All. A

AUTOMOBILE CLUB BRESCIA

REGOLAMENTO

IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Approvato con delibera del Presidente n. 2/2025 del 9 settembre 2025

INDICE

DISPOSIZIONI GENERALI **2**

Art. 1 - Finalità e ambito di applicazione 3

Art. 2 - Titolare e Contitolare del trattamento dei dati personali 3

Art. 3 - Responsabile del trattamento 4

Art. 4 - Interessato 4

Art. 5 - Dato personale 4

Art. 6 - Trattamento dei dati 5

OBBLIGHI DEL TITOLARE **5**

Art. 7 - Liceità, correttezza e durata del trattamento 5

Art. 8 - Informativa 6

Art. 9 - Richiesta del consenso 6

Art. 10 - Trattamento dei dati particolari 7

Art. 11 - Esercizio dei diritti da parte dell'Interessato 8

Art. 12 - Formazione 9

SISTEMA DI GESTIONE DEI DATI PERSONALI (SISTEMA DATA GOVERNANCE AC) **9**

Art. 13 - Articolazione del sistema 9

Art. 14 - Organigramma privacy 10

Art. 15 - Procedura per la gestione delle richieste degli Interessati 10

Art. 16 - Registro delle attività di trattamento e valutazione d'impatto 11

Art. 17 - Procedura di notifica e comunicazione in caso di violazione dei dati personali (Procedura data breach) 11

Allegati:

All. n. 1 Procedura per la gestione delle richieste degli Interessati

All. n. 2 Procedura di notifica e comunicazione in caso di violazione dei dati personali (Procedura data breach)

DISPOSIZIONI GENERALI

Art. 1
Finalità e ambito di applicazione

1. Il presente Regolamento (Regolamento Privacy AC) individua, nell'ambito dell'Automobile Club, i soggetti tenuti al rispetto dei principi e delle disposizioni dettate dal Regolamento UE 2016/679 (GDPR) in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati, nonché delle altre disposizioni vigenti in materia, per assicurare tutela piena ed effettiva ai diritti dell'Interessato.

2. A tal fine, il Regolamento Privacy AC, quale misura organizzativa adottata ai sensi degli artt. 24 e 25 del GDPR, stabilisce il sistema di gestione dei dati personali adottato dall'AC (Sistema Data Governance AC) con riferimento alle attività di trattamento di dati personali effettuate nella veste di Titolare, Contitolare o Responsabile del trattamento, sia nell'assolvimento della propria missione istituzionale, sia nello svolgimento dei servizi delegati dallo Stato e da altre Amministrazioni.

Art. 2
Titolare e Contitolare del trattamento dei dati personali

1. L'AC è il Titolare (di seguito, anche solo Titolare) del trattamento dei dati personali di competenza, ai sensi dell'art. 4, par.7, del GDPR, ogni qualvolta determina le finalità e i mezzi di trattamento dei dati personali.

2. L'AC, nella persona del Presidente quale legale rappresentante, ai sensi dell'art. 5, par.2 del GDPR, assicura il rispetto dei principi di liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione nella conservazione, integrità e riservatezza di cui all'art. 5, par.1 del GDPR, e adotta misure idonee a comprovarlo in ottemperanza al principio di "responsabilizzazione" (accountability).

3. Il Titolare è tenuto al rispetto degli obblighi generali previsti dagli artt. 24 e segg. del GDPR e a predisporre ed aggiornare il registro delle attività di trattamento svolte sotto la propria responsabilità (Registro dei Trattamenti).

4. L'AC assume il ruolo di Contitolare del trattamento, ai sensi dell'art.26 del GDPR, quando determina in modo congiunto, con uno o più Titolari, le finalità e i mezzi del trattamento dei dati personali. A tal fine, con accordo interno scritto, i Contitolari stabiliscono in modo trasparente, così come previsto dall'art.26 del GDPR, sia i rispettivi ruoli e responsabilità per assicurare l'osservanza degli obblighi derivanti dal GDPR stesso e l'esercizio dei diritti degli interessati, sia la spettanza degli oneri di comunicazione delle informazioni previsti dagli artt.13 e 14 del GDPR.

