SISTEMA SANITARIO REGIONALE
ASL ROMA 5

INFORMAZIONI PRIVACY SISTEMI GPS ISTALLATI SULLE AUTOVETTURE AZIENDALI, AI SENSI DELL'ART. 13 GDPR

SCUDOMED Srl

Finalità del trattamento: monitoraggio da remoto degli autoveicoli aziendali per la sicurezza del patrimonio aziendale, l'incolumità dei lavoratori e la prevenzione di atti illeciti.

Base giuridica: art. 6, par. 1, lett. f), in quanto il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento.

Destinatari del trattamento:

- dipendenti del Titolare da quest'ultimo autorizzati;
- Amministratori di sistema;
- Responsabili del trattamento nominati;
- Enti, Organismi, Autorità verso i quali il Titolare del trattamento ha un obbligo di comunicazione previsto dalla legge.

Periodo di conservazione: i dati personali verranno conservati per un periodo congeniale alla realizzazione delle finalità del trattamento.

Diritti dell'interessato: l'interessato dispone dei diritti di cui all'art. 15 GDPR e ss., più precisamente, diritto di accesso, diritto di rettifica, diritto di limitazione di trattamento, diritto di opposizione, nonché il diritto di proporre reclamo all'Autorità Garante (art. 77 GDPR e 141 Codice Privacy e ss. mm. ii.).

Titolare del trattamento: Azienda Sanitaria Locale Roma 5, con sede legale in Via Acquaregna n.1/15 - 00019 – Tivoli (RM) - C.F. /P.IVA 04733471009, in persona del Direttore Generale, Dr. Giorgio Giulio Santonocito.

E-mail: protocollo.generale@aslroma5.it

PEC: protocollo@pec.aslromag.it

Data Protection Officer (DPO): Scudo Privacy S.r.l., nella persona del Dott. Carlo Villanacci

E-mail: dpo@scudoprivacysrl.com

DPIA
ex art. 35 GDPR

INDICE

IL CONTESTO NORMATIVO DEL DATA PROTECTION IMPACT ASSESSMENT

Il *Data Protection Impact Assessment* (per brevità anche DPIA) è uno strumento importante in termini di responsabilizzazione *(principio di accountability),* in quanto soccorre e sostiene il Titolare del trattamento non soltanto nel rispettare e far rispettare le prescrizioni del GDPR, ma anche nel dimostrare di aver adottato le misure idonee a mitigare il rischio durante tutte le fasi trattamentali. In altri termini, la Valutazione d'Impatto sulla Protezione dei Dati è una procedura di *risk management* che permette di dimostrare la conformità con le norme in materia di protezione dei dati personali europee e domestiche. Muovendo i passi dal dettato normativo, segue il testo dell'art. 35 GDPR:

"ART. 35

Valutazione d'impatto sulla protezione dei dati

Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi."

La disciplina sul *DPIA,* contenuta nel GDPR, deve essere integrata anche da quanto specificato dal *WP29* (oggi *European Data Protection Board* - EDPB) nelle linee guida concernenti la valutazione di impatto sulla protezione dei dati, nonché i criteri per stabilire se un trattamento possa o meno presentare un rischio privacy più o meno elevato.

In particolare, le linee guida citate ampliano l'obbligatorietà della valutazione di impatto, oltre ai casi espressamente indicati dal regolamento all´art. 35, par. 3, GDPR, anche in quelli che comportano la comunicazione di dati su larga scala tra diversi titolari e/o trattamenti

sistematici di dati genetici o sanitari, tenendo conto del volume dei dati, della durata e dell'attività di trattamento.

Il presente documento è, inoltre, uno strumento dedicato alla valutazione del rischio ed ha lo scopo di fornire informazioni basate sia su evidenze che su metodi di analisi, al fine di rendere agevole l'adozione di decisioni informate circa il trattamento di particolari rischi.
Le informazioni ottenute consentono, quindi, di identificare i fattori determinanti, gli eventi potenzialmente dannosi e suggerire le azioni correttive possibili da mettere in atto per prevenire la ripetizione degli eventi stessi.
Nella prospettiva della gestione del rischio privacy, tale documento risponde al principio fondamentale dell'*accountability*, intesa quale dimostrazione di come il titolare del trattamento abbia posto in essere tutte le misure di sicurezza volte a tutelare i diritti e le libertà degli interessati.

