AUTOMOBILE CLUB MATERA

“Regolamento di organizzazione dell’Automobile Club Matera per l’attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali”

Regolamento adottato con Delibera Presidenziale n° 1 del 08-04-2025

1. Introduzione

Il 24.05.2016 è entrato in vigore il Regolamento UE n. 2016/679 (in seguito, “Regolamento”; “GDPR”) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

L’impronta del Regolamento impone un maggior rigore nella gestione dei trattamenti e degli adempimenti più articolati e incisivi a fronte di una necessaria maggiore cautela nel trattamento dei dati.

In particolare, il nuovo Regolamento europeo ha come oggetto la tutela delle persone, con riguardo al trattamento e alla circolazione dei dati; il principio cardine è infatti la tutela del diritto e della libertà fondamentale alla protezione dei dati nonché il principio generale alla portabilità e circolazione dei dati personali nell’UE (artt. 1, 2, 3 GDPR).

In questo contesto il regolamento in materia di *privacy* rappresenta uno strumento utile per ottenere un maggiore equilibrio tra i contrapposti interessi dei soggetti coinvolti come, ad esempio, il rapporto tra l’Ente, i cittadini, le imprese e tutte le organizzazioni del territorio.

L’Automobile Club Matera è da tempo impegnato nel perseguire politiche di rispetto della tutela dei dati personali, avendo già fatto propri i principi cardine in tema di *privacy*, quale elemento di protezione e valorizzazione della propria attività pubblicistica.

Al fine di garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell’interessato, con particolare riferimento alla riservatezza, all’identità personale e al diritto alla protezione dei dati personali, L’Ente, con la supervisione dell’Automobile Club d’Italia in qualità di Ente federante, ha avviato dal 2021, un

processo di aggiornamento e revisione delle attività connesse alla protezione dei dati personali, al fine di consentire un innalzamento dell'attuale livello di protezione di questi ultimi.
A tal fine, l'Ente si è dotato di un sistema di regole e procedure al fine di poter essere costantemente aggiornato in materia, in linea con l'esperienza maturata dall'Ente e con le evoluzioni normative. L'Automobile Club Matera ha adottato il presente regolamento, al fine di dotarsi di un modello di "*governance*" e di presidi organizzativi in linea con le nuove previsioni del Regolamento europeo.

1.1 Premessa

Il presente documento è redatto seguendo quanto previsto dal GDPR e dalla normativa italiana, oltreché dai Provvedimenti dell'Autorità Garante per la protezione dei dati personali (di seguito Autorità Garante o Autorità di controllo) che risultino essere applicabili alle attività esplicate dall'Automobile Club Matera ("Normativa *Privacy*").
Il presente documento verrà aggiornato ed approvato in caso di modificazioni della normativa che implichino una modifica degli assetti e delle procedure adottate dall'ACI e dall'Automobile Club Matera.

1.2 Termini e definizioni

Si riportano alcune definizione chiave in ambito privacy:
Amministratore di sistema: Il soggetto preposto alla gestione di sistemi informatici con i quali vengono effettuati Trattamenti di Dati Personali.
Autenticazione informatica: L'insieme degli strumenti elettronici e delle procedure attraverso il quale viene verificata la corretta Identità di un utente.
Autorità di controllo: Si intende l'Autorità di cui all'articolo 51 del Regolamento Europeo in Materia di Protezione dei Dati Personali – *General Data Protection Regulation* [GDPR, Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016], ovvero una o più Autorità pubbliche indipendenti incaricate da uno Stato Membro di vigilare l'applicazione del Regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali.
Banca dati: Una banca dati è una raccolta di informazioni/dati, in forma cartacea o informatica, organizzati in modo strutturato e omogeneo, in modo da poter essere facilmente reperite, aggiornate e modificate attraverso l'utilizzo di apposite chiavi di ricerca.
Cancellazione sicura: Eliminazione di dati presenti sul supporto elettronico con modalità che li rendano inintelligibili e non recuperabili.
Credenziali di autenticazione: I dati e i dispositivi, assegnati a un soggetto e a esso univocamente correlati, utilizzati per l'autenticazione informatica.
Danno: Conseguenza pregiudizievole derivante dal concretizzarsi di una minaccia.