Art. 3
Responsabile del trattamento

1. Nel caso in cui vi siano trattamenti che debbano essere effettuati per conto dell'AC (Titolare), l'AC nomina, con contratto o con altro atto giuridico scritto, il Responsabile del trattamento individuandolo, ai sensi dell'art. 28 del GDPR, tra i soggetti che assicurano adeguate garanzie di trattamento dei dati in conformità al GDPR e di piena tutela dei diritti degli Interessati.

2. L'AC può, a sua volta, essere nominato, da altro Titolare, Responsabile del trattamento quando svolga un trattamento di dati personali per conto di altro soggetto giuridico, pubblico o privato.

Art. 4
Interessato

1. L'Interessato è la persona fisica cui si riferiscono i dati personali oggetto di trattamento.

Art. 5
Dato personale

1. E' dato personale, ai sensi del GDPR, qualsiasi informazione che identifichi o renda identificabile una persona fisica, come il nome, il numero di identificazione (ad es., numero di telefono personale, Codice Fiscale, numero di matricola, codici/numeri identificativi dell'attività *on-line* tra cui l'indirizzo *Internet Protocol* e simili) i dati relativi al domicilio, ubicazione o residenza, gli elementi caratteristici o distintivi dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

2. Ai sensi dell'art. 4 del GDPR, sono altresì dati personali quelli:

- relativi alla salute, vale a dire attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni sullo stato di salute della stessa;

- genetici, vale a dire relativi alle caratteristiche genetiche ereditarie o acquisite da una persona fisica, che forniscono informazioni univoche sulla sua fisiologia o sulla sua salute e che risultano dall'analisi di un suo campione biologico;

- biometrici, vale a dire ottenuti con un trattamento tecnico specifico e relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona, che ne consentono o confermano l'identificazione univoca, come l'immagine facciale o i dati dattiloscopici.

Art. 6
Trattamento dei dati

1. Ai sensi dell'art. 4 del GDPR, costituisce attività di trattamento dati qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

OBBLIGHI DEL TITOLARE

Art. 7
Liceità, correttezza e durata del trattamento

1. Qualsiasi trattamento di dati personali deve essere lecito e corretto.

2. Avuto riguardo agli ambiti istituzionalmente presidiati dall'AC, il Titolare adotta ogni misura tecnica od organizzativa necessaria a garantire la liceità e correttezza del trattamento. In linea con quanto previsto dall'art.6 del GDPR, è lecito il trattamento che si fonda su una base giuridica pertinente, prevista dal diritto dell'Unione europea o, nell'ordinamento interno, da una norma di legge o regolamentare e, in particolare, su una delle seguenti condizioni:

- sull'assolvimento degli obblighi legali cui è tenuto il Titolare;
- sulla necessità di conclusione o esecuzione di un contratto di cui l'Interessato sia parte, ovvero sull'esecuzione di misure precontrattuali adottate su richiesta dell'interessato;
- sull'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
- sul consenso dell'Interessato al trattamento per una o più specifiche finalità.

3. L'AC adotta le misure più opportune per rendere conoscibile all'Interessato, in modo trasparente e facilmente accessibile, l'identità e i recapiti del Titolare e le modalità con cui lo stesso raccoglie, utilizza o altrimenti tratta i dati personali dell'Interessato; inoltre, si adopera affinché l'Interessato sia posto nelle condizioni di conoscere i propri diritti, relativi al trattamento, e le modalità di esercizio degli stessi.

4. Il Titolare garantisce che i dati personali raccolti e trattati sono adeguati, pertinenti e limitati a quanto necessario per le finalità di trattamento e che vengono trattati solo se la finalità non è ragionevolmente conseguibile con altri

mezzi.

5. Il Titolare assicura che i dati personali sono conservati per il tempo minimo necessario. A tal fine, il Titolare stabilisce, per ciascun trattamento, un termine per la cancellazione e distruzione dei dati personali raccolti, effettuando verifiche periodiche sulla necessarietà della conservazione dei dati raccolti.

6. Il Titolare adotta misure adeguate a garantire la correzione o cancellazione dei dati inesatti, la sicurezza e riservatezza del trattamento nonché ad impedire l'accesso o l'utilizzo non autorizzato dei dati personali.

Art. 8
Informativa

1. In tutti i casi in cui vengano raccolti dati personali presso l'Interessato o presso altri soggetti, il Titolare fornisce allo stesso tutte le informazioni previste, rispettivamente, agli artt. 13 e 14 del GDPR, qualunque siano le condizioni di liceità o basi giuridiche del trattamento di cui all'art. 6 del GDPR.