La responsabilizzazione, quale obbligo di rendere conto di ciò che si fa e ciò che si fa fare, rappresenta il fulcro della nuova frontiera della privacy in quanto aspetto essenziale per l'esercizio di una corretta ed efficace *governance*.

Il Regolamento UE 2016/679 pone, altresì, la necessità di rendere conto anche dell'adozione di comportamenti proattivi, tali da "*dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del GDPR*" (artt. 23-25, in particolare, e l'intero Capo IV del GDPR).

Ne consegue, dunque, che è affidato al Titolare del trattamento dei dati il compito di decidere autonomamente le modalità, le misure di sicurezza e i limiti del trattamento stesso, nel rispetto delle disposizioni normative ed alla luce dei criteri indicati nel Regolamento UE, oltre che a quelli indicati dall'ordinamento interno (Codice Privacy - D.lgs. 196/2003 ss.mm.ii.) e rispetto alle Linee Guida e Regole Deontologiche previste dal Garante per la Protezione dei Dati Personali.

Il primo fra tali criteri è sintetizzato dall'espressione inglese "*data protection by design and by default*" (art. 25 GDPR), ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio e per impostazione predefinita le garanzie indispensabili al fine di soddisfare i

requisiti del Regolamento stesso e tutelare i diritti e le libertà degli interessati, tenendo conto del contesto complessivo ove il trattamento viene svolto e dei rischi connessi.

Fondamentali fra tali attività sono quelle relative al successivo criterio del rischio inerente al trattamento; quest'ultimo è da ritenersi, infatti, come il rischio capace di impattare negativamente sulle libertà e sui diritti degli interessati (considerando 75-77).

Tali criticità dovranno essere analizzate attraverso un apposito processo di valutazione (artt. 35 e 36 GDPR) tenendo conto dei rischi noti o ipotizzabili e delle misure tecniche, fisiche e organizzative che il Titolare ritiene di dover adottare per mitigare tali rischi.

In ossequio a tali criteri, il presente documento viene redatto in base alle tecniche ed alle modalità della norma ISO/IEC 31000:2018, "*Risk Management – Principles and guidelines*", che descrive in dettaglio il processo logico e sistematico che porta alla mitigazione e controllo dei rischi.

La *ratio* della scelta risiede nella necessità di conferire connotati positivi alla gestione del rischio, anche attraverso la percezione dello stesso come opportunità, mediante una lettura del pericolo quale possibilità di innovazione.

Ulteriore ed importante elemento di valutazione è il contenuto dello standard ISO/IEC 31010:2009 (*Risk Management e Risk Assessment Techniques*) ove vengono riportati i concetti della gestione dei rischi e le diverse tecniche atte alla loro valutazione nei diversi ambiti.

È, infine, doveroso adeguarsi alle disposizioni contenute nelle norme:

- ISO/IEC 29134:2017 ("*Information technology – Security techniques – Guidelines for privacy impact assessment*") che indica linee guida applicabili a tutte le tipologie di strutture, pubbliche e private, al fine di creare, organizzare ed implementare progetti GDPR *compliant*;

- ISO/IEC 27002:2017 ("*Information Technology - Security techniques - Code of practice for information security controls*") che indica le linee guida per gli standard di sicurezza delle informazioni organizzative e pratiche di gestione della sicurezza delle informazioni, compresa la selezione, l'implementazione e la gestione dei controlli;

- ISO/IEC 27005:2018 ("*Information security risk management*") che, è in parte applicabile anche alla valutazione del rischio connesso al trattamento dei dati

personali; assumono importanza determinante le appendici dedicate all'approfondimento di alcuni aspetti della gestione dei rischi e, in particolare, quella relativa al catalogo delle minacce;

- ISO/IEC 27701:2019 ("*Security techniques -- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -- Requirements and guidelines*") che fornisce requisiti e linee guida per costruire, implementare, mantenere e migliorare costantemente un PIMS (*Privacy Information Management System* o sistema di gestione delle informazioni sulla privacy), sia qualora l'organizzazione operi come titolare del Trattamento (*Data Controller*), che come Responsabile (*Data Processor*).