***Data Breach*:** Violazione della sicurezza che comporta, accidentalmente o volontariamente, la distruzione, perdita, alterazione, pubblicazione o accesso non autorizzato di dati personali trasmessi, conservati o in altro modo trattati.

***Data Protection Officer* o DPO:** Soggetto designato dal Titolare del trattamento in funzione delle sue qualità professionali al fine di informare e fornire consulenza al Titolare stesso nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dalla Normativa *Privacy*.

Dato anonimo: Il dato che in origine, o a seguito di trattamento, non si riferisce a una persona fisica identificata o identificabile.

Dati appartenenti a particolari categorie: I dati personali idonei a rivelare l'origine razziale o etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i 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.

Dati giudiziari: I dati personali relativi a condanne penali e reati ai sensi dell'art. 10 del GDPR, nonché i dati idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da *a)* a *o)* e da *r)* a *u)*, del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Dato personale: Qualsiasi informazione riguardante una persona fisica identificata o identificabile. 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.

Diffusione: La trasmissione di dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Informazione: Trasmissione dei dati e l'insieme delle strutture che la consentono.

Interessato: La persona fisica identificata o identificabile mediante i dati personali trattati.

Minaccia: evento il cui concretizzarsi potrebbe arrecare un danno ai beni dell'Ente.

Misure adeguate: L'insieme delle misure tecniche e organizzative volte a garantire la liceità del trattamento effettuato, anche con riferimento alla disponibilità, autenticità, integrità e la riservatezza dei dati personali conservati o trasmessi, individuate sulla base e in relazione ai rischi individuati rispetto ad una determinata attività di trattamento.

Normativa Privacy: Complessivamente, il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, la normativa italiana di riferimento (in particolare, il D.Lgs. 196/2003, come modificato e integrato dal D.Lgs. 101/2018 di adeguamento, nonché le regole di condotta/regole tecniche ad esso allegate e i Provvedimenti dell'Autorità Garante per la protezione dei dati personali applicabili al contesto).

Persone Autorizzate al trattamento: Le persone fisiche autorizzate dall'Automobile Club Matera a compiere operazioni di trattamento dei dati personali, nell'ambito e sotto l'autorità dell'Ente stesso, in ottemperanza alle istruzioni ricevute mediante apposita nomina.

Responsabile esterno del trattamento: La persona giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento, appositamente designata ai sensi e in conformità all'art. 28 del GDPR.

Rischio: Possibilità che un evento non voluto e potenzialmente dannoso si verifichi, facendo venir meno la riservatezza e/o integrità e/o disponibilità dei dati personali e, quindi, mettendo a repentaglio la tutela dei diritti e le libertà delle persone fisiche.

Sistema di autorizzazione: L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

Titolare del trattamento o Titolare: La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

Trattamento: 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.

1.3 Obiettivi del documento

Il presente Regolamento definisce la portata e l' attuazione della Normativa *Privacy* all'interno dell'Automobile Club Matera: esso, in particolare, delinea un sistema organico e strutturato di gestione di tutti gli aspetti concernenti i profili "*privacy*" attraverso un modello di gestione uniforme, fornendo ai soggetti che di tale sistema fanno parte indicazioni chiare, sia sul piano tecnico/operativo che sul piano organizzativo, sulle modalità di applicazione della Normativa *Privacy*.

Il presente documento, pertanto:

- Definisce i requisiti per il trattamento dei dati personali, affinché esso avvenga, all'interno del quadro delineato dalla Normativa *Privacy*, nel rispetto delle prescrizioni

previste dalla normativa stessa e individua – disciplinandone le modalità – gli adempimenti da porre in essere per garantire la conformità alla normativa in parola;

- Fornisce indicazioni sulle modalità di trattamento dei dati personali;
- Individua le misure tecniche ed organizzative che l'Ente adotta per garantire – ed essere in grado di dimostrare – la conformità alla Normativa Privacy delle attività di trattamento dei dati delle persone fisiche che l'Automobile Club Matera effettua direttamente, oppure avvalendosi di soggetti terzi;
- Disciplina i ruoli e le responsabilità in modo da evitare la possibile irrogazione delle sanzioni amministrative pecuniarie;

Le presenti Linee Guida sono rivolte a tutto il personale dell'Automobile Club Matera.