2. L'informativa racchiude tutte le informazioni indicate al comma 1, ha contenuti semplici ed intellegibili, soprattutto quando i destinatari sono minori, ed è facilmente accessibile. A tal fine, viene resa per iscritto o in formato elettronico, tramite lo stesso sito *web* o le *app* istituzionali se i servizi sono offerti *on-line*, adottando modalità di comunicazione che possono tracciare la presa visione dell'informativa da parte dell'Interessato ovvero dare evidenza dell'avvenuta comunicazione della stessa all'Interessato.

Art. 9
Richiesta del consenso

1. Qualora non ricorrano le condizioni di liceità, o basi giuridiche, disciplinate all'art. 6 del GDPR o dal D. Lgs. 30 giugno 2003, n. 196 (di seguito, Codice privacy), Parte II, e dalle altre disposizioni normative vigenti, l'AC, nella sua veste di Titolare, acquisisce il consenso da parte dell'Interessato quale condizione di liceità del trattamento dei dati personali comuni, rispettando le prescrizioni di cui agli artt. 5 e 7 del GDPR.

2. Il Titolare assicura, in particolare, che l'Interessato manifesti il consenso mediante atto positivo, da cui possa evincersi l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, attraverso una dichiarazione scritta oppure con strumenti elettronici, mediante la richiesta di selezione di una specifica casella. Se il trattamento ha più finalità, il consenso viene chiaramente richiesto e acquisito dall'Interessato per ciascuna di esse.

3. Per il principio di responsabilità, in particolare, il Titolare adotta misure organizzative tali da poter dimostrare, in qualsiasi momento:

- che l'Interessato ha espressamente acconsentito al trattamento;

- che il consenso è informato, essendo state rese chiaramente riconoscibili almeno l'identità del Titolare e le specifiche finalità del trattamento;
- di aver posto l'Interessato nelle condizioni di scegliere liberamente, senza subire alcun pregiudizio, di prestare o di rifiutare il proprio consenso a uno specifico trattamento.

4. Al fine di rendere significativo il consenso del minore che abbia compiuto 14 anni, il Titolare, in occasione dell'offerta diretta di servizi *on-line* (c.d. servizi della società dell'informazione), fornisce tutte le informazioni relative al trattamento con un linguaggio particolarmente chiaro, semplice, conciso ed esaustivo, facilmente accessibile e comprensibile dal minore stesso (cfr. art. 8 GDPR e art. 2 *quinquies* del Codice privacy).

5. Il Titolare adotta misure organizzative che consentono all'Interessato di revocare il consenso prestato, in qualsiasi momento, senza alcun condizionamento e con la stessa facilità con cui è stato accordato.

Art. 10
Trattamento dei dati particolari

1. Il Titolare impartisce, per iscritto, specifiche istruzioni ai propri collaboratori e a tutto il personale autorizzato al trattamento di categorie particolari di dati di cui all'art. 9 del

2. GDPR (dati relativi alla salute o alla vita sessuale/orientamento sessuale; dati personali che rivelino l'origine razziale/etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica), fermo restando che il trattamento è ammesso:

- per motivi di interesse pubblico rilevante, ai sensi dell'art. 2-*sexies* Codice privacy, nei soli casi previsti dal diritto dell'Unione europea o, nell'ordinamento interno, da disposizioni di legge o di regolamento o da atti amministrativi generali che specificano i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi della persona fisica (a titolo esemplificativo, accesso ai documenti amministrativi, accesso civico, archiviazione nel pubblico interesse o per fini di ricerca storica);
- per assolvere gli obblighi ed esercitare diritti del Titolare o dell'interessato in materia di diritto del lavoro e della sicurezza sociale ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria;
- qualora l'Interessato abbia manifestato, in modo esplicito, il proprio consenso al trattamento;
- qualora riguardi dati personali resi manifestamente pubblici dall'interessato.

3. Il Titolare adotta misure organizzative che assicurino il rispetto degli obblighi di legge e che siano in grado di comprovarlo.

