AUTORIZZAZIONE AL TRATTAMENTO DEI DATI PERSONALI

Premesso che

- a decorrere dal 14 aprile 2016 è in vigore il Regolamento (UE) n. 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (d'ora innanzi anche "GDPR" o "Regolamento");
- in base a quanto previsto dagli artt. 29 e 32 paragrafo 4 del Regolamento e dall'art. 2-quaterdecies del d.lgs. 196/2003, le operazioni di trattamento possono essere effettuate solo da persone autorizzate che operano sotto la diretta autorità del Titolare, attenendosi alle istruzioni da questi impartite;
- per "trattamento", ai sensi dell'art. 4 paragrafo 2 del Regolamento, si intende "qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati";
- per "dati personali", ai sensi dell'art. 4 paragrafo 1 del Regolamento, si intende "qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); altresì si considera identificabile "la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale";
- per "dati particolari", ai sensi dell'art. 9 del Regolamento, si intende i dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
- ai fini del rispetto della normativa, ciascuna persona che tratta dati personali deve essere autorizzata e istruita in merito agli obblighi normativi per la gestione dei suddetti dati durante lo svolgimento delle proprie mansioni;
- tale autorizzazione non comporta alcuna modifica della qualifica professionale o delle mansioni assegnate.

Tutto quanto sopra premesso

AUTOMOBILE CLUB UDINE, C.F./P.IVA 00160740304, con sede in Udine, Viale Tricesimo n°46, in qualità di Titolare del Trattamento, (di seguito anche "ACU" o "Titolare") individua l'area

GESTORE DELLE SEGNALAZIONI

e contestualmente

AUTORIZZA

ciascun soggetto preposto alla suddetta area (di seguito convenzionalmente indicato come "Addetto" o "Autorizzato") al trattamento dei dati personali.

Compiti e responsabilità del gestore delle segnalazioni

Il Gestore delle Segnalazioni è tenuto a eseguire i propri compiti seguendo scrupolosamente quanto delineato nella "Policy Whistleblowing". Questa policy specifica in modo dettagliato i ruoli e le responsabilità assegnate al Gestore, garantendo che ogni azione e procedura sia condotta in piena aderenza alle normative vigenti sulla protezione dei dati e sulla gestione delle segnalazioni.
È fondamentale che il Gestore si attenga alle direttive esposte nella policy per assicurare l'integrità del processo di segnalazione e la protezione dei dati personali degli interessati, oltre a garantire che le segnalazioni vengano trattate con il massimo livello di confidenzialità e sicurezza.

In particolare, i compiti del Gestore delle Segnalazioni sono:

- Ricezione delle Segnalazioni: accogliere tutte le segnalazioni pervenute tramite i canali dedicati, garantendo l'anonimato del segnalante, salvo che la divulgazione dell'identità sia consensuale o imposta da obblighi legali.
- Valutazione Preliminare: effettuare una prima valutazione delle segnalazioni per determinare la loro ammissibilità secondo i criteri stabiliti dalla Policy Whistleblowing, scartando quelle manifestamente infondate o non pertinenti.
- Indagine: condurre o supervisionare le indagini sulle segnalazioni ritenute ammissibili, assicurando un approccio oggettivo e la protezione dei dati personali, in linea con il GDPR e il D.Lgs. 196/03.
- Risposta al Segnalante: fornire riscontri al segnalante in merito allo stato di avanzamento della segnalazione e delle eventuali misure adottate, rispettando i termini previsti dalla normativa e dalla policy interna.
- Formazione e Aggiornamento: partecipare a sessioni di formazione sull'applicazione della Policy Whistleblowing e aggiornarsi costantemente sulle evoluzioni normative e sulle best practice relative alla gestione delle segnalazioni di illeciti.
- Riservatezza e Protezione dei Dati: mantenere la massima riservatezza su tutte le informazioni gestite, compiendo tutte le azioni necessarie a proteggere i dati personali in conformità alle disposizioni del GDPR e del D.Lgs. 196/03.

Istruzioni per l'Autorizzato:

- svolgere il trattamento dati esclusivamente per fini legati alla gestione delle segnalazioni, seguendo le direttive del Titolare del trattamento e utilizzando eventuali strumenti elettronici forniti allo scopo;
- seguire rigorosamente le procedure di sicurezza per la protezione dei dati predisposte dal Titolare;
- trattare i dati personali in modo lecito e corretto, assicurando che siano pertinenti e non eccedenti le necessità del trattamento;
- mantenere la riservatezza su tutte le informazioni acquisite durante l'attività di Gestore delle Segnalazioni;
- assicurare che tutte le segnalazioni siano trattate in modo confidenziale e che l'identità del segnalante sia protetta, conformemente a quanto stabilito dal D.Lgs. 24/23;
- garantire che le segnalazioni siano gestite senza ritardi ingiustificati e con un alto livello di sicurezza delle informazioni, prevenendo accessi non autorizzati e divulgazioni non autorizzate.
- ricevere, trattare e conservare le segnalazioni in modo sicuro e confidenziale, proteggendo l'identità del segnalante e le informazioni relative alla segnalazione;
- fornire feedback al segnalante entro i termini previsti dalla normativa, specificando lo stato della segnalazione e le azioni intraprese;
- cooperare con le autorità competenti e, se del caso, trasferire le segnalazioni alle autorità esterne preposte, garantendo il rispetto delle procedure di comunicazione sicura;
- mantenere un registro delle segnalazioni ricevute, delle indagini svolte e dei risultati ottenuti, assicurando che tale registro sia accessibile solo alle persone autorizzate;
- adottare tutte le misure necessarie per prevenire ritorsioni contro il segnalante, garantendo la protezione dei diritti del segnalante in conformità con il D.Lgs. 24/23;
- informare tempestivamente il Titolare del trattamento in caso di violazioni della sicurezza dei dati personali, seguendo le procedure previste dal GDPR e dalle linee guida interne.

Ambito di trattamento

Il Gestore delle Segnalazioni avrà accesso a dati personali e identificativi, dati particolari, e dati relativi a eventuali reati o condanne penali, necessari per l'esecuzione delle sue funzioni.

Procedura operativa in caso di violazione dei dati personali: indicazioni per gli autorizzati

Secondo quanto previsto dall'art. 4 del GDPR, per violazione dei dati personali si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.
Alcuni possibili esempi:

- l’accesso o l’acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l’impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

Cosa fare se si verifica un data breach

Nel caso in cui un Autorizzato ritenga che possa essersi verificata una violazione dei dati personali nei termini sopra descritti, dovrà inviare prontamente una comunicazione al Titolare contenente almeno:

- data e orario in cui la Violazione dei Dati si è verificata
- sommaria descrizione della Violazione dei dati personali.

Sarà compito del Titolare verificare l’accaduto per decidere se attivare la procedura prevista dall’articolo 33 del GDPR.

L’Autorizzato si impegna a mantenere il segreto nei confronti di chiunque, per quanto riguarda fatti, informazioni, dati e atti di cui venga a conoscenza nell'espletamento dell’incarico ricevuto. In particolare, si impegna a non cedere, non consegnare, non copiare, non riprodurre, non comunicare, non divulgare, non rendere disponibili in qualsiasi modo o a qualsiasi titolo a terzi, le informazioni acquisite nell'esecuzione del servizio. L’Autorizzato assicura, inoltre, che il trattamento di dati sarà effettuato ai soli fini dell’espletamento dell’incarico ricevuto.

La cessazione, a qualsiasi titolo, del rapporto di lavoro/collaborazione comporta, automaticamente e senza necessità di comunicazione, la perdita dell’autorizzazione a trattare dati personali. Gli obblighi relativi alla riservatezza, alla comunicazione e alla diffusione dovranno essere osservati anche in seguito a modifica dell’incarico e/o cessazione del rapporto di lavoro/collaborazione.

Udine 31 ottobre 2024

Per il Titolare
Automobile Club Udine
f.to Il Presidente
Dott. Gianfranco Romanelli

L’Autorizzato

f.to Direttore
Dott.ssa Maddalena Valli