- ISO 31000:2018 ("Risk management -- Principles and guidelines") fornisce principi e linee guida generali per la gestione del rischio ed è applicabile a tutte le tipologie di organizzazioni. La ISO 31000 può essere applicata a qualsiasi tipo di rischio e nel corso dell'intero ciclo di vita di un'organizzazione, in merito a molteplici attività come la definizione di strategie e decisioni, operazioni, processi, funzioni, progetti, prodotti, servizi e beni.

In conclusione, il rischio può essere definito come la combinazione delle probabilità di un evento e della gravità delle sue conseguenze. Qualunque tipo di iniziativa implica potenzialmente eventi e conseguenze che rappresentano possibili benefici (elementi positivi) o minacce alla sicurezza dell'attività trattamentale posta in essere (elementi negativi).

I principali impatti sui diritti e le libertà degli interessati, qualora il rischio di accesso illegittimo, modifica indesiderata e/o perdita di dati dovesse concretizzarsi, sono rappresentati da:

- perdita del controllo dei dati personali;
- limitazione dei diritti;
- discriminazione;
- furto o usurpazione d'identità;
- frodi;

- perdite finanziarie;
- decifratura non autorizzata alla pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale;
- conoscenza da parte di terzi non autorizzati;
- qualsiasi altro danno economico o sociale significativo;
- danni fisici o psicolgici.

Le principali minacce che potrebbero concretizzare il rischio di accesso illegittimo, modifica indesiderata e/o perdita dei dati personali consistono in:

- danni fisici, ossia azioni offensive finalizzate a distruggere, esporre, alterare, disabilitare, sottrarre o ottenere l'accesso non autorizzato a risorse fisiche come l'infrastruttura, l'hardware o l'interconnessione. Rientrano in questa categoria atti di vandalismo, furto, sabotaggio, perdita di informazioni e attacchi massivi riguardanti qualsiasi tipo di infrastruttura, anche quella Internet;
- eventi naturali, ossia eventi che possono distruggere, danneggiare o rendere irrecuperabili risorse fisiche come l'infrastruttura, l'hardware o l'interconnessione (ad esempio fenomeni climatici, incendi, allagamenti, ecc.);
- perdita di servizi essenziali, ossia interruzioni, perdite o malfunzionamenti dei servizi accessori fondamentali per il corretto funzionamento dell'infrastruttura hardware o di interconnessione alle reti informatiche e dati (ad esempio interruzioni nei collegamenti di rete, blackout);
- disturbi, ossia disturbi elettromagnetici o di contorno che possono causare interruzioni o malfunzionamenti dell'infrastruttura hardware o di interconnessione (ad esempio disturbi di rete di tipo intermittente o continuo);
- compromissione di informazioni, ossia azioni mirate ad ascoltare, interrompere o prendere il controllo di una comunicazione di terzi senza il consenso. Le minacce

'legali' comprendono la violazione di norme e leggi, nonché il mancato rispetto dei requisiti contrattuali da parte di prestatori di servizi verso gli utilizzatori dell'infrastruttura di rete (ad esempio furto di documenti o di supporti di memorizzazione);

- problemi tecnici, definiti come guasto o malfunzionamento. Ne sono esempi guasti o interruzioni di dispositivi di rete o sistemi, bug di software o errori di configurazione. Le 'interruzioni' sono disordini inattesi del servizio o riduzione della qualità che scendono al di sotto di un livello richiesto (ad esempio problemi ai software, uso dei servizi da parte di persone non autorizzate);

- azioni non autorizzate, ossia azioni che mirano ai sistemi, alle infrastrutture e/o alle reti mediante azioni dannose. Le minacce comuni sono generalmente definite come attacchi informatici e azioni correlate (ad es. spam, malware, spyware, botnet, manipolazione di hardware e software, alterazioni delle configurazioni, DDoS, sfruttamento di bug dei software, violazione di dati, furto di identità);