4. Il Titolare impartisce, per iscritto, specifiche istruzioni ai propri collaboratori e a tutto il personale autorizzato al trattamento dei dati personali relativi a condanne penali e reati, ai sensi dell'art. 10 del GDPR, adottando misure organizzative che assicurino che il trattamento venga effettuato solamente sotto il controllo dell'Autorità pubblica, nei soli casi in cui è autorizzato dal diritto dell'Unione Europea o è previsto da una norma di legge dell'ordinamento giuridico nazionale, adottando idonee garanzie per tutelare i diritti e le libertà degli interessati, come specificato all'art. 2-*octies* del Codice privacy.

Art. 11
Esercizio dei diritti da parte dell'Interessato

1. Ai sensi dell'art. 12 del GDPR, l'AC, in qualità di Titolare, adotta misure organizzative che consentono, con modalità facilmente accessibili, l'esercizio dei diritti riconosciuti all'Interessato (artt. 15-22 GDPR), quali:

- diritto ad ottenere la conferma che sia in corso un trattamento di dati che riguardano l'Interessato e, in caso di esercizio di questo diritto, l'accesso ai dati personali ed alle informazioni indicate dall'art. 15, par. 1 del GDPR;
- diritto ad ottenere, ai sensi dell'art. 16 del GDPR, la rettifica dei dati personali inesatti che riguardano l'Interessato, senza ingiustificato ritardo, nonché ad ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa;
- diritto ad ottenere la cancellazione dei dati personali che riguardano l'Interessato (cd. diritto all'oblio), senza ingiustificato ritardo, nel rispetto delle condizioni e secondo le modalità indicate dall'art. 17 del GDPR;
- diritto ad ottenere la limitazione (temporanea) del trattamento, al ricorrere di una delle ipotesi indicate dall'art. 18 del GDPR, secondo le modalità indicate nello stesso articolo;
- diritto ad ottenere, ai sensi dell'art. 19 del GDPR, la comunicazione, a ciascuno dei destinatari cui sono trasmessi i dati personali dell'Interessato, di eventuali rettifiche, cancellazioni o limitazioni del trattamento, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato per l'AC;
- diritto di ricevere, ai sensi dell'art. 20 del GDPR, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che riguardano l'Interessato, forniti dallo stesso al Titolare, nei soli casi in cui il trattamento si basa sul consenso o su un contratto ed è effettuato con mezzi automatizzati, e il diritto a trasmettere i medesimi dati ad un altro Titolare senza impedimenti (cd. portabilità dei dati). Qualora tecnicamente possibile, il diritto alla portabilità dei dati comprende anche il diritto di ottenere la trasmissione diretta dei dati personali da un Titolare del trattamento all'altro Titolare;
- diritto di opporsi, alle condizioni e nel rispetto dei limiti previsti dall'art. 21 del GDPR, al trattamento dei dati personali che riguardano l'Interessato. In caso di opposizione, l'AC si astiene dal trattare ulteriormente i dati salvo che

dimostri l'esistenza di motivi legittimi oppure ciò sia necessario per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, secondo quanto previsto dallo stesso art. 21;

- diritto a non essere sottoposto, ai sensi dell'art. 22 del GDPR, a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che riguardano l'Interessato o che incida in modo analogo significativamente sulla sua persona, salvo quanto previsto dallo stesso art. 22.

2. Il Titolare impartisce istruzioni ai propri collaboratori e al personale autorizzato al trattamento dei dati personali e adotta adeguate misure organizzative tali da assicurare, in caso di dati personali concernenti persone decedute, l'esercizio dei relativi diritti, ai sensi dell'art. 2-*terdecies* del Codice privacy, da parte di chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario o per ragioni familiari meritevoli di protezione.

Art. 12
Formazione

1. Il Titolare organizza periodicamente sessioni e interventi formativi specifici in materia di trattamento e protezione dei dati personali, rivolti al personale e ai propri collaboratori che partecipano ai trattamenti ed alle connesse attività di controllo.

SISTEMA DI GESTIONE DEI DATI PERSONALI (SISTEMA DATA GOVERNANCE AC)

Art. 13
Articolazione del sistema

1. In linea con le previsioni normative di cui all'art. 24 GDPR e all'art. 2-*quaterdecies* del Codice privacy, l'AC si dota di un proprio sistema di gestione dei dati personali (Sistema Data Governance AC) che comprende l'adozione di misure organizzative quali la *Procedura per la gestione delle richieste degli Interessati* (All. 1), la *Procedura per la gestione dei casi di violazione dei dati personali* (Procedura data breach AC) (All. 2), l'*Organigramma privacy AC Brescia*, il *Registro delle attività di Trattamento*, il *Registro degli incidenti data breach*.

2. Il sistema Data Governance AC è adottato dal Presidente dell'AC, in qualità di legale rappresentante, che ne cura anche i successivi aggiornamenti.

Art. 14
Organigramma privacy

1. L'Organigramma privacy individua, nell'ambito dell'AC, le figure di Referente, Designato e Autorizzato e i rispettivi ruoli, funzioni, rapporti gerarchici nonché le relative responsabilità afferenti all'intero ciclo dell'attività di trattamento di dati personali, così come specificato nei rispettivi atti di nomina di cui all'Organigramma privacy.

2. Il Direttore dell'AC riveste la funzione di Referente, giusta nomina del Presidente dell'AC stesso quale Titolare del trattamento. Tenuto conto dell'organizzazione della Struttura, il Referente nomina tra i propri dipendenti i Designati e gli Autorizzati al trattamento.

3. Il Designato al trattamento dei dati personali, titolare di posizione organizzativa o di polo funzionale, è nominato dal Referente con atto formale scritto e lo coadiuva nell'esecuzione delle proprie mansioni indicate nell'atto di nomina.

4. L'Autorizzato al trattamento dei dati personali è nominato con atto formale del Referente, ha accesso ai dati la cui conoscenza sia strettamente necessaria per lo svolgimento dei compiti assegnati e svolge le mansioni stabilite nell'atto di nomina.

Art. 15
Procedura per la gestione delle richieste degli Interessati

1. L'AC si dota di una procedura per l'esercizio dei diritti riconosciuti agli Interessati dagli artt. 15-22 del GDPR, che garantisce la certezza della data nell'acquisizione delle richieste, l'identificazione dell'Interessato richiedente, l'accettabilità delle richieste nel rispetto delle limitazioni all'esercizio dei diritti stabilite dagli artt. 2 *undecies* - 2 *terdecies* del Codice privacy, il tracciamento dei tempi di risposta nonché la verifica del destinatario della documentazione prodotta in adempimento alle richieste.

2. La "Procedura per la gestione delle richieste degli Interessati" (All. 1) è pubblicata con tale denominazione sul sito web istituzionale dell'AC, sezione "Protezione Dati Personali", ed è corredata da un "Modulo" che gli Interessati possono impiegare per la presentazione delle proprie richieste.

3. L'AC risponde, in forma scritta e preferibilmente - salvo diversa indicazione dell'Interessato - con strumenti elettronici che ne favoriscano l'accessibilità, a tutte le richieste degli Interessati senza ingiustificato ritardo e, comunque, entro un mese dal ricevimento delle istanze, anche nei casi in cui tali istanze sono pervenute con modalità o canali diversi da quelli indicati nella procedura ovvero non vengono accolte.

4. Nei casi di particolare complessità o a causa del numero di richieste pervenute, il termine di risposta può essere prorogato di due mesi, dando comunicazione all'interessato della proroga e dei motivi della sua adozione

entro un mese dal ricevimento della richiesta, ai sensi dell'art. 12, par. 3 del GDPR.

5. In considerazione dell'oggetto della richiesta dell'interessato, l'AC provvede al riscontro direttamente oppure, ove necessario, avvalendosi della consulenza del DPO.

Art. 16
Registro delle attività di trattamento e valutazione d'impatto

1. L'AC predispone e tiene costantemente aggiornato il *Registro delle attività di trattamento* svolte sotto la propria responsabilità, in qualità di Titolare ovvero in qualità di Responsabile del trattamento per conto di altro Titolare, inserendo tutte le informazioni previste dall'art. 30 del GDPR.

2. Il Registro delle attività di trattamento è tenuto in forma scritta, anche in formato elettronico o su piattaforma informatica, ed è reso accessibile in modalità visione al Responsabile della Protezione dei Dati (RPD).

3. L'AC, quale Titolare, effettua la valutazione di impatto (DPIA) dei trattamenti previsti sulla protezione dei dati nei casi in cui, ai sensi dell'art. 35 del GDPR, un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

4. In tutti i casi in cui si renda necessario e, comunque, ogni qualvolta si verifichino variazioni del rischio rappresentato dalle attività relative al trattamento, il Titolare procede ad un riesame per verificare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati.

