Allegato al Regolamento Privacy AC

AUTOMOBILE CLUB UDINE

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 Udine, 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 e dei Responsabili del trattamento, anche mediante pubblicazione sul 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/Direttore**, 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). La gestione operativa delle violazioni è curata dal Referente/Direttore. In caso di assenza o impedimento del Referente/Direttore, si applica quanto previsto dall'art. 14 del Regolamento Privacy AC.

Il **Responsabile del trattamento -** nei casi in cui l'AC lo abbia nominato - è tenuto a notificare al Titolare senza ingiustificato ritardo e, comunque, entro il termine stabilito nell'atto di nomina,

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 Referente/Direttore 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/Direttore, 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 automobileclubudine@legalmail.it o segreteia@acu.ud.it, per conoscenza, al *Data protection Officer* contattabile all'indirizzo *e-mail* m.annibalidpo@aci.it., al contempo avvisando telefonicamente il Referente/Direttore.

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).

Ai fini della valutazione, il Referente/Direttore raccoglie, per quanto possibile, le informazioni utili, quali la data e l'ora della violazione e della sua scoperta, la tipologia dei dati e le categorie di Interessati coinvolti e il loro numero approssimativo, la causa della violazione, i sistemi coinvolti e le misure già adottate, avvalendosi, ove necessario, del supporto del DPO, dei Responsabili del trattamento e di consulenti esterni.

B) **se** la **violazione dei dati personali può ragionevolmente** comportare un **rischio per i diritti e le libertà delle persone fisiche,** il Titolare **notifica la violazione al Garante per i dati**

personali (Garante Privacy), mediante la procedura telematica resa disponibile dal Garante, **senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza o ha ricevuto la segnalazione.** Se la notifica non viene effettuata entro 72 ore, il Titolare indica i motivi del ritardo.

La comunicazione di notifica della violazione al Garante privacy deve riportare almeno:

- una descrizione della natura della violazione di dati personali, compreso il numero approssimativo e le categorie di Interessati nonché il numero di registrazioni di dati personali in questione;
- il nome e i dati di contatto del Responsabile della protezione dati o di altro Referente/Direttore per acquisire maggiori informazioni;
- una descrizione delle probabili conseguenze della violazione di dati personali;
- una descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio al *data breach* e quelle, se del caso, previste per attenuarne i possibili effetti negativi.

Qualora non sia possibile fornire tali informazioni contestualmente, le stesse possono essere trasmesse successivamente, senza ulteriore ingiustificato ritardo.

III valuta **se la violazione comporti un rischio elevato per i diritti e le libertà degli individui:**

a) In caso **affermativo**:

il Titolare deve, senza ingiustificato ritardo, informare l'Interessato della violazione e, ove richiesto, fornire informazioni sulle misure che può adottare per proteggersi dalle conseguenze della violazione. In caso di omessa comunicazione, il Garante Privacy può richiedere o disporre che venga effettuata la comunicazione all'Interessato. La comunicazione descrive con un linguaggio semplice e chiaro la natura della violazione e contiene almeno il nome e i dati di contatto del DPO, la descrizione delle probabili conseguenze della violazione e delle misure adottate o di cui si propone l'adozione.

Il **Titolare non è tenuto a darne comunicazione all'interessato** quando ricorra una delle seguenti ipotesi:

1) il Titolare del trattamento ha adottato misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione (ad esempio, misure che rendono i dati personali incomprensibili a coloro che non siano autorizzati ad accedervi, come la cifratura);

2) il Titolare del trattamento ha successivamente adottato misure idonee a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

3) la comunicazione agli Interessati richiederebbe sforzi sproporzionati. In questo caso, il Titolare effettua una comunicazione pubblica o altra simile, tramite la quale gli interessati vengono informati con efficacia equivalente.

b) In **caso negativo** (rischio non elevato), **il Titolare** non è tenuto a comunicare la violazione agli Interessati, ferma restando la notifica al Garante Privacy ove dovuta ai sensi del punto II, lettera B), e adotta le misure più idonee per documentare e conservare gli atti relativi all'evento di *data breach.*

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. Ogni violazione è altresì annotata nel Registro degli incidenti data breach, anche quando non sia stata notificata al Garante Privacy, con l'indicazione delle circostanze, delle conseguenze e dei provvedimenti adottati nonché, in caso di mancata o tardiva notifica, delle relative ragioni.

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.

VI Misure successive. Conclusa la gestione della violazione, il Referente/Direttore valuta, anche con il supporto dei Responsabili del trattamento e del DPO, l'adozione di misure idonee a prevenire il ripetersi di eventi analoghi.