Introduzione

Verizon Connect offre Soluzioni della Forza Lavoro Mobile nell'ambito del Gestione della Flotta e del Gestione del Servizio Esterno. I nostri Prodotti monitorano le prestazioni della flotta di veicoli che possono avere un forte impatto su un'azienda. Si tratta, ad esempio, di dove si trovano i veicoli, di come si comportano i conducenti sulla strada e di quanto carburante consumano. Queste informazioni vengono poi inserite in dashboard riassuntive, in modo da poter valutare rapidamente i dati. Reveal è uno strumento essenziale che consente di fare di più in meno tempo, di garantire un migliore servizio clienti e, in ultima analisi, di migliorare i risultati aziendali. Grazie ai nostri prodotti di Field Service siamo anche in grado di gestire l'intero ciclo di vita delle richieste di assistenza dei nostri clienti sin dal primo contatto, tramite la presentazione di un preventivo, la programmazione del lavoro, la spedizione, la definizione dell'itinerario ideale per i conducenti e l'incasso del pagamento.

Il presente eBook risponde alle FAQ sui Servizi di localizzazione della flotta di Reveal ("i servizi" o "Reveal") venduti da Verizon Connect sulla piattaforma Reveal e contiene una descrizione sintetica di alcune delle considerazioni e dei requisiti chiave in materia di protezione dei dati che è necessario esaminare prima, durante e dopo l'utilizzo del servizio. Se da un lato il presente eBook si concentra principalmente su questioni relative alla protezione dei dati, si dovrebbe valutare se ulteriori requisiti giuridici pertinenti avranno un impatto sull'implementazione e l'utilizzo dei servizi. A titolo di esempio, in alcuni paesi, le disposizioni del diritto del lavoro si applicheranno in caso di utilizzo dei servizi su veicoli guidati dai dipendenti.

Ove opportuno, si è fatto riferimento agli orientamenti normativi disponibili al momento della pubblicazione. Le autorità di regolamentazione esaminano e rivedono regolarmente i propri orientamenti ed è pertanto opportuno seguire da vicino gli sviluppi in questo settore, poiché, in quanto Titolare del trattamento dei dati personali raccolti e utilizzati tramite il servizio, l'utente ha la responsabilità ultima di garantire la conformità alle leggi applicabili.

Le informazioni contenute nel presente eBook non costituiscono una consulenza di natura legale o professionale. Si consiglia di consultare sempre un avvocato adeguatamente qualificato per qualsiasi problematica o questione legale specifica. Verizon Connect non si assume alcuna responsabilità per le informazioni contenute nel presente eBook e declina ogni responsabilità in relazione alle stesse.

FAQ su Reveal

1. A chi si riferiscono i dati raccolti tramite i servizi?
In primo luogo, saranno raccolti i dati relativi ai dipendenti e agli appaltatori che guidano i veicoli in cui sono implementati i servizi. Possono essere raccolti anche dati relativi ad altri interessati (ad esempio, passeggeri o altri famigliari di un conducente che hanno accesso al veicolo), a seconda di come e perché si utilizza il servizio.

2. Con quale modalità vengono raccolti i dati per il servizio?
Il servizio raccoglie dati da due fonti:

- Il dispositivo di bordo installato sui veicoli: Raccoglie dati relativi alla posizione e alle attività dei veicoli. Se si conosce (o si potrebbe individuare) il conducente a cui viene assegnato ciascun veicolo, anche questi dati saranno dei dati personali.
- Sulle nostre piattaforme sono presenti diverse applicazioni mobili che possono essere installate per utilizzare in modo efficace il nostro servizio, come ad esempio le nostre applicazioni relative al prodotto Field Service (Work, Workforce, Field) e le nostre applicazioni relative alla Gestione della flotta (Manager/Spotlight, Video, ELD). Per utilizzare l'applicazione, ogni conducente deve fornire alcuni dati in fase di registrazione.

Nel presente eBook, tutti i dati personali raccolti tramite il servizio sono collettivamente definiti "Dati personali di Reveal".

3. Quali dati personali sono raccolti tramite il servizio?
È l'utente a stabilire la maggior parte dei dati personali che sarà raccolta tramite il servizio; i dati che si

desidera raccogliere variano a seconda di come e perché si utilizza la soluzione. L'utente ha il pieno controllo del tipo di dati che raccoglie. L'utente ha pertanto la responsabilità giuridica di assicurarsi della necessità di ottenere i dati che raccoglie per poter utilizzare il servizio.
I dati personali raccolti tramite il dispositivo di bordo del veicolo possono includeree:

- Dati relativi alla localizzazione (GPS) di veicoli e persone;
- Dati relativi al tachigrafo (tempi di guida);
- Velocità e comportamento del conducente del veicolo;
- Dati relativi agli eventi del veicolo (ad esempio, coinvolgimento in un incidente, ingresso o uscita da un'area monitorata);
- Ulteriori dati relativi al veicolo (ad esempio consumo di carburante, pressione dei pneumatici, dati operativi).

Tra i dati personali raccolti tramite l'applicazione possono figurare:

- Nome del conducente;
- Numero di telefono, indirizzo e-mail e domicilio del conducente;
- Credenziali di accesso del conducente;
- Registrazioni del conducente (ad esempio, assegnazione del veicolo, numero del conducente, posizioni all'interno di un'area monitorata);
- Geolocalizzazione GPS.

4. Tramite Reveal si raccolgono "categorie particolari" di dati o dati relativi a reati?
Ai sensi della normativa in materia di protezione dei dati personali, le categorie particolari di dati sono dati personali relativi a razza, origine etnica, opinioni politiche, religione, appartenenza sindacale, genetica, biometria (se utilizzata per scopi identificativi), salute, vita sessuale, orientamento sessuale. Così come avviene per i dati relativi a reati, il trattamento delle categorie particolare di dati è più limitato.

Tramite il servizio non si richiedono infatti categorie particolari di dati o dati relativi a reati (ad esempio, ai conducenti non viene chiesto di inserire nell'applicazione questo tipo di dati). Mentre le categorie particolari di dati possono essere ottenute dai dati relativi alla localizzazione (ad esempio, i dati relativi alla geolocalizzazione possono rivelare che un conducente visita abitualmente un determinato centro religioso o medico), ciò non rende applicabili i requisiti del GDPR relativi al trattamento di categorie particolari di dati, a meno che i dati relativi alla localizzazione non vengano di fatto utilizzati per estrapolare questo tipo di categoria particolare di dati. Tuttavia, a seconda di come e perché il servizio viene utilizzato, i dati relativi a (presunti) reati potrebbero essere trattati a partire dai dati raccolti (ad esempio, i dati relativi all'attività del veicolo potrebbero indicare che il conducente ha superato un limite di velocità).

Ciò che si configura come un reato varia da paese a paese, così come la classificazione di "categorie particolari" di dati o di dati relativi a reati. Qualora si raccolgano dati che potrebbero essere considerati dati relativi a reati, conformemente alla normativa in materia di protezione dei dati, l'utente, in quanto Titolare del trattamento di tali dati personali, sarà soggetto a obblighi supplementari ai sensi del GDPR e della legislazione nazionale.

5. Chi ha accesso ai Dati personali di Reveal?
I Dati personali di Reveal trattati in fase di erogazione del servizio sono a disposizione dei dipendenti Verizon interessati secondo il principio della "privilegio necessario". I Dati personali di Reveal sono inoltre messi a disposizione di società terze che prestano servizi a Verizon, per consentir alle stesse la gestione del servizio (ad esempio, terzi che prestano servizi di hosting). Verizon può anche comunicare i Dati personali di Reveal a terzi, ove previsto dalla legge (ad esempio, alle Autorità di polizia).

Oltre alle finalità descritte sopra, è possibile scegliere di comunicare i Dati personali di Reveal per le proprie finalità. Si sceglierà chi all'interno dell'azienda dovrebbe avere accesso ai Dati personali di Reveal (ad esempio, sarà necessario incaricare degli amministratori che potranno accedere al portale online per visualizzare in tempo reale la posizione del veicolo e i dati relativi alle attività). È inoltre possibile scegliere di condividere i Dati personali di Reveal con terzi, quali altre aziende del gruppo o altri fornitori di piattaforme (ad esempio, quando un'altra piattaforma si interfaccia con Reveal).

6. Verizon trasferisce i Dati personali di Reveal al di fuori dello Spazio economico europeo ("SEE")?

Verizon custodisce i Dati personali di Reveal in centri dati situati sia all'interno che all'esterno del SEE. Un elenco di tali paesi è disponibile qui: https://www.verizon.com/about/privacy/data-processing-activities. Laddove Verizon condivida i Dati personali di Reveal al di fuori del SEE all'interno del gruppo Verizon, tali trasferimenti avverranno in conformità alle Norme vincolanti d'impresa per il titolare del trattamento e il responsabile del trattamento approvate dall'UE.

7. Per quanto tempo Verizon conserva i Dati personali di Reveal?
I Dati personali di Reveal saranno conservati per tutto il tempo concordato nelle clausole contrattuali e in conformità alle impostazioni di conservazione selezionate nel prodotto. Il termine varia a seconda dell'obbligo giuridico di conservazione dei dati o di eventuali obblighi di comunicazione richiesti dall'utente. È responsabilità dell'utente, in qualità di Titolare del trattamento, assicurarsi di aver compreso per quanto tempo è tenuto per legge a conservare i Dati personali di Reveal. Al termine dei servizi, Verizon Connect cancellerà in modo sicuro i Dati personali di Reveal.

8. Verizon utilizza i Dati personali di Reveal per le proprie finalità?
I Dati personali di Reveal vengono raccolti da Verizon per l'erogazione del servizio Reveal richiesto. Per tali finalità, Verizon sarà il Responsabile del trattamento.

Nella misura consentita dalla legge, Verizon fa un uso secondario di dati anonimizzati raccolti tramite Reveal per le proprie finalità e per migliorare i prodotti e i servizi. Sono incluse l'analisi per l'ottimizzazione della soluzione Reveal e la comunicazione alle compagnie di assicurazione. Dai dati anonimizzati non sarà possibile identificare persone o imprese che utilizzano Reveal.

9. In che modo Verizon garantisce la sicurezza dei Dati personali di Reveal?
Per una descrizione delle misure di sicurezza tecniche e organizzative che Verizon mette in atto per ottemperare ai propri obblighi ai sensi del GDPR, consultare l'Allegato sulla sicurezza delle informazioni dei sistemi interni di Verizon all'indirizzohttps://www.verizon.com/about/privacy/verizon-internal-systems-information-security-exhibit.

Requisiti in materia di protezione dei dati

Questa sezione illustra le modalità di applicazione dei requisiti in materia di protezione dei dati all'utilizzo di Reveal.

Alla fine della presente sezione è stata inserita una checklist degli Articoli nel Regolamento Generale sulla Protezione dei Dati, con indicazione di dove sono trattati nel presente eBook. Questo permetterà di verificare se una particolare disposizione del GDPR è rilevante per Reveal e dove è trattata nel presente eBook. È stato inoltre inserito un elenco di fonti di informazioni aggiuntive.

A. Valutazione d'impatto sulla protezione dei dati

La valutazione d'impatto sulla protezione dei dati ("DPIA") è un processo volto a descrivere e valutare il trattamento dei dati personali e a individuare e gestire i rischi che il trattamento dei dati comporta per gli interessati.

Nel complesso, le autorità di controllo della protezione dei dati ritengono che le DPIA debbano essere svolte quando un'azienda tratta dati personali al fine di valutare le prestazioni, la posizione o i movimenti dei dipendenti[1]. È probabile che l'utilizzo del servizio preveda lo svolgimento di una DPIA, sebbene ciascuna autorità di controllo abbia pubblicato i propri criteri in termini di DPIA. Per stabilire se è necessario procedere a una DPIA andrebbero consultati i criteri dell'autorità di controllo competente.

La DPIA dovrebbe:

[1] WP29 *Linee guida sulla valutazione d'impatto sulla protezione dei dati (DPIA) e per stabilire se il trattamento "potrebbe comportare un rischio elevato" ai fini del Regolamento 2016/679 (GL248) pag.10*

- Descrivere il tipo di trattamento dei Dati personali di Reveal;
    - Le informazioni contenute nel presente e-Book relativamente a quali dati vengono raccolti, alla modalità di raccolta e trattamento degli stessi saranno utili a tal fine.
- Le finalità del trattamento - e, se la base giuridica per l'utilizzo del servizio è che il trattamento è necessario per una finalità che rientra nei legittimi interessi, quali sono tali interessi.
- Valutare se il trattamento è necessario e proporzionato per il conseguimento di tali finalità;
    - Ciò significa considerare se è ragionevolmente possibile conseguire la finalità in un altro modo che comporti un minore trattamento di dati personali.
    - A titolo di esempio, se un'azienda desidera verificare le ore lavorate da una persona, potrebbe farlo con un processo alternativo piuttosto che monitorare la sua posizione durante l'intero turno, in quanto ciò sarebbe chiaramente sproporzionato.
- Valutare i rischi per gli interessati che il trattamento presenta e il modo in cui tali rischi possono essere affrontati;
    - Ad esempio, se un dipendente è autorizzato a utilizzare un veicolo per uso privato, la localizzazione del veicolo mentre il dipendente non lavora risulterebbe invadente e non necessaria per la finalità del datore di lavoro. Tale rischio potrebbe essere attenuato consentendo al dipendente di interrompere il servizio al di fuori dell'orario di lavoro, attivando "Privacy Switch" ("Funzione privacy") disponibile e assicurandosi che i dipendenti siano a conoscenza di questa opzione.
- Descrivere le misure di sicurezza; e
- Descrivere le ulteriori misure atte a garantire la protezione dei dati personali e a dimostrarne la conformità.
    - La DPIA dovrebbe trattare gli ulteriori argomenti illustrati nel presente eBook.
    - In particolare, la DPIA dovrebbe indicare in che modo vengono rispettati i diritti degli interessati.

In fase di realizzazione della DPIA, andrebbe consultato il proprio Responsabile della protezione dei dati (se presente). Se del caso, bisognerebbe inoltre consultare gli interessati i cui dati saranno sottoposti a trattamento ovvero i loro rappresentanti - ad esempio, tramite Consultazione con dipendenti, rappresentanze sindacali o comitati aziendali - e tener conto dei risultati di tale consultazione nella DPIA.

Se con la DPIA si giunge alla conclusione che l'utilizzo dei Dati Personali di Reveal per le finalità previste comporta rischi elevati e non attenuati per gli interessati, andrebbe consultata l'autorità di controllo competente (nel Regno Unito è l'Ufficio del Commissario per l'informazione).

Sarà necessario riesaminare tutte le DPIA e valutare periodicamente l'utilizzo del servizio e dei Dati personali di Reveal rispetto alle stesse.

B. Informativa sulla privacy

Come avviene per tutti i trattamenti di dati personali, è obbligatorio assicurarsi di fornire agli interessati informazioni chiare ed esaurienti circa la raccolta e l'utilizzo dei loro Dati personali di Reveal.

La presente sezione contiene una descrizione delle informazioni che è necessario inserire nell'informativa sulla privacy per soddisfare i requisiti in materia di protezione dei dati. Si dovrebbe tuttavia valutare se ulteriori requisiti giuridici pertinenti avranno ripercussioni sul contenuto dell'informativa sulla privacy e sulle modalità di implementazione del servizio. A titolo di esempio, in alcuni paesi, le disposizioni del diritto del lavoro prevedono l'inserimento di informazioni aggiuntive nell'informativa sulla privacy o in altri documenti interni. Il GDPR prevede l'inserimento nell'informativa sulla privacy delle seguenti informazioni:

- Identità e dati di contatto (e quelli del responsabile della protezione dei dati, se ne è stato nominato uno);
- Le finalità e le basi giuridiche del trattamento (e, quando si trattano i Dati personali di Reveal per una finalità che rientra nei "legittimi interessi", quali sono tali interessi);
    - Le sezioni del presente eBook relative alle finalità e alla base giuridica saranno utili per considerare e descrivere questi aspetti.
- Le categorie di Dati personali di Reveal trattati (e le fonti), se non ottenuti direttamente

dall'interessato;
    - La precedente Sezione 3 "Quali dati personali sono raccolti tramite il servizio?" sarà utile per la descrizione.
- I destinatari dei Dati personali di Reveal e tutti i paesi non appartenenti al SEE verso cui vengono trasferiti i Dati personali di Reveal (unitamente alle informazioni sulle garanzie messe in atto);
- Il periodo di conservazione dei Dati personali di Reveal;
- Se la comunicazione dei Dati personali di Reveal è obbligatoria e le possibili conseguenze della mancata comunicazione di tali dati;
- L'esistenza di un eventuale processo decisionale automatizzato relativo alle persone fisiche (compresa la profilazione), unitamente a informazioni significative sulla logica utilizzata, nonché la rilevanza e le conseguenze previste di tale trattamento per l'interessato;
- Una descrizione dei diritti dell'interessato (compreso il diritto di revocare il consenso, se si trattano i Dati personali di Reveal laddove l'interessato abbia dato il proprio consenso) e della possibilità di presentare un reclamo all'autorità di controllo.

L'informativa sulla privacy presentata deve inoltre soddisfare i requisiti supplementari di cui all'art. 12 del GDPR (ad esempio, che le informazioni fornite agli interessati siano concise, trasparenti, comprensibili e facilmente accessibili, in un linguaggio semplice e chiaro).

Utenti del servizio in Francia
Oltre ai summenzionati requisiti del GDPR, la legge francese in materia di protezione dei dati impone di informare gli interessati del loro diritto di definire delle linee guida in merito all'utilizzo dei loro dati personali dopo il decesso.

Avviso a bordo del veicolo

Dato che la raccolta dei Dati personali di Reveal è un tipo di raccolta di dati meno visibile per gli interessati, sebbene possa avere conseguenze significative, è necessario impegnarsi in modo particolare per segnalare ai conducenti l'uso del servizio. Oltre all'esauriente informativa sulla privacy descritta sopra, gli orientamenti normativi stabiliscono che è necessario informare chiaramente i conducenti che sul veicolo che stanno guidando è stato installato un dispositivo di localizzazione e che vengono monitorati i loro movimenti (e il comportamento di guida, se viene utilizzata la tecnologia specifica). In teoria, queste informazioni dovrebbero essere esposte in modo ben visibile su ogni veicolo interessato, a portata di vista del conducente.[2]

Utenti del servizio in Polonia
Oltre ai contenuti sopra elencati, per cui l'utilizzo del servizio equivale al monitoraggio dei dipendenti, l'avviso a bordo del veicolo dovrebbe altresì riportare:
- Quali dati vengono raccolti e registrati;
- Dove e per quanto tempo tali dati sono conservati; e
- Chi ha accesso ai dati[3].

Attuazione delle politiche

Qualora i Dati personali di Reveal siano utilizzati per l'applicazione di regole e norme, sarà necessario assicurarsi che ciò sia lecito e che i dipendenti sappiano quali sono le regole pertinenti e che, tramite il servizio, si procederà a un monitoraggio per verificare se sono state rispettate.

[2] WP29 *Parere 2/2017 sul trattamento dei dati sul luogo di lavoro* (GL249), pag.20
[3] Ufficio per la protezione dei dati (polacco), *Protezione dei dati sul luogo di lavoro. Linee guida per i datori di lavoro,* pag. 37

C. Registro delle attività di trattamento

In qualità di Titolare del trattamento, l'utente dovrà tenere un Registro delle attività di trattamento ("RAT") come indicato all'art. 30 del GDPR. Sarà necessario assicurarsi che il trattamento dei Dati personali di Reveal sia inserito nel proprio RAT. Sarà necessario inserire informazioni circa:

- Il nome dell'azienda e i dati di contatto (e, se del caso, nome e dati di contatto del responsabile della protezione dei dati, del rappresentante e/o del Contitolare del trattamento);
- La finalità per la quale si utilizzano i Dati personali di Reveal;
- Una descrizione delle categorie di Dati personali di Reveal e delle categorie di interessati i cui dati sono trattati.
    - La precedente Sezione 3 "Quali dati personali sono raccolti tramite il servizio?" sarà utile per la compilazione.
- Le categorie di destinatari a cui saranno comunicati i Dati personali di Reveal;
    - La precedente Sezione 5 "Chi ha accesso ai Dati personali di Reveal?" sarà utile per la compilazione. È inoltre necessario indicare i destinatari ai quali si garantisce l'accesso ai Dati personali di Reveal.
- I trasferimenti dei Dati personali di Reveal verso paesi al di fuori del SEE;
    - Nella precedente Sezione 6 "Verizon trasferisce i Dati personali di Reveal al di fuori del SEE?" viene spiegato dove sono trasferiti i dati e quali garanzie sono messe in atto per proteggere i Dati personali di Reveal.
- I termini;
    - Nella precedente Sezione 7 "Per quanto tempo Verizon conserva i Dati personali di Reveal?" vengono indicati i termini.
- Le informazioni sulle misure di sicurezza, ove possibile.
    - Per una descrizione delle misure di sicurezza tecniche e organizzative che Verizon mette in atto per ottemperare ai propri obblighi ai sensi del GDPR, consultare l'Allegato sulla sicurezza delle informazioni dei sistemi interni di Verizon al seguente url: https://www.verizon.com/about/privacy/verizon-internal-systems-information-security-exhibit

Verizon dispone delle informazioni necessarie per assistere l'utente riguardo a tale obbligo al seguente link: https://www.verizon.com/about/privacy/data-processing-activities

Utenti del servizio nel Regno Unito
Se si trattano dati relativi a reati e la base giuridica per il trattamento è una delle condizioni di cui all'Allegato 1 della Legge sulla protezione dei dati del 2018, sarà necessario aggiungere delle colonne nel RAT (relative alla base giuridica e alle condizioni del trattamento, nonché alla conservazione/cancellazione dei dati rilevanti in linea con la propria Politica specifica, se necessaria).

D. Finalità

Sarà necessario indicare le finalità per le quali si desidera utilizzare il servizio e i Dati personali di Reveal, ad esempio:

- Rilevando e prevenendo la perdita dei beni aziendali;
- Migliorando la produttività dei dipendenti;
- Ottimizzando i percorsi e le risorse e risparmiando carburante;
- Fornendo ai clienti dati relativi alla localizzazione in tempo reale;
- Garantendo la sicurezza e la protezione dei dipendenti, ad esempio assicurando che siano rispettate le pause per il riposo e per i pasti.

È importante essere chiari sin dall'inizio sulle finalità per le quali il servizio viene utilizzato.

- È necessario che vi sia una "base giuridica" per ogni singola finalità per la quale i Dati personali di Reveal sono trattati;
- È necessario assicurarsi di non trattare una quantità di Dati personali di Reveal superiore a quella ragionevolmente necessaria per tale finalità;
- È necessario comunicare agli interessati quali sono tali finalità.

Una volta raccolti i Dati personali di Reveal per tali finalità, sarà quindi possibile utilizzarli unicamente per tali finalità o per altre finalità compatibili. Talvolta, la legislazione applicabile prevede eccezioni a questo principio.

Utenti del servizio in Francia

I dispositivi di geolocalizzazione possono essere installati unicamente sui veicoli utilizzati dai dipendenti per le seguenti finalità[4]:

- Localizzazione, giustificazione e fatturazione dei servizi di trasporto passeggeri;
- Garanzia della sicurezza e della protezione dei dipendenti, delle merci e dei veicoli (in particolare, localizzazione dei veicoli rubati);
- Ottimizzazione dell'assegnazione delle risorse nei casi in cui i servizi sono erogati in aree geografiche vaste, in particolare nell'ambito dei servizi di emergenza;
- Monitoraggio dell'orario di lavoro (ma solo quando non sono disponibili metodi alternativi di monitoraggio dello stesso);
- Rispetto degli obblighi giuridici o normativi;
- Garanzia del rispetto delle norme del datore di lavoro sull'uso dei veicoli professionali.

Per contro, è vietato l'uso di un dispositivo di geolocalizzazione installato sui veicoli dei dipendenti[5]:

- Per verificare il rispetto dei limiti di velocità;
- Per la localizzazione costante dei dipendenti;
- Per verificare l'orario di lavoro, laddove siano disponibili metodi alternativi;
- Nel veicolo di un dipendente che ha libertà di organizzazione del proprio ruolo (ad esempio, un rappresentante di commercio);
- Per monitorare l'uso privato del veicolo laddove questo sia consentito (ad esempio, durante le pause o da parte di dipendenti che possono organizzare liberamente i loro viaggi); oppure
- Per localizzare i rappresentanti sindacali o soggetti simili che agiscono nell'esercizio delle loro funzioni.

Utenti del servizio in Germania

Sono di norma vietati i sistemi di localizzazione tramite i quali i dipendenti possono essere monitorati in modo permanente.[6]

Utenti del servizio in Polonia

Se e nella misura in cui l'utilizzo del servizio costituisce un monitoraggio dei dipendenti, le aziende possono trattare i Dati personali di Reveal esclusivamente per la finalità legittima di "garantire che i dipendenti facciano un uso efficiente dell'orario di lavoro e un uso corretto delle attrezzature e degli strumenti". L'autorità di controllo polacca suggerisce che questa finalità legittima è piuttosto ampia e può consentire di:

- Localizzare un veicolo in caso di furto;
- Svolgere indagini sulla responsabilità di un dipendente per un danno a un veicolo; oppure
- Ottimizzare i percorsi e le risorse e risparmiare carburante;

Utenti del servizio in Portogallo

I servizi non possono essere utilizzati per il monitoraggio del comportamento dei dipendenti e possono essere utilizzati solo su veicoli impiegati dai dipendenti per le seguenti finalità consentite[7]:

- **Gestione della flotta in caso di prestazione di servizi esterni:**
  - Servizi di assistenza tecnica;
  - Distribuzione di beni;
  - Trasporto di passeggeri;
  - Trasporto di merci; e

[4] Linee guida della CNIL sulla geolocalizzazione dei veicoli dei dipendenti, 2018

[5] Linee guida della CNIL sulla geolocalizzazione dei veicoli dei dipendenti, 2018

[6] Commissario per la protezione dei dati e della libertà di informazione Renania-Palatinato, *Sulla legittimità della localizzazione GPS dei dipendenti*; Commissario per la protezione dei dati e della libertà di informazione Baden-Wuerttemberg, *Protezione dei dati sull'occupazione*, 2018, pagg. 36-37

[7] Linea guida del CNPD e Codice del lavoro

- Sicurezza privata.

- **Protezione delle merci:**
  - Trasporto di materiali pericolosi; e
  - Trasporto di materiali di valore elevato.

Se i servizi sono utilizzati specificamente per la geolocalizzazione dei veicoli utilizzati dai dipendenti in caso di furto, il datore di lavoro non può accedere ai dati di geolocalizzazione raccolti fino a quando e a meno che il veicolo non venga rubato. Ulteriori dati relativi ai veicoli (come la velocità media, la rottura, il consumo di carburante) possono essere raccolti ma non collegati a dati personali che rendono identificabile il conducente.

E. Basi giuridiche

Per ciascuna finalità per la quale si utilizzano i Dati personali di Reveal sarà necessario individuare una base giuridica ai sensi dell'art. 6 del GDPR. A seconda del caso, sarà possibile utilizzare i Dati personali di Reveal in quanto necessari per:

- **Rispettare un obbligo di legge:** ad esempio, quando si è obbligati per legge a controllare l'uso/le ore di guida dei veicoli installando sugli stessi un tachigrafo;
- **Eseguire un contratto con l'interessato:** ad esempio, quando una buona guida rappresenta una condizione per l'assunzione;
- **Perseguire una finalità che rientra nei legittimi interessi:** ad esempio, proteggere i conducenti (e gli altri utenti della strada), applicare buone abitudini di guida, monitorare la flotta, migliorare l'efficienza in termini di carburante e manutenzione, difendersi da incidenti e false accuse, garantire la salute e la sicurezza del personale e prestare assistenza in materia di premi assicurativi.

È indispensabile assicurarsi che vi sia una base giuridica legittima per il trattamento dei dati e di essere in grado di giustificarla a un'Autorità di controllo della protezione dei dati, come previsto.

Si dovrà dimostrare che il trattamento dei dati personali di Reveal è "necessario". "Necessario" significa che il trattamento dei Dati personali di Reveal deve essere un modo mirato e proporzionato per il conseguimento della finalità; il trattamento deve essere "più che auspicabile, ma meno che indispensabile o assolutamente necessario"[8]. La valutazione deve essere basata sui fatti, tenendo conto dell'obiettivo perseguito e di eventuali opzioni meno invasive per il conseguimento del medesimo obiettivo. Se esistono alternative realistiche e meno invasive, il trattamento non sarà "necessario"[9].

Laddove ci si basi su legittimi interessi, sarà necessario condurre e documentare un "test di bilanciamento" per garantire che sui propri legittimi interessi non prevalgano gli interessi, i diritti e le libertà degli interessati. Il trattamento dovrebbe essere necessario per la finalità (cioè proporzionato alle esigenze aziendali) e dovrebbero essere incluse garanzie volte a proteggere il diritto al rispetto della vita privata degli interessati. Se gli interessi degli interessati prevalgono sui propri, non si dovrebbe procedere al trattamento.

Consenso: I Dati personali di Reveal possono anche essere trattati con il consenso dell'interessato. Tuttavia, il consenso è valido solo se espresso liberamente. Gli interessati devono inoltre essere liberi di revocare il loro consenso - senza pregiudizio. Ciò rende difficile ottenere un consenso valido nell'ambito dei rapporti di lavoro.[10]
Molte autorità di controllo della protezione dei dati si sono espresse sulle basi giuridiche nel contesto della telematica. A titolo di esempio:

[8] *Consiglio del South Lanarkshire contro il Commissario per l'informazione scozzese* [2013] UKSC 55
[9] Comitato europeo per la protezione dei dati (EDPB), *Linee guida 2/2019 sul trattamento dei dati personali ai sensi dell'articolo 6(1)(b) del GDPR nel contesto della fornitura di servizi online alle persone interessate, adottate il 9 aprile 2019*, pag. 7
[10] Ad esempio, i consensi dei dipendenti non sono sistematicamente considerati validi in Germania (Commissario per la protezione dei dati e della libertà di informazione (LDi) NRW, 24ª *Relazione sulla protezione dei dati e della libertà di informazione 2017-2018*, pagg. 65, 66) e il consenso non costituisce una base giuridica valida per il trattamento dei dati personali nell'ambito dei rapporti di lavoro in Portogallo (Linea guida del CNPD sull'uso dei pedaggi per la geolocalizzazione nel contesto lavorativo e interpretazione rigorosa delle disposizioni del Codice del lavoro).

- Nel Regno Unito e in Polonia, dove l'uso privato di un veicolo è consentito, raramente sarà giustificato il controllo dei movimenti quando questo è utilizzato a titolo privato, senza il libero consenso di colui che lo utilizza.[11]
- In Portogallo, il consenso non costituisce una base giuridica valida per il trattamento dei dati ottenuti dalla geolocalizzazione.[12]
- I dispositivi di localizzazione dei veicoli non dovrebbero essere considerati dispositivi per localizzare o monitorare il comportamento o la posizione dei conducenti o di altro personale, ad esempio tramite invio di avvisi sulla velocità del veicolo.[13]
- Il trattamento dei dati relativi alla localizzazione può essere giustificato quando avviene in fase di monitoraggio del trasporto di persone o merci, per il miglioramento della distribuzione delle risorse o per la sicurezza del dipendente, del veicolo o delle merci trasportate, ma può essere eccessivo quando i dipendenti sono liberi di organizzare il viaggio a loro piacimento o quando viene effettuato unicamente per monitorare il lavoro di un dipendente, laddove questo può essere monitorato con altri mezzi.[14]
  La trasmissione a un cliente di informazioni eccessive sul conducente che consegna materiale, ad esempio la fotografia del passaporto (oltre al suo nome e alla sua posizione) per consentire al cliente di verificarne l'identità al momento dell'arrivo non dovrebbe avere una base giuridica (vi sarebbe un "legittimo interesse" a fornire la fotografia a fini identificativi, ma ciò è considerato sproporzionato per il superamento del test di bilanciamento).[15]

Dati relativi a reati

Se tra i Dati personali di Reveal trattati figurano dati relativi a reati (tenuto conto delle legislazioni locali e dell'interpretazione locale dei "reati"), l'art. 10 del GDPR limita il trattamento di tali dati personali.

I dati relativi a reati possono essere trattati solo se sotto il controllo di un'"autorità ufficiale" o se consentito dalle leggi nazionali o dell'UE applicabili, per cui è necessario consultare le legislazioni locali per individuare, ad esempio, le disposizioni pertinenti:

Utenti del servizio in Francia
Ai sensi della Legge francese sulla protezione dei dati personali, la raccolta di dati personali relativi al comportamento di una persona che può o potrebbe essere classificato come reato o crimine è vietata. È pertanto vietata la raccolta di informazioni sull'eventuale superamento dei limiti di velocità da parte di una persona o di informazioni relative al comportamento di una persona da cui possono emergere violazioni delle norme di circolazione.

Utenti del servizio in Germania
Attualmente, in Germania il normale trattamento dei Dati personali di Reveal non costituisce un trattamento di dati relativi a reati. L'uso dei servizi specifici per l'accertamento di reati sarebbe comunque limitato dall'articolo 26(1) della Legge federale sulla protezione dei dati (BDSG) (ad esempio, nel caso in cui i movimenti dei veicoli siano monitorati per l'accertamento di furti, frodi o traffico di droga da parte dei dipendenti - si precisa che, in tal senso, le infrazioni per eccesso di velocità non costituiscono reati). Questo non sarebbe un caso di "normale" utilizzo di Reveal ed è quindi probabile che al trattamento per tale finalità si proceda esclusivamente in via eccezionale (ad esempio, se un datore di lavoro indaga su casi per cui sospetta che un dipendente abbia commesso un reato), ma qualora si utilizzino i servizi per tale finalità, è necessario consultare l'articolo 26(1) della BDSG.

Utenti del servizio in Italia
In generale, il trattamento dei Dati personali di Reveal non costituisce un trattamento di dati relativi a reati

[11] Ufficio del Commissario per l'informazione *Il codice delle prassi di lavoro*, pag. 76; Ufficio per la protezione dei dati (polacco), *Protezione dei dati sul luogo di lavoro. Linee guida per i datori di lavoro,* pag. 38
[12] Linea guida del CNPD sull'uso dei pedaggi per la geolocalizzazione nel contesto lavorativo e interpretazione rigorosa delle disposizioni del Codice del lavoro
[13] WP29 *Parere 13/2011 sui Servizi di geolocalizzazione su dispositivi mobili intelligenti*
[14] WP29 *Parere 5/2005 sull'uso dei dati relativi alla localizzazione al fine di fornire servizi a valore aggiunto*
[15] WP29 *Parere 2/2017 sul trattamento dei dati sul luogo di lavoro*

come intesi in Italia (solo le violazioni che sarebbero punibili con una sanzione amministrativa pecuniaria). È tuttavia necessario verificare se eventuali modifiche della legislazione locale introducano reati per i quali i Dati personali di Reveal possono essere rilevanti.

Utenti del servizio in Polonia
Ai sensi del Codice del lavoro polacco del 1974 al trattamento dei dati relativi a reati dei dipendenti si applicano alcuni requisiti specifici; in particolare non è possibile basarsi sul consenso di un dipendente per il trattamento dei suoi dati relativi a reati. È necessaria una base giuridica alternativa, molto probabilmente perché i dati sono trattati per adempiere a un obbligo di legge ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria.

Utenti del servizio in Portogallo
Il trattamento dei dati relativi a reati per la prevenzione o l'accertamento di un atto illecito (quale, potenzialmente, la commissione di infrazioni stradali/per eccesso di velocità) è ammesso in determinate circostanze e laddove il trattamento risulti necessario ai fini o in relazione a qualsiasi procedimento giudiziario, consulenza legale ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria. I dati personali devono, tuttavia, essere pseudonimizzati entro sette giorni dalla raccolta.

Utenti del servizio in Spagna
In generale, il trattamento dei Dati personali di Reveal non costituisce un trattamento di dati relativi a reati come intesi in Spagna (solo le violazioni delle norme di circolazione). È tuttavia necessario verificare se eventuali modifiche della legislazione locale introducono reati per i quali i Dati personali di Reveal possono essere rilevanti, poiché in Spagna il trattamento dei dati relativi a reati è limitato - gli unici casi (potenzialmente) rilevanti in cui si potrebbe procedere al trattamento dei dati relativi a reati in questo contesto sono quando: (i) la finalità è la prevenzione, l'indagine, l'accertamento o il perseguimento di reati o l'applicazione del diritto penale, (ii) il trattamento è disciplinato da una norma con forza ed effetto di legge o dal diritto dell'UE.

Utenti del servizio nel Regno Unito
Nel Regno Unito, è necessario garantire che, oltre a una base giuridica, sia soddisfatta una condizione per il trattamento ai sensi dell'articolo 9 del GDPR o dell'Allegato 1 della Legge sulla protezione dei dati del 2018. Ad esempio, per quanto riguarda i dati relativi a reati, la Legge sulla protezione dei dati del 2018 consente il trattamento dei dati personali per la prevenzione o l'accertamento di un atto illecito (quale, potenzialmente, la commissione di infrazioni stradali/per eccesso di velocità) in determinate circostanze e laddove il trattamento risulti necessario ai fini o in relazione a qualsiasi procedimento giudiziario, consulenza legale ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria.

F. Minimizzazione dei dati

È necessario assicurarsi di utilizzare esclusivamente i Dati personali di Reveal che siano adeguati, pertinenti e limitati a quanto necessario (tenuto conto delle proprie finalità). In ultima analisi, ciò significa che è necessario individuare e utilizzare la quantità minima di Dati personali di Reveal di cui si ha bisogno per il conseguimento delle finalità.

Se si consente ai dipendenti di fare uso personale dei veicoli, solitamente non vi è necessità di raccogliere dati su dove il veicolo viene condotto al di fuori dell'orario di lavoro. Il servizio ha una funzionalità che garantisce che i dipendenti non siano monitorati al di fuori dall'orario di lavoro. Tale funzionalità viene definita "Privacy Switch" ("Funzione privacy") e rappresenta un modo semplice ed economico per garantire la conformità. In alcuni paesi (quali Francia, Germania e Portogallo), la possibilità per i dipendenti di utilizzare la "Privacy Switch" ("Funzione privacy") è prevista dagli orientamenti normativi.[16]

G. Esattezza dei dati

Sarà necessario assicurarsi che i Dati personali di Reveal utilizzati non siano errati od oggettivamente

[16] Commissario per la protezione dei dati bavarese, 27ª Relazione di attività 2016, pag. 241; Linee guida della CNIL sulla geolocalizzazione dei veicoli dei dipendenti, 2018; Delibera del CNPD 7680/2014

fuorvianti. Nel quadro dei Dati personali di Reveal, è particolarmente importante adottare misure volte a garantire l'esattezza dei dati personali (ad esempio, assicurandosi che le registrazioni dei veicoli assegnati ai dipendenti siano effettuate in modo accurato) e valutare attentamente qualsiasi contestazione circa l'esattezza dei dati personali (ad esempio, un conducente che contesta la propria posizione in un determinato momento).

H. Conservazione dei Dati personali di Reveal

I Dati personali di Reveal dovranno essere conservati solo per il tempo necessario per il conseguimento della finalità specificata. Sarà necessario valutare se risultano applicabili gli obblighi di conservazione previsti dalla legge (ad esempio, per la conservazione dei registri relativi alle ore lavorative). Questi aspetti dovranno essere trattati nella politica di conservazione.

I. Sicurezza dei Dati personali di Reveal

Sarà necessario mettere in atto misure "tecniche e organizzative adeguate" volte a garantire la riservatezza, l'integrità e la disponibilità dei Dati Personali di Reveal, in conformità all'art. 32 del GDPR. È possibile ricorrere a una valutazione dei rischi per individuare particolari problematiche che emergono dall'utilizzo di Reveal e dei Dati personali di Reveal per stabilire il livello di sicurezza "adeguato" (tenendo conto dello stato dell'arte e dei costi di attuazione). Una volta messe in atto, le misure tecniche e organizzative andrebbero testate regolarmente per assicurarsi che continuino ad essere adeguate. Qualora condivida i Dati personali di Reveal con un'altra azienda che agisce in qualità di Responsabile del trattamento per suo conto, l'utente si dovrà assicurare che quest'ultimo fornisca garanzie sufficienti (e si impegni contrattualmente) per mettere in atto misure tecniche e organizzative adeguate per la protezione dei dati.

In caso di violazione della sicurezza dei dati personali, sarà necessario rispettare le disposizioni di cui agli artt. 33 e 34 del GDPR. L'utente riceverà una notifica senza ingiustificato ritardo. Potrebbe essere necessario informare l'autorità di controllo competente entro 72 ore dal momento in cui si è venuti a conoscenza dell'incidente (a meno che non si ritenga improbabile che possa costituire un rischio per i diritti e le libertà degli interessati). Qualora la violazione possa comportare un rischio elevato per i diritti e le libertà degli interessati, sarà altresì necessario informare queste ultime senza ingiustificato ritardo. Si dovrà valutare il modo in cui rilevare il verificarsi di una violazione relativa ai Dati personali di Reveal, quali misure adottare per mitigare la violazione e in che modo si intende segnalarla internamente a un livello superiore e valutare se la notifica risulti necessaria.

<u>Utenti del servizio in Francia</u>
Ai sensi delle Linee guida della CNIL sulla geolocalizzazione dei veicoli dei dipendenti[17], sarà necessario mettere in atto, in particolare, quanto segue:

- politica di autorizzazione all'accesso;
- misure per i trasferimenti di dati sicuri; e
- un registro dei log in caso di accesso e trattamento dei dati.

<u>Utenti del servizio in Spagna</u>
In caso di rettifica o cancellazione dei dati personali, la Legge spagnola sulla protezione dei dati impone ai Titolari del trattamento di "bloccare" i dati nell'ambito delle misure tecniche e organizzative che mettono in atto in conformità all'art. 32 - ciò significa che i dati personali pertinenti devono essere estratti e conservati in una banca dati separata e che devono essere adottate misure tecniche e organizzative per impedire il trattamento dei dati (compresi accessi o visualizzazioni). I dati personali pertinenti devono essere conservati in una banca dati separata e protetta per accogliere le richieste eventualmente avanzate dagli organismi pubblici competenti (come le autorità giurisdizionali, il pubblico ministero, le autorità di controllo della protezione dei dati, ecc.) ovvero nel caso in cui il trasferimento dei dati a tali organismi pubblici sia necessario per esercitare o difendere un diritto in sede giudiziaria. Per definire il periodo durante il quale i dati personali devono essere "bloccati" occorre tener conto dei termini di prescrizione per le diverse azioni legali che possono essere

[17] *Linee guida della CNIL sulla geolocalizzazione dei veicoli dei dipendenti,* 2018

intentate in seguito al trattamento dei dati pertinenti. I dati personali possono essere completamente cancellati una volta scaduti i termini di prescrizione pertinenti.

In qualità di Titolare del trattamento dei Dati personali di Reveal, l'utente deve assicurarsi di poter adempiere a tale obbligo. Verizon assiste l'utente nell'adempimento di tale obbligo, consentendogli di scaricare copie di alcuni Dati personali di Reveal tramite la dashboard self-service di Reveal e fornendogli, su richiesta, ulteriori Dati personali di Reveal.

J. Diritti degli interessati

Sarà necessario stabilire il modo in cui adempiere all'obbligo di rispondere alle richieste degli interessati. Ai sensi del GDPR, gli interessati godono dei seguenti diritti in relazione ai loro dati personali:

- Diritto di accesso;
- Diritto di rettifica;
- Diritto alla cancellazione;
- Diritto di limitazione di trattamento;
- Diritto alla portabilità dei dati;
- Diritto di opposizione;
- Diritti in materia di processo decisionale automatizzato relativo alle persone fisiche e di profilazione.

È necessario informare gli interessati mediante l'informativa sulla privacy di tali diritti.
L'applicazione di tali diritti può essere limitata (ad esempio, il diritto alla portabilità dei dati sussiste solo se i dati personali sono trattati sulla base giuridica della necessità contrattuale o del consenso) e possonoapplicate delle deroghe (ad esempio, se la divulgazione di dati ledesse i diritti altrui, tra cui la protezione di segreti commerciali).

In generale, si dovrà rispondere a tali richieste entro un mese e assicurarsi che la risposta soddisfi i requisiti supplementari previsti dall'art. 12 del GDPR (ad esempio, che le informazioni fornite agli interessati siano concise, trasparenti, comprensibili e facilmente accessibili, utilizzando un linguaggio chiaro e semplice).

Ove possibile, Verizon può prestare assistenza per rispondere alle richieste degli interessati in merito al servizio.

<u>Utenti del servizio in Francia</u>
Ai sensi della Legge francese sulla protezione dei dati personali, gli interessati hanno il diritto di definire delle linee guida in merito all'utilizzo dei loro dati personali dopo il decesso. È necessario assicurarsi di essere in grado di rispondere a questo tipo di richiesta.

K. Condivisione dei Dati personali di Reveal

Oltre agli interessati che richiedono l'accesso ai propri dati personali, sarà necessario stabilire in che modo rispondere alle richieste di terzi di accedere ai Dati personali di Reveal. A titolo di esempio, tra queste potrebbero figurare richieste da parte delle forze dell'ordine e delle compagnie di assicurazione nel caso in cui un veicolo sia stato coinvolto in un incidente.

Qualsiasi condivisione dei Dati personali di Reveal (ad esempio, con altre aziende del gruppo o con un altro fornitore di servizi) dovrà soddisfare tutti i requisiti in materia di protezione dei dati indicati nel presente eBook (ad esempio, la condivisione deve essere lecita, proporzionata, trasparente, ecc.). L'utente dovrà valutare se è necessario stipulare contratti o altri accordi con l'azienda (ad esempio, nel caso in cui l'altra azienda agisca in qualità di Responsabile del trattamento per suo conto o di Contitolare del trattamento assieme all'utente). Qualora tale condivisione implichi un trasferimento dei Dati personali di Reveal al di fuori dello Spazio economico europeo ("**SEE**"), sarà necessario assicurarsi che il trasferimento sia consentito ai sensi del GDPR.

<u>Utenti del servizio in Francia</u>
Secondo le linee guida della CNIL, è necessario limitare l'accesso ai dati relativi a (o risultanti da) dispositivi di

geolocalizzazione (a seconda dei casi): (i) al personale autorizzato, (ii) al datore di lavoro della persona cui si riferiscono i dati di geolocalizzazione; e (ii) al personale autorizzato di un cliente al quale si forniscono servizi pertinenti. In linea di principio, il nome del conducente non deve essere condiviso, a meno che tali dati non siano particolarmente pertinenti e necessari.

L. Processo decisionale automatizzato

La normativa in materia di protezione dei dati vieta alle imprese di adottare decisioni basate esclusivamente sul trattamento automatizzato di dati personali laddove la decisione abbia effetti giuridici o effetti altrettanto significativi. Sarà necessario individuare tali usi del servizio. Ciò potrebbe essere rilevante laddove:

- Lo stipendio di un conducente venga calcolato automaticamente in base al momento in cui questi inizia/termina la guida di un veicolo;
- Il conducente riceva automaticamente un avviso per l'ingresso in un'area monitorata;
- L'idoneità del conducente a ricevere un bonus venga calcolata automaticamente in base al numero di lavori assegnati e ultimati, così come registrato dal servizio.

Se vi è una revisione umana significativa di una decisione prima che questa venga adottata, tali restrizioni non si applicano.

Le aziende sono autorizzate ad adottare questo tipo di decisioni esclusivamente automatizzate quando la decisione è:

- Necessaria per l'esecuzione o la stipula di un contratto;
- Autorizzata dal diritto dell'Unione o degli Stati membri cui è soggetto il Titolare del trattamento e che stabilisce anche misure idonee a tutelare i diritti, le libertà e i legittimi interessi dell'interessato; oppure
- Basata sul consenso esplicito dell'interessato.

In caso di processo decisionale automatizzato relativo alle persone fisiche, è necessario fornire agli interessati informazioni chiare (cfr. sopra, "Informativa sulla privacy") e, almeno, concedere agli stessi il diritto di ottenere l'intervento umano nel processo decisionale, di esprimere il proprio punto di vista e di contestare la decisione.

Utenti del servizio in Portogallo
Non è consentito l'uso di dati di geolocalizzazione e di telemetria dei veicoli al solo scopo del processo decisionale automatizzato.[18]

M. Consultazione con dipendenti/comitati aziendali/rappresentanze sindacali

Ai sensi della normativa di diritto del lavoro, potrebbe essere necessario consultare i dipendenti, i comitati aziendali o le rappresentanze sindacali in merito all'implementazione del servizio ovvero a ulteriori utilizzi che si sceglie di fare dei Dati Personali Reveal. In alternativa, potrebbe essere necessario consultare i sindacati o i rappresentanti dei lavoratori secondo le condizioni previste da eventuali accordi con i lavoratori, volontariamente implementati e in vigore. Anche se non richiesto, potrebbe essere opportuno consultare il personale in merito all'utilizzo del servizio e dei Dati Personali Reveal come parte integrante del processo di DPIA.

Nell'eventualità che si raggiunga un accordo vincolante con il comitato aziendale, tale accordo costituirebbe una "norma più specifica" volta a garantire i diritti di protezione dei dati dei dipendenti ai sensi dell'articolo 88(1) del GDPR. Ciò significa che un tale accordo può, in alcune circostanze, garantire la certezza giuridica su come utilizzare Reveal all'interno dell'azienda. Per soddisfare il requisito di una "norma più specifica" ai sensi dell'articolo 88(1) del GDPR, l'accordo aziendale deve essere vincolante secondo le leggi locali in materia di occupazione e deve tenere adeguatamente conto degli interessi dei lavoratori in materia di protezione dei dati (cfr. articolo 88(2) del GDPR). In caso di dubbio, è necessario rivolgersi a un consulente legale.

[18] Linea guida del CNPD sull'uso dei pedaggi per la geolocalizzazione nel contesto lavorativo e interpretazione rigorosa delle disposizioni del Codice del Lavoro

Utenti del servizio in Francia
Secondo l'art. L2312-38 del Codice del Lavoro francese, è necessario informare e consultare i Comitati aziendali (*Conseil Economique et Social*) prima di adottare qualsiasi sistema o mezzo che permetta di monitorare l'attività dei dipendenti, come il monitoraggio della geolocalizzazione.

Utenti del servizio in Germania
Ai sensi dell'articolo 87(6) della Legge a tutela dei lavoratori (Betriebsverfassungsgesetz -BetriebsVG), il comitato aziendale, se esistente all'interno dell'azienda, ha il diritto di co-determinare l'introduzione e l'uso di apparecchiature tecniche destinate a monitorare il comportamento o le prestazioni dei dipendenti. Il "controllo permanente" del comportamento e delle prestazioni dei dipendenti attraverso il monitoraggio non è consentito - il datore di lavoro è tenuto a escludere tale "controllo" permanente dei dipendenti per mezzo di accordi del comitato aziendale o di regolamenti unilateralmente vincolanti.[19]

L'articolo 26(4) della Legge federale sulla protezione dei dati stabilisce esplicitamente che il trattamento dei dati può essere consentito sulla base di accordi aziendali, se questi soddisfano i requisiti di cui all'articolo 88(2) del GDPR.

Utenti del servizio in Italia
Potrebbe essere necessario consultare il/i sindacato/i dell'azienda, se del caso, od ottenere l'autorizzazione dall'Ispettorato del lavoro competente per l'esecuzione del servizio e l'utilizzo dei Dati Personali di Reveal per ottemperare all'art. 4 (2) della Legge n. 300/1970 (Statuto dei lavoratori), a meno che i Dati personali di Reveal trattati si limitino ai dati strettamente necessari per adempiere agli obblighi di legge.

Utenti del servizio in Polonia
Occorre definire la finalità, l'ambito e i metodi di monitoraggio nel proprio Regolamento aziendale (una politica interna obbligatoria in Polonia per i datori di lavoro con oltre 50 dipendenti) o nel Contratto collettivo di lavoro aziendale. Se nell'azienda sono presenti sindacati, per le modifiche al Regolamento di lavoro o al Contratto collettivo di lavoro aziendale sarà necessaria la collaborazione con i sindacati.

Per quanto riguarda i dipendenti esistenti, sarà necessario informarli che si intende introdurre un sistema di monitoraggio. Ciò dovrebbe avvenire entro due settimane prima dell'introduzione del sistema di monitoraggio.

Utenti del servizio in Portogallo
Secondo l'art. 21 del Codice del lavoro portoghese, è necessario informare e consultare i Comitati aziendali (Comissão de Trabalhadores) prima di adottare qualsiasi sistema o mezzo che permetta di monitorare l'attività dei dipendenti, come il monitoraggio della geolocalizzazione.

Utenti del servizio in Spagna
Ai sensi dell'art. 64(1) dello Statuto dei lavoratori spagnolo, è necessario informare i rappresentanti dei lavoratori prima di mettere in atto qualsiasi misura che possa interessare i lavoratori, tra cui l'adozione di dispositivi di geolocalizzazione o qualsiasi ulteriore soluzione di monitoraggio.

A supporto di quanto precede, l'art. 90(2) della Legge Organica 3/2018, del 5 dicembre, sulla protezione dei dati personali e la concessione dei diritti digitali stabilisce che, prima dell'adozione di dispositivi di geolocalizzazione, i rappresentanti dei dipendenti e dei lavoratori debbano essere informati dell'esistenza e delle caratteristiche di tali dispositivi.

N. Attenuazione del rischio e protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

È necessario assicurarsi che siano state adottate tutte le misure necessarie per attenuare i rischi per le persone fisiche (come identificate durante il processo di DPIA) e per rispettare i requisiti di "protezione dei dati fin dalla

[19] Commissario per la protezione dei dati e della libertà di informazione Baden-Wuerttemberg, *Protezione dei dati sull'occupazione*, 2018; Centro indipendente per la protezione dei dati Schleswig-Holstein, Relazione di attività 2017-2018, 103

progettazione e protezione per impostazione predefinita". La protezione dei dati fin dalla progettazione significa che le questioni relative alla privacy dovrebbero essere prese in considerazione e trattate sin dall'inizio di un'attività di trattamento dei dati (ossia in fase di progettazione) e durante il ciclo di vita di tale attività di trattamento. La protezione dei dati per impostazione predefinita prevede di garantire che siano trattati i dati minimi necessari per il conseguimento della(e) finalità (ad esempio, invece di consentire un ampio accesso ai Dati personali di Reveal, l'accesso dovrebbe essere limitato a persone specifiche secondo il principio della "necessità di sapere").

Le linee guida delle autorità di controllo della protezione dei dati forniscono esempi di attenuazione dei rischi nell'ambito della telematica e del monitoraggio dei dipendenti:

- Ai conducenti dovrebbe essere consentito di disabilitare temporaneamente il monitoraggio della localizzazione in determinate circostanze (ad esempio, quando visitano una clinica medica), laddove sia loro consentito l'uso personale dei veicoli aziendali.[20]
- Quando vi è la necessità di monitorare la posizione di un veicolo al di fuori dell'orario di lavoro di un dipendente (ad esempio, per prevenire il furto del veicolo), l'implementazione deve essere proporzionata ai rischi, ad esempio quando la posizione del veicolo non è registrata (o visibile) al di fuori dell'orario di lavoro, a meno che il veicolo non esca da un'area ampia e circoscritta (ad esempio, una regione).[21]
- Il numero di dipendenti che hanno accesso ai Dati personali di Reveal deve essere ridotto al minimo. Il personale deve essere adeguatamente formato e soggetto agli obblighi di riservatezza e sicurezza.[22] Valutare quali dipendenti sono più idonei ad accedere ai Dati personali di Reveal (ad esempio, non i manager di linea).[23]

O. Nomina di un Responsabile della protezione dei dati (DPO)

L'art. 37 del GDPR stabilisce diversi criteri per la nomina di un responsabile della protezione dei dati ("DPO"). Le attuali attività di trattamento potrebbero non prevedere già la nomina di un DPO. Tuttavia, l'utilizzo dei servizi può far sorgere la necessità di disporre di un DPO in base all'art. 37(1)(b), che prevede la nomina di un DPO quando le attività principali di un'organizzazione consistono nel monitoraggio regolare e sistematico su vasta scala degli interessati. L'uso dei servizi di monitoraggio dei conducenti e del loro comportamento di guida rientra probabilmente nell'ambito di applicazione dell'articolo. 37, paragrafo 1, lettera b), nel qual caso sarà necessario nominare un DPO. Ulteriori disposizioni del GDPR (artt. 38 e 39) stabiliscono i requisiti relativi alla posizione e ai compiti del DPO - si dovrà anche rispettarli qualora sia prevista la nomina di un DPO.

<u>Utenti del servizio in Germania</u>
Ai sensi dell'articolo 38 della Legge federale sulla protezione dei dati (BDSG), è obbligatorio nominare un DPO se vengono impiegate in modo permanente almeno 20 persone per il trattamento automatizzato di dati personali o se il trattamento dei dati personali necessita la conduzione di una DPIA. In caso di utilizzo dei servizi in Germania è probabile che sia necessario nominare un DPO.

Ulteriori informazioni

Legislazione

- Regolamento generale sulla protezione dei dati (UE) 2016/679 ("GDPR")
- Legge sulla protezione dei dati del 2018 (Regno Unito)
- Legge 58/2019 del 8 Agosto 2019 (Portogallo)
- Codice del lavoro (Portogallo)
- Legge costituzionale 3/2018, 5 dicembre 2018, sulla protezione dei dati personali e la garanzia dei diritti digitali (Spagna)
- Legge federale sulla protezione dei dati (Bundesdatenschutzgesetz – BDSG) 2018 (Germania)
- Legge sull'ordinamento aziendale (Betriebsverfassungsgesetz -BetriebsVG) (Germania)
- Decreto legislativo 196/2003 (Codice in materia di protezione dei dati) (Italia)

[20] Articolo 29 Gruppo di lavoro *Parere 2/2017 sul trattamento dei dati sul luogo di lavoro* (GL249), pag. 20
[21] Articolo 29 Gruppo di lavoro *Parere 2/2017 sul trattamento dei dati sul luogo di lavoro* (GL249), pag. 20
[22] Ufficio del Commissario per l'informazione, *Codice delle prassi di lavoro*, pag. 67
[23] Ufficio del Commissario per l'informazione, *Codice delle prassi di lavoro*, pag. 67

- Legge n° 300/1970 (Statuto dei lavoratori) (Italia)
- Decreto legislativo 101/2018 (Italia)
- Legge francese sulla protezione dei dati n° 78-17 (Francia)
- Codice del lavoro francese (Francia)

Giurisprudenza

Consiglio del South Lanarkshire contro il Commissario per l'informazione scozzese [2013] UKSC 55 (Regno Unito)

Orientamenti normativi

UE

- Articolo 29 Gruppo di lavoro *Parere 5/2005 sull'uso dei dati relativi alla localizzazione al fine di fornire servizi a valore aggiunto* (WP115)
- Articolo 29 Gruppo di lavoro *Parere 13/2011 sui Servizi di geolocalizzazione su dispositivi mobili intelligenti* (WP185)
- Articolo 29 Gruppo di lavoro *Linee guida sulla valutazione d'impatto sulla protezione dei dati (DPIA) e per stabilire se il trattamento "potrebbe comportare un rischio elevato" ai fini del Regolamento 2016/679* (WP248)
- Articolo 29 Gruppo di lavoro *Parere 2/2017 sul trattamento dei dati sul luogo di lavoro* (WP249)
- Articolo 29 Gruppo di lavoro *Parere 2016/679 Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento* (WP251)
- Comitato europeo per la protezione dei dati *Linee guida 2/2019 sul trattamento dei dati personali ai sensi 6(1)(b) del GDPR nel contesto della fornitura di servizi online alle persone interessate (versione per la consultazione pubblica)*

Francia

- Linee guida della CNIL sulla geolocalizzazione dei veicoli dei dipendenti, 2018

Germania

- Commissario per la protezione dei dati e della libertà di informazione Renania-Palatinato, *Sulla legittimità della localizzazione GPS dei dipendenti*
- Commissario per la protezione dei dati e della libertà di informazione Baden-Wuerttember, *Protezione dei dati sull'occupazione* 2018
- Conferenza delle autorità federali e statali (Länder) indipendenti per la protezione dei dati personali (Datenschutzkonferenz - DSK), Breve rapporto n° 14: *Protezione dei dati sull'occupazione* (17 dicembre 2018)
- Commissario per la protezione dei dati bavarese, *27° Relazione di attività 2016*
- Conferenza delle autorità federali e statali (Länder) indipendenti per la protezione dei dati personali (Datenschutzkonferenz - DSK), Breve rapporto n° 17: *Categorie particolari di dati personali* (27 marzo 2018)
- Conferenza delle autorità federali e statali (Länder) indipendenti per la protezione dei dati personali (Datenschutzkonferenz - DSK), Breve rapporto n° 19: *Informazione e impegno dei dipendenti a rispettare i requisiti in materia di protezione dei dati ai sensi del GDPR* (29 maggio 2018)
- Commissario per la protezione dei dati e della libertà di informazione Renania-Vestfalia (LDi NRW), 24ª Relazione sulla protezione dei dati e della libertà di informazione 2017-2018, *Posizionamento via satellite per la determinazione della posizione dei veicoli aziendali - nessun mezzo consentito per il monitoraggio dei dipendenti*
- Commissario per la protezione dei dati e della libertà di informazione di Berlino, *Relazione annuale 2018*
- Centro indipendente per la protezione dei dati Schleswig-Holstein, Relazione di attività 2017-2018
- Commissario per la protezione dei dati e della libertà di informazione Bassa Sassonia, 24ª Relazione di attività 2017-2018, *Monitoraggio GPS dei veicoli aziendali*

Polonia

- Ufficio Polacco per la Protezione dei Dati, *Protezione dei dati sul luogo di lavoro. Linee guida per i datori di lavoro*

Portogallo

- Delibera del CNPD 7680/2014 (Linea guida sull'uso della geolocalizzazione nel contesto lavorativo).

Regno Unito

- *Codice deotologico* e *Indicazioni supplementari* dell'Information Commissioners Office

Lista di controllo del GDPR

Articolo del GDPR	**Argomento**	**Rilevanza per Reveal**	**Riferimento eBook**
Art. 1, 2 o 3	Oggetto e finalità; ambito di applicazione materiale; e territoriale	Nessuna rilevanza specifica	N/A
Art. 4	Definizioni	Definisce i concetti di "dati personali" e di "categorie particolari" di dati personali	"*FAQ su Reveal*", sezioni 3 e 4
Art. 5	Principi e responsabilità	Il trattamento dei Dati personali di Reveal deve essere conforme ai principi di protezione dei dati e il Titolare del trattamento deve essere in grado di dimostrarne la conformità	*"Soddisfazione dei requisiti di protezione dei dati"*, in generale
Artt. 6 e 7	Liceità del trattamento e condizioni per il consenso	È necessaria una base giuridica per ciascuna finalità del trattamento dei Dati personali di Reveal	*"Soddisfazione dei requisiti di protezione dei dati"*, sezione E
Art. 8	Condizioni per il consenso dei minori nei SSI	Nessuna rilevanza specifica	N/A
Artt. 9 e 10	Trattamento di categorie particolari di dati personali e di dati relativi a reati	È necessaria una condizione per ciascuna finalità del trattamento dei Dati personali di Reveal, laddove i dati personali corrispondano una categoria particolare di dati o dati relativi a reati	"*FAQ su Reveal"*, sezione 4, e *"Soddisfazione dei requisiti di protezione dei dati"*, sezione E
Art. 11	Trattamento che non prevede l'identificazione	Nessuna rilevanza specifica	N/A
Art. 12	Informazione, comunicazione e modalità trasparenti per l'esercizio dei diritti dell'interessato	Tutte le informazioni fornite agli interessati i cui Dati personali di Reveal sono sottoposti a trattamento devono essere concise, trasparenti, comprensibili e facilmente accessibili, utilizzando un	*"Soddisfazione dei requisiti di protezione dei dati"*, sezioni B e J

		linguaggio semplice e chiaro.	
Artt. 13 e 14	Informazioni da fornire all'interessato	Agli interessati i cui Dati personali di Reveal sono sottoposti a trattamento deve essere fornita l'informativa sulla protezione dei dati	*"Soddisfazione dei requisiti di protezione dei dati"*, sezione B
Art. 15	Diritto di accesso	Su richiesta degli interessati, deve essere garantito l'accesso ai Dati personali di Reveal (con riserva di deroghe)	*"Soddisfazione dei requisiti di protezione dei dati"*, sezione J
Art. 16	Diritto di rettifica	Su richiesta degli interessati, i Dati personali di Reveal devono essere rettificati	*"Soddisfazione dei requisiti di protezione dei dati"*, sezione J
Art. 17	Diritto alla cancellazione	Su richiesta degli interessati, i Dati personali di Reveal devono essere cancellati, se il diritto risulta applicabile	*"Soddisfazione dei requisiti di protezione dei dati"*, sezione J
Art. 18	Diritto di limitazione	Su richiesta degli interessati, i Dati personali di Reveal devono essere limitati, se il diritto risulta applicabile	*"Soddisfazione dei requisiti di protezione dei dati"*, sezione J
Art. 19	Obbligo di notifica relativo alla rettifica, alla cancellazione o alla limitazione	Qualora pervenga una richiesta di rettifica, cancellazione o limitazione relativa ai Dati personali di Reveal, la richiesta deve essere notificata ai terzi a cui sono stati comunicati i dati	*"Soddisfazione dei requisiti di protezione dei dati"*, sezione J
Art. 20	Diritto alla portabilità dei dati	Su richiesta degli interessati, i Dati personali di Reveal devono essere trasmessi agli stessi (o a terzi nominati), se il diritto risulta applicabile	*"Soddisfazione dei requisiti di protezione dei dati"*, sezione J
Art. 21	Diritto di opposizione	Su richiesta degli interessati, i Dati personali di Reveal non devono più essere trattati, se il diritto risulta applicabile	*"Soddisfazione dei requisiti di protezione dei dati"*, sezione J
Art. 22	Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione	Le decisioni esclusivamente automatizzate relative a persone fisiche che	*"Soddisfazione dei requisiti di protezione dei dati"*, sezione L

		hanno effetti giuridici o effetti altrettanto significativi per gli interessati possono essere adottate solo in conformità all'articolo. 22	
Art. 23	Limitazioni	Nessuna rilevanza specifica	N/A
Art. 24	Responsabilità del Titolare del trattamento	Devono essere messe in atto misure tecniche e organizzative adeguate, volte a garantire (e dimostrare) che il trattamento sia conforme al GDPR.	*"Soddisfazione dei requisiti di protezione dei dati"*, in generale
Art. 25	Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita	Le questioni relative alla protezione dei dati dovrebbero essere affrontate sin dall'inizio e durante il ciclo di vita del trattamento dei Dati personali di Reveal e dovrebbero essere trattati i dati personali strattamente necessari al conseguimento della propria finalità	*"Soddisfazione dei requisiti di protezione dei dati"*, sezioni F e N
Art. 26	Contitolari del trattamento	Nessuna rilevanza specifica	N/A
Art. 27	Rappresentanti dei Titolari del trattamento o dei Responsabili del trattamento non stabiliti nell'Unione	Nessuna rilevanza specifica	N/A
Art. 28	Responsabile del trattamento	Si deve ricorrere unicamente a Responsabili del trattamento che presentino garanzie sufficienti per il trattamento dei Dati personali di Reveal e i Responsabili del trattamento devono essere soggetti ad obblighi contrattuali in tal senso	*"Soddisfazione dei requisiti di protezione dei dati"*, sezione I
Art. 29	Trattamento sotto l'autorità del Titolare del trattamento o del Responsabile del trattamento	Nessuna rilevanza specifica	N/A
Art. 30	Registro delle attività di trattamento	Il trattamento dei Dati personali di Reveal deve figurare nel registro delle attività di trattamento	*"Soddisfazione dei requisiti di protezione dei dati"*, sezione C

Art. 31	Cooperazione con l'autorità di controllo	Nessuna rilevanza specifica	N/A
Art. 32	Sicurezza del trattamento	Per proteggere la sicurezza dei Dati personali di Reveal devono essere messe in atto misure tecniche e organizzative adeguate	*"Soddisfazione dei requisiti di protezione dei dati"*, sezione I
Artt. 33 e 34	Notifica di violazione dei dati (all'autorità di controllo e agli interessati)	In caso di violazione dei dati personali che riguardino i Dati personali di Reveal, deve essere inviata una notifica alle autorità di controllo e agli interessati, se sono state raggiunte le soglie	*"Soddisfazione dei requisiti di protezione dei dati"*, sezione I
Artt. 35 e 36	Valutazione d'impatto sulla protezione dei dati e consultazione preventiva	Deve essere effettuata una valutazione d'impatto sulla protezione dei dati per il trattamento dei Dati personali di Reveal e può essere necessaria la consultazione con le autorità di controllo se il trattamento presenta rischi elevati e non attenuati per gli interessati.	*"Soddisfazione dei requisiti di protezione dei dati"*, sezione A
Artt. 37, 38 e 39	Responsabile della protezione dei dati	Rilevanza; Il responsabile della protezione dei dati deve essere nominato se le attività principali del Titolare del trattamento consistono nel monitoraggio "regolare e sistematico" degli interessati su vasta scala o nel trattamento su vasta scala di categorie particolari di dati o di dati relativi a reati.	*"Soddisfazione dei requisiti di protezione dei dati"*, sezione Q
Artt. 40, 41, 42 e 43	Codici di condotta, certificazione e accreditamento	Nessuna rilevanza specifica	N/A
Artt. 44 - 50	Trasferimenti	Qualsiasi trasferimento dei Dati personali di Reveal al di fuori del SEE verso paesi che non sono "adeguati" (ad esempio, ad altri fornitori di piattaforme o a società del gruppo) deve essere effettuato	"*FAQ su Reveal"*, sezione 6, e *"Soddisfazione dei requisiti di protezione dei dati"*, sezione K

		solo in presenza di un meccanismo di trasferimento o di una deroga.	
Artt. 51 - 59	Autorità di controllo e competenza, compiti, poteri e relazioni di attività	Nessuna rilevanza specifica	N/A
Artt. 60 - 67	Cooperazione e coerenza	Nessuna rilevanza specifica	N/A
Artt. 68 - 76	Comitato europeo per la protezione dei dati	Nessuna rilevanza specifica	N/A
Art. 77	Diritto di proporre reclamo all'autorità di controllo	Nessuna rilevanza specifica	N/A
Art. 78	Diritto a un ricorso giurisdizionale nei confronti dell'autorità di controllo	Nessuna rilevanza specifica	N/A
Artt. 79 - 82	Diritto a un ricorso giurisdizionale effettivo nei confronti del Titolare o Responsabile del trattamento e risarcimento	Nessuna rilevanza specifica	N/A
Artt. 83 - 84	Sanzioni amministrative pecuniarie e altre sanzioni	Nessuna rilevanza specifica	N/A
Artt. 85 - 91	Disposizioni relative a specifiche situazioni di trattamento	Nessuna rilevanza specifica	N/A
Artt. 92 - 93	Atti delegati e atti di esecuzione	Nessuna rilevanza specifica	N/A
Artt. 94 - 99	Disposizioni finali	Nessuna rilevanza specifica	N/A