5. Ai sensi dell'art. 36 del GDPR, l'AC consulta il Garante per la protezione dei dati personali (Garante) prima di procedere al trattamento, qualora la valutazione di impatto sulla protezione dei dati indichi che il trattamento può presentare un rischio elevato nonostante le misure adottate dal Titolare per attenuare il rischio. In tale evenienza, è facoltà dell'AC chiedere supporto al Responsabile della Protezione dei Dati che impartisce, ove necessario, indicazioni operative utili per assicurare omogeneità procedurale nella valutazione di impatto dei trattamenti di cui l'Ente è Titolare.

Art. 17
Procedura di notifica e comunicazione in caso di violazione dei dati personali (Procedura *data breach*)

1. Ai sensi dell'art. 33 del GDPR, l'AC, quale Titolare, in caso di violazione dei dati personali effettua la notifica al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento della conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e libertà delle persone fisiche cui i dati violati si riferiscono. Qualora il Titolare

non riesca a notificare la violazione entro le 72 ore dalla conoscenza, la comunicazione tardiva al Garante deve esplicitare i motivi del ritardo.

2. Ai sensi dell'art. 34 del GDPR, l'AC è tenuto a comunicare la violazione dei dati personali anche all'Interessato quando la stessa è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche. La comunicazione non è richiesta se sussistono le condizioni indicate al par. 3 dell'art. 34 del GDPR.

3. L'AC, quale Responsabile, dopo essere venuto a conoscenza della violazione, informa il Titolare senza ingiustificato ritardo ovvero secondo le tempistiche indicate dal Titolare.
4. L'AC, in qualità di Titolare, al fine di assicurare tempestività ed efficacia nella gestione delle violazioni di dati nell'ambito dell'AC, adotta una "Procedura per la gestione dei casi di violazione dei dati personali" (Procedura data breach)" (All. 2), che individui i ruoli e le responsabilità dei soggetti coinvolti, i canali di contatto dedicati, le modalità operative di gestione delle segnalazioni, le azioni da intraprendere ivi comprese le forme di comunicazione al Garante Privacy e agli Interessati.

5. L'AC predispone e mantiene costantemente aggiornato un registro per documentare gli incidenti di sicurezza che comportino violazione dei dati personali (Registro incidenti data breach).

All.1

PROCEDURA PER LA GESTIONE DELLE RICHIESTE DEGLI INTERESSATI

(***Art. 15 Regolamento in materia di protezione dei dati personali dell'Automobile Club Brescia***)

TIPOLOGIE DI ISTANZE

Gli Interessati, presentando una istanza scritta tramite il modulo messo a disposizione sul sito *web* dell'Automobile Club Brescia ovvero con altre modalità (es. posta ordinaria, PEC), hanno il diritto di ottenere dal Titolare del trattamento:

1) la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano (art. 15 GDPR);

2) l'accesso ai propri dati personali oggetto di trattamento (art. 15 GDPR);

3) informazioni sul trattamento in corso, relative ai seguenti ambiti (art. 15 GDPR):

- finalità del trattamento;
- categorie di dati personali trattate dal Titolare;
- destinatari cui i dati personali sono stati o saranno comunicati, precisando se trattasi di destinatari di Paesi terzi o organizzazioni internazionali. In caso di comunicazione dei dati a Paesi esteri od organizzazioni internazionali, dare evidenza all'Interessato circa l'esistenza di adeguate garanzie per il trasferimento dei suoi dati personali (cfr. art. 46 GDPR);
- periodo di conservazione dei dati, se possibile, o i criteri per determinarlo;
- diritto dell'Interessato di chiedere al Titolare del trattamento la rettifica o la cancellazione dei dati personali che lo riguardano ovvero la limitazione del trattamento degli stessi o di opporsi a tale trattamento;
- diritto dell'Interessato di proporre reclamo a un'autorità di controllo;
- diritto dell'Interessato di avere tutte le informazioni disponibili sull'origine/fonte dei dati nei casi in cui i dati non siano raccolti presso lo stesso;
- sull'esistenza di un processo decisionale automatizzato, compresa la profilazione (cfr. art. 22, parag. 1 e 4 GDPR), nonché diritto di ricevere indicazioni sulla logica impiegata nella profilazione, sull'importanza e sulle conseguenze per l'Interessato derivanti dalla profilazione stessa;

4) la rettifica dei dati personali inesatti che lo riguardano nonché l'integrazione di quelli incompleti (art. 16 GDPR);

5) la cancellazione dei dati personali che lo riguardano, qualora sussista una delle condizioni previste dall'art. 17 del GDPR;

6) la limitazione del trattamento, nei casi previsti dall'art. 18 del GDPR;

7) la portabilità dei dati personali che lo riguardano, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, nonché richiedere la loro trasmissione ad un altro Titolare, se tecnicamente fattibile;

8) che il Titolare si astenga dal trattare ulteriormente i dati personali a fronte di un'istanza di opposizione presentata dall'Interessato ai sensi dell'art. 21 del GDPR;

9) la revoca, in qualsiasi momento, del consenso prestato.

PROCEDURA INTERNA DI ACQUISIZIONE E TRATTAZIONE DELLE ISTANZE

I. Tutte le richieste degli Interessati devono essere acquisite al protocollo, al fine di garantire la certezza della data di ricezione/acquisizione.

II. Il Titolare valuta l'accettabilità della richiesta avuto riguardo alle limitazioni all'esercizio dei diritti stabilite dal Codice Privacy (artt. 2 *undecies* - 2 *terdecies*).

III. Una volta ritenuta l'istanza procedibile, occorre identificare l'Interessato richiedente acquisendo copia di un valido documento di identità.

IV. Il Titolare assicura sempre un riscontro scritto all'Interessato, anche nei casi in cui l'istanza non può essere accolta.

V. La comunicazione all'Interessato di non accoglimento dell'istanza deve essere adeguatamente motivata con l'indicazione dei presupposti di fatto e di diritto che giustificano il rigetto.

VI. Il Titolare è tenuto a rispondere alle istanze dell'Interessato senza ingiustificato ritardo e comunque entro un mese dal ricevimento della richiesta stessa ed anche se la richiesta sia pervenuta con un canale diverso da quello messo a disposizione sul sito istituzionale dell'AC.

VII. Il termine di risposta può essere prorogato nei casi di particolare complessità o a causa del numero di richieste pervenute per un termine massimo di due mesi. La comunicazione di proroga deve essere protocollata e inviata all'Interessato entro un mese dalla ricezione dell'istanza indicandone i motivi.

VIII. La risposta all'istanza viene data per iscritto, con le stesse modalità impiegate dall'Interessato, ovvero con altra modalità dallo stesso indicata, preferibilmente con strumenti elettronici.

IX. Al fine di comprovare l'avvenuta evasione delle istanze, le risposte alle richieste degli Interessati devono essere protocollate prima dell'invio.

Via Enzo Ferrari, 4/6
25134 Brescia
Tel. 030 23971
C.F. e P.IVA 00299060178
www.brescia.aci.it

All.2

AUTOMOBILE CLUB BRESCIA

PROCEDURA

PER LA GESTIONE DEI CASI DI VIOLAZIONE DEI DATI PERSONALI

(*PROCEDURA DATA BREACH* - *A*rt. 17 Regolamento in materia di protezione dei dati personali dell'Automobile Club Brescia)

AMBITO DI APPLICAZIONE

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

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'Automobile Club Brescia**.**

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'Automobile Club**, 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'Automobile Club Brescia** 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'Automobile Club Brescia** 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 segreteria@aci.brescia.it per conoscenza, al *Data protection Officer* contattabile all'indirizzo *e-mail* m.annibalidpo@aci.it, al contempo avvisando telefonicamente il Titolare al n. 030.2397327.

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 - *N*e 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).

Via Enzo Ferrari, 4/6
25134 Brescia
Tel. 030 23971
C.F. e P.IVA 00299060178
www.brescia.aci.it

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) **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 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.

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.

Via Enzo Ferrari, 4/6
25134 Brescia
Tel. 030 23971
C.F. e P.IVA 00299060178
www.brescia.aci.it

b) In **caso negativo** (rischio non elevato), **il Titolare** non deve notificare l'evento al Garante Privacy né agli Interessati ma deve adottare le misure più idonee per documentare e conservare gli atti relativi all'evento di *data breach.*

IV - *Obbligo d****i 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. 883 del GGDPR e/o di misure correttive ai sensi dell'art. 5858, par.2,2, dello stesso Regolamento.

Via Enzo Ferrari, 4/6
25134 Brescia
Tel. 030 23971
C.F. e P.IVA 00299060178
www.brescia.aci.it