- compromissione di funzioni, ossia un danno involontario o accidentale che si riferisce a distruzione, danni fisici e perdite di informazioni per lo più dovuti ad alterazioni del sistema o all'utilizzo inadeguato dei sistemi;

- attacchi di ingegneria sociale, ossia danni veicolati attraverso una serie di tecniche basate su processi cognitivi di influenzamento, inganno e manipolazione che, sfruttando l'ingenua disponibilità e buona fede, nonché l'ignoranza e poca attenzione della vittima, sono finalizzate all'ottenimento di informazioni riservate o sensibili (ad esempio attacchi phishing, divulgazione involontaria delle informazioni).

Data Protection Impact Assessment (DPIA)

Titolare del trattamento: **ASL Roma 5**

Nome Attività: MONITORAGGIO DA REMOTO DEGLI AUTOMEZZI AZIENDALI ASSISITI DA SISTEMI GPS

Data di creazione: 22 dicembre 2022

A) CONTESTO

Servizio di monitoraggio da remoto che prevede l'utilizzo di OBU – On Board Unit dotate di GPS ed una piattaforma web per il monitoraggio e la gestione della flotta, accessibile mediante browser.

1) Finalità del trattamento:

- Monitoraggio da remoto degli autoveicoli aziendali per la sicurezza del patrimonio aziendale, l'incolumità dei lavoratori e la prevenzione di atti illeciti

2) Categorie di interessati:

- ✓ Dipendenti

3) Numero di interessati:

- ✓ Da 1 a 100

4) Sono somministrate le informazioni privacy all'interessato?

- ✓ Si

5) Come sono rese all'interessato le informazioni privacy?

- ✓ Cartellonistica
- ✓ Consegna diretta all'interessato

- ✓ Tramite sito web istituzionale

6) Sono previste modalità per l'esercizio dei diritti dell'interessato? (quali, il diritto di accesso, di rettifica, di cancellazione, di limitazione, di portabilità dei dati, di opposizione)

- ✓ Si

7) Quali sono le modalità per l'esercizio dei diritti dell'interessato?

- ✓ Tramite raccomandata A/R
- ✓ A mezzo mail/PEC

8) Categorie di dati personali:

- ✓ Dati anagrafici in chiaro
- ✓ Dati di traffico ed ubicazione/geolocalizzazione

9) Elencare le attività di trattamento effettuate:

- ✓ Registrazione
- ✓ Conservazione
- ✓ Consultazione
- ✓ Selezione
- ✓ Estrazione
- ✓ Utilizzo
- ✓ Comunicazione
- ✓ Cancellazione
- ✓ Distruzione

10) Modalità di conservazione:

- ✓ Digitale

11) Cancellazione:

- ✓ Sino al raggiungimento delle finalità di trattamento

12) Categorie di destinatari:

- ✓ Responsabile del trattamento *ex* art. 28 GDPR

- ✓ Persona Autorizzata per Designazione ex art. 29 GDPR e 2 quaterdecies Codice Privacy
- ✓ Autorità di Giustizia
- ✓ Forze dell'Ordine Pubblico

13) Piattaforme, dispositivi e/o applicativi utilizzati nell'ambito dell'attività di trattamento in esame:

- ➢ OBU – On Board Unit dotate di GPS; piattaforma web accessibile attraverso browser per il monitoraggio e la gestione della flotta

14) Avviene un trasferimento di dati personali al di fuori dei confini nazionali?

- ✓ No

15) Base Giuridica del Trattamento *ex* art. 6 GDPR:

- ✓ Legittimo interesse del titolare (art. 6, par. 1, lett. f)

16) Tipologia di trattamento:

- ✓ Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti

B) MISURE DI SICUREZZA

B.1) MISURE DI SICUREZZA ORGANIZZATIVE

17) Sicurezza dell'archiviazione della documentazione cartacea:

- ✓ Non applicabile

18) Nomina delle Persone autorizzate per designazione

- ✓ Si

19) Nomina dei delegati al trattamento:

- ✓ Si

20) Nomina dei Responsabili del trattamento:

- ✓ Si

21) Elaborazione ed adozione di policy privacy aziendali:

- ✓ Si

22) Quali?

- ➢ Policy videosorveglianza e GPS

23) Controllo degli accessi fisici:

- ✓ Si

24) Quali?

- ➢ Videosorveglianza per accesso alla struttura

25) Formazione del personale:

- ✓ Si

26) Altra misura di sicurezza fisica e/o organizzativa implementata:

- ➢ Nessuna.

B.2) MISURE DI SICUREZZA TECNICHE

27) Crittografia *Database*:

- ✓ Non applicabile

28) Sistema operativo *workstation*:

- ✓ Linux
- ✓ Windows

29) Aggiornamento sistema operativo:

- ✓ Linux Si
- ✓ Windows Si

30) Configurazione *workstation*:

- ✓ Utente con restrizioni
- ✓ Cambio password temporizzato

31) Tecniche di anonimizzazione:

- ✓ Non applicabile

32) Tecniche di pseudonimizzazione:

- ✓ Non applicabile

33) Partizionamento:

- ✓ Non applicabile.

34) Controllo degli accessi logici:

- ✓ Si

35) Quali strumenti vengono utilizzati?

- ➢ Autenticazione con credenziali cifrate.

36) Tracciabilità:

- ✓ Si

37) Quali strumenti vengono utilizzati?

- ➢ File di *log*

38) Misure anti malware:

- ✓ Anti-*virus*
- ✓ Gestione e aggiornamento delle patch di sicurezza

39) Backup:

- ✓ *Backup* continuo.

40) Sicurezza dei canali informatici:

- ✓ Firewall
- ✓ Protocolli di rete
- ✓ HTTPS
- ✓ Sistema di Autenticazione

C) DPIA

41) Vengono applicate e/o osservate linee guida, *best practice* di settore, norme UNI/ISO/IEC, codice di condotta, regolamenti aziendali, etc.?

- ✓ No

42) La finalità di trattamento è specifica, esplicita e legittima?

- ✓ **Specifica**: è ben delineata ed individuata nella finalità del Titolare di monitorare da remoto, mediante apposita piattaforma, gli automezzi aziendali assistiti da sistemi GPS;
- ✓ **Esplicita**: si, in quanto rappresentata agli interessati per il tramite delle Informazioni privacy *ex* art. 13 GDPR sottoposte all'attenzione di questi, somministrate con cartellonistica;
- ✓ **Legittima:** in quanto conforme alla normativa privacy, poiché è sorretta da idonee basi giuridiche del trattamento e, nello specifico: art. 6, par. 1, lett. f), in quanto "*il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento*".

43) Come viene rispettato il principio di minimizzazione dei dati?

- ➢ Sono raccolti esclusivamente i dati necessari al conseguimento della specifica finalità del trattamento.

C.1) ACCESSO ILLEGITTIMO

44) Quali potrebbero essere i principali impatti sui diritti e le libertà degli interessati se il rischio di accesso illegittimo dovesse concretizzarsi?

- ✓ Perdita del controllo dei dati personali
- ✓ Conoscenza da parte di terzi non autorizzati

45) Quali sono le principali minacce che potrebbero concretizzare il rischio?

- ✓ Danni fisici
- ✓ Compromissione di informazioni
- ✓ Azioni non autorizzate
- ✓ Attacchi di ingegneria sociale

46) Quali sono le principali fonti di rischio?

- ✓ Fonti umane interne

- ✓ Fonti umane esterne

ALTAMENTE PROBABILE (4)	4	8	12	16
PROBABILE (3)	3	6	9	12
POCO PROBABILE (2)	2	4	6	8
IMPROBABILE (1)	1	2	3	4
1, 2, 3 TRASCURABILE 4, 6, 8 LIMITATO 9, 12, 16 MASSIMO	LIEVE (1)	MEDIO (2)	GRAVE (3)	GRAVISSIMO (4)

C.2) MODIFICA INDESIDERATA

47) Quali potrebbero essere i principali impatti sui diritti e le libertà degli interessati se il rischio di modifica indesiderata dei dati dovesse concretizzarsi?

- ✓ Discriminazione
- ✓ Frodi
- ✓ Qualsiasi altro danno economico o sociale significativo

48) Quali sono le principali minacce che potrebbero concretizzare il rischio?

- ✓ Azioni non autorizzate

49) Quali sono le principali fonti di rischio?

- ✓ Fonti umane interne
- ✓ Fonti umane esterne

ALTAMENTE PROBABILE (4)	4	8	12	16
PROBABILE (3)	3	6	9	12
POCO PROBABILE (2)	2	4	6	8
IMPROBABILE (1)	1	2	3	4
1, 2, 3 TRASCURABILE 4, 6, 8 LIMITATO 9, 12, 16 MASSIMO	LIEVE (1)	MEDIO (2)	GRAVE (3)	GRAVISSIMO (4)

C.3) PERDITA ACCIDENTALE

50) Quali potrebbero essere i principali impatti sui diritti e le libertà degli interessati se il rischio di perdita di dati dovesse concretizzarsi?

- ✓ Limitazione dei diritti

51) Quali sono le principali minacce che potrebbero concretizzare il rischio?

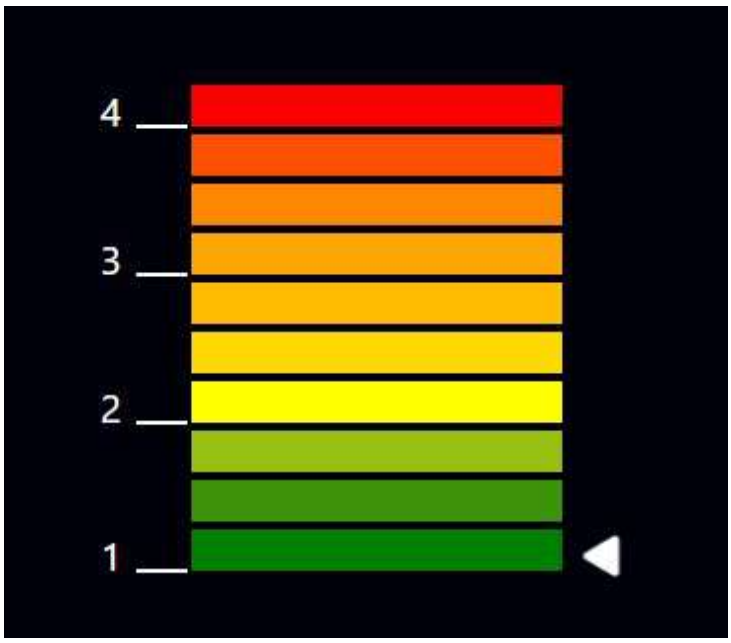
- ✓ Danni fisici
- ✓ Eventi naturali
- ✓ Perdita di servizi essenziali
- ✓ Azioni non autorizzate
- ✓ Compromissione di funzioni

52) Quali sono le principali fonti di rischio?

- ✓ Fonti umane interne
- ✓ Fonti umane esterne
- ✓ Fonti non umane

ALTAMENTE PROBABILE (4)	4	8	12	16
PROBABILE (3)	3	6	9	12
POCO PROBABILE (2)	2	4	6	8
IMPROBABILE (1)	1	2	3	4
1, 2, 3 TRASCURABILE 4, 6, 8 LIMITATO 9, 12, 16 MASSIMO	LIEVE (1)	MEDIO (2)	GRAVE (3)	GRAVISSIMO (4)

GRAFICO DPIA



TRASCURABILE
LIMITATO
SIGNIFICATIVO
MASSIMO

INFORMAZIONI PRIVACY AI FINI DEL MONITORAGGIO DA REMOTO DEGLI AUTOMEZZI AZIENDALI FORNITI DI GPS

L'Azienda Sanitaria Locale Roma 5, con sede legale in Via Acquaregna n.1/15 - 00019 – Tivoli (RM) - C.F. /P.IVA 04733471009 (di seguito "ASL Roma 5") in qualità di Titolare del trattamento informa ai sensi dell'art. 13 Regolamento UE n. 679/2016 (in seguito "GDPR") e del Codice Privacy, ss. mm. ii., che i dati personali saranno trattati con le modalità e per le finalità seguenti:

1. **Finalità e base giuridica del Trattamento**

   I dati personali raccolti dal Titolare sono trattati esclusivamente per **finalità** legate al servizio di monitoraggio da remoto e gestione delle OBU – On Board Unit dotate di GPS, realizzato tramite una piattaforma web accessibile mediante browser.