Il presente documento è da considerarsi ad uso interno e sarà data massima pubblicità in modo tale da risultare accessibile esclusivamente al personale dell'Ente.

Obiettivo ulteriore del presente documento è quello, di concerto con le attività formative che verranno poste in essere, di innalzare la cultura di una corretta e sicura gestione dei dati personali e consentire il rispetto e l'effettiva operatività del Sistema di gestione *privacy* qui delineato.

Viene dunque proposto un regolamento che descrive i ruoli e le responsabilità dei soggetti coinvolti nel trattamento dei Dati Personali nella propria titolarità.

2. Modello Organizzativo: Ruoli e Responsabilità

Di seguito vengono presentati i ruoli chiave identificati del regolamento:

- Interessato;
- Titolare del Trattamento;
- DPO;
- Responsabile del Trattamento;
- Persona Autorizzata al Trattamento;
- Persona Autorizzata al trattamento di Videosorveglianza;
- Amministratore di Sistema;
- Data manager;

Per ciascuna delle seguenti figure, di seguito sono descritti elementi tipici ed eventuali responsabilità e ruoli definiti nell'ambito del Regolamento.

2.1 Interessato

Con il termine "Interessato" si fa riferimento alla persona fisica resa identificata o identificabile dai Dati Personali trattati (a titolo esemplificativo e non esaustivo: dipendenti, candidati all'assunzione, visitatori, committenti, richiedenti servizi ecc.).

2.2 Titolare del trattamento

Il "Titolare" è la persona fisica/giuridica che determina le finalità e i mezzi del trattamento dei Dati Personali, oppure che viene individuato come tale dalla legge stessa che prevede e disciplina le attività che comportano il trattamento di dati personali.

Il Titolare ha la facoltà di nominare "Persone Autorizzate al Trattamento", impartendo a queste ultime specifiche istruzioni riguardo allo svolgimento di operazioni di Trattamento su una o più delle categorie di Dati Personali. Analogamente, i soggetti esterni all'organizzazione del Titolare che trattano dati per suo conto devono essere da questi nominati Responsabili del trattamento e devono ricevere specifiche istruzioni circa le modalità di trattamento e di protezione dei dati personali.

2.3 Responsabile del Trattamento

Ai sensi dell'art. 28 del GDPR, il "Responsabile del Trattamento" è la persona fisica/giuridica che tratta Dati Personali per conto del Titolare. Quest'ultimo ricorre unicamente a Responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato. Il trattamento dei dati da parte di un Responsabile è disciplinato da un contratto che vincoli il Responsabile stesso alle indicazioni fornite dal Titolare del trattamento e che definisce:

- L'oggetto e la durata del trattamento dei dati;
- La natura e le finalità del trattamento;
- Il tipo di dati personali e le categorie di soggetti interessati;
- Le istruzioni/restrizioni per qualsiasi trasferimento di dati personali sia all'interno che all'esterno dell'Ente;
- L'applicazione di misure di sicurezza adeguate;
- I diritti del Titolare del trattamento;
- Gli obblighi del Responsabile del trattamento.

Si indicano, qui di seguito, i principali obblighi del Responsabile:

- Assicurarsi che il trattamento dei Dati Personali avvenga secondo le istruzioni impartite dal Titolare;
- Assicurarsi che sia garantito l'esercizio dei diritti da parte degli interessati;
- Procedere all'identificazione delle Persone Autorizzate al trattamento, fornendo alle stesse adeguate istruzioni in relazione al Trattamento effettuato/da effettuare;
- Garantire che le Persone Autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

- Adottare tutte le misure richieste ai sensi dell'articolo 32 del GDPR;
- Assistