AUTOMOBILE CLUB LECCO
PROCEDURA PER LA GESTIONE DEI CASI DI VIOLAZIONE DEI DATI PERSONALI
(*PROCEDURA DATA BREACH* - art.17 Regolamento privacy AC)

AMBITO DI APPLICAZIONE

La presente **procedura di gestione delle violazioni di dati personali** (**PROCEDURA *DATA BREACH***) definisce le attività che l'Automobile Club Lecco, in qualità di Titolare del trattamento, deve porre in essere in caso di violazione di dati personali.

L'AC favorisce la piena conoscibilità della Procedura *data breach* da parte di tutti i dipendenti anche mediante pubblicazione nella sezione "Utilita" del sito Istituzionale dell'AC, per consentirne l'opportuna conoscenza e consultazione dall'esterno, da parte di coloro che potrebbero rilevare/sospettare violazioni di dati personali che coinvolgo l'AC.

Costituiscono violazioni di dati personali (di seguito, violazione della sicurezza o *data breach*) gli incidenti di sicurezza o qualsiasi altro evento che comporti in modo accidentale o illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata ovvero l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dall'AC**.**

Le violazioni di dati personali possono essere:
a) **violazioni della riservatezza,** si hanno in presenza di divulgazione o di accesso non autorizzato o accidentale ai dati personali. Sono tali, ad esempio, l'invio per errore ovvero non dovuto di dati personali particolari, la divulgazione di dati personali oltre il perimetro definito dalla normativa di riferimento o nell'informativa resa all'Interessato, l'accesso non autorizzato da parte di un dipendente o in conseguenza di un attacco informatico a dati personali o altre informazioni tali che rendono identificabile l'Interessato, l'impiego dei dati personali trattati per finalità illecite;
b) **violazioni dell'integrità**, si verificano nel caso in cui avvenga una modifica non autorizzata o accidentale dei dati personali trattati;
c) **violazioni della disponibilità**, si hanno in caso di perdita o di distruzione accidentale o non autorizzata dei dati personali. Sono tali, ad esempio, l'eliminazione accidentale di file critici, la perdita di dati causati da un attacco *ransomware* o la perdita di chiavi di crittografia.

SOGGETTI COINVOLTI

Il Titolare, nella persona del Presidente quale legale rappresentante dell'AC, è responsabile della gestione del *data breach* e, unitamente al Referente, ogni qualvolta venga direttamente a conoscenza di un *data breach* ovvero quando ne sia informato, a qualsiasi titolo, si attiva immediatamente per adottare ogni misura idonea a limitare l'estensione della violazione e a contenere il rischio (ad esempio, sospensione *account* utente compromesso, blocco accesso non autorizzato).
Il Responsabile del trattamento - nei casi in cui l'AC lo abbia nominato - è tenuto a notificare al Titolare senza ingiustificato ritardo e, comunque, non oltre 24 (ventiquattro) ore da quando ne abbia avuto conoscenza, qualsiasi distruzione, perdita, alterazione, divulgazione o accesso non autorizzato ai dati personali ovvero sospetti che si stia verificando una violazione di sicurezza presso la propria struttura. In tali casi, il Responsabile assiste il Titolare medesimo nell'adempimento di tutti obblighi normativamente previsti.
Il personale che presta servizio o collabora, a qualsiasi titolo, presso l'AC è tenuto a segnalare, senza indugio, al Titolare e per opportuna conoscenza al DPO ogni incidente di sicurezza – rilevato o sospettato - che ritenga possa riguardare dati personali detenuti o comunque trattati dall'AC

stesso, avvalendosi dei canali di contatto a ciò dedicati. Analogo obbligo grava sulle società di servizi dell'AC e su ogni altro soggetto che fornisce all'AC servizi informatici o di altra natura.

In caso di conoscenza o di segnalazione di violazioni di sicurezza da parte di soggetti terzi (ad es. Interessato, Garante Privacy, stampa), il Titolare, avvalendosi del Referente, si attiva - senza ritardo – per informare il DPO e per raccogliere ogni informazione utile per individuare l'evento e verificarne la fondatezza. Al contempo il Titolare adotta le misure più idonee per circoscrivere i rischi dando seguito a tutti gli adempimenti normativamente previsti.

Canali di segnalazione: Ogni evento rilevato o presunto di *data breach* va segnalato senza ritardo alla casella di posta elettronica info@acilecco.it, per conoscenza, al *Data protection Officer* contattabile all'indirizzo *e-mail* m.annibalidpo@aci.it.,

OBBLIGHI DEL TITOLARE: PROCEDURA DI NOTIFICA E SEGNALAZIONE AL GARANTE PRIVACY

Il Titolare che rilevi, venga a conoscenza o sia informato di un incidente di sicurezza:

I – ne dà immediata e formale comunicazione scritta al DPO, qualora non sia stato già informato dal soggetto che ha segnalato la violazione di sicurezza;
II – valuta i fatti e stabilisce se si è verificata una violazione di dati personali e in caso affermativo:
A) valuta il rischio per gli Interessati, in termini di:
- perdita del controllo dei dati degli Interessati;
- limitazioni dei diritti/discriminazione;
- furto o usurpazione di identità;
- perdite finanziarie/danno economico, sociale o reputazionale (sia per l'Interessato che per il Titolare);
- decifratura non autorizzata dei dati;
- perdita di riservatezza dei dati personali particolari (es. dati relativi alla salute o a condanne penali).

IV – Obbligo di verbalizzazione e documentazione delle attività. Tutte le attività e le riunioni aventi ad oggetto un *data breach* devono essere verbalizzate (per iscritto) e opportunamente documentate. Ad ogni segnalazione viene assegnato un numero identificativo, formato da un numero/anno e, non appena possibile, si procede alla protocollazione.

V – Sanzioni per omessa notifica al Garante Privacy. La violazione dell'obbligo di notifica del *data breach* al Garante Privacy e/o l'omessa comunicazione agli Interessati, ove sussistano i requisiti stabiliti dagli artt. 33 e 34 del GDPR, può comportare l'applicazione in capo al Titolare e al Responsabile del trattamento di sanzioni amministrative pecuniarie a norma dell'art.83 del GDPR e/o di misure correttive ai sensi dell'art. 58, par. 2, dello stesso Regolamento.