   La **Base Giuridica** del trattamento dei dati personali di cui al punto n. 2 delle seguenti informazioni privacy si rinviene nell'art. 6, par. 1, lett. f) GDPR, poiché "*il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento*".

2. **Categorie di Dati personali**

   Per le finalità di cui al punto n. 1 potranno essere raccolte e, successivamente trattate, le seguenti categorie di dati personali:

   - dati anagrafici;
   - dati di geolocalizzazione.

3. **Modalità di Trattamento**

   Il trattamento dei dati personali è realizzato per mezzo delle operazioni indicate all'art. 4, par. 1, n. 2 GDPR e più precisamente: raccolta, registrazione, organizzazione, conservazione, consultazione, utilizzo, blocco, comunicazione, cancellazione e distruzione dei dati.

   I dati sono trattati dai Titolare con modalità, strumenti e procedure informatiche e cartacee, strettamente necessari per realizzare le finalità descritte al punto n. 1.

   Il trattamento avviene mediante l'accesso ad una piattaforma web mediante browser, al fine di monitorare e gestire la flotta aziendale.

   Il Titolare predispone inoltre misure di sicurezza fisiche, tecniche e organizzative adeguate ai sensi dell'art. 32 GDPR per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati (*Data Breach*).

4. **Periodo di Conservazione**

   I dati personali raccolti saranno conservati per il tempo necessario al raggiungimento delle finalità del trattamento indicate al punto n. 1 delle presenti informazioni privacy, salvo il tempo più lungo necessario per adempiere agli obblighi di legge e/o a quanto richiesto dalle Autorità competenti.

5. **Accesso ai dati personali**

I dati personali potranno essere accessibili per le finalità di cui al punto n. 1 dai dipendenti del Titolare del trattamento coinvolti ed espressamente autorizzati dal Titolare stesso, dall'Amministratore di sistema, nonché dai Responsabili del trattamento specificamente individuati per iscritto, nell'ambito delle rispettive funzioni ed in conformità alle istruzioni impartite dal Titolare; infine, ad altri Enti, Organismi, Autorità verso i quali il Titolare del trattamento ha un obbligo di comunicazione previsto dalla legge.

6. **Diritti dell'interessato**

   L'interessato dispone dei diritti di cui all'art. 15 GDPR e ss., più precisamente diritto di accesso, diritto di rettifica, diritto alla cancellazione, diritto di limitazione di trattamento, diritto di opposizione, nonché il diritto di proporre reclamo all'Autorità Garante (art. 77 GDPR e 141 Codice Privacy e ss. mm. ii).

7. **Modalità di esercizio dei diritti**

   Il soggetto interessato potrà in qualsiasi momento esercitare i diritti di cui al punto n. 6 delle presenti informazioni privacy, inviando apposita raccomandata A/R o comunicazione all'indirizzo PEC del Titolare:

   - AZIENDA SANITARIA LOCALE ROMA 5, con sede legale in Via Acquaregna n.1/15 - 00019 – Tivoli (RM), PEC: (protocollo@pec.aslromag.it).

8. **Identità e dati di contatto del:**

   - **Titolare del trattamento – Azienda Sanitaria Locale Roma 5 (ASL RM 5)**

     In persona del Direttore Generale, Dr. Giorgio Giulio Santonocito
     E-mail: protocollo.generale@aslroma5.it
     PEC: protocollo@pec.aslromag.it

   - **DPO (RPD) – Scudo Privacy S.r.l.**

     In persona del Dott. Carlo Villanacci
     E-mail: dpo@scudoprivacysrl.com

SISTEMA SANITARIO REGIONALE

ASL
ROMA 5

U.O.C. GESTIONE AMMINISTRATIVA
POLI E DISTRETTI
VIA ACQUAREGNA, 1/15
00019 TIVOLI (RM)