della Privacy e i punti di miglioramento individuati e valutati dal Responsabile Privacy in collaborazione con gli incaricati del Trattamento, in quanto ciò rappresenta il primo passo per mantenere vivo il processo di miglioramento continuo.
A questa verifica si aggiunge un periodico riesame delle possibili azioni correttive conseguenti ai risultati dei controlli e dei monitoraggi interni e la definizione di obiettivi per le strutture aziendali coinvolte nella gestione della Privacy.
Il riesame prevede le seguenti fasi:

- verifica del raggiungimento degli obiettivi annuali di monitoraggio e formazione;
- valutazione degli scostamenti; formulazione dei nuovi obiettivi;
- eventuali richieste di modifica del Sistema di Gestione per la Privacy.

Firma del Titolare del trattamento
Salerno Mobilità S.p.A.
Amministratore Unico
Camillo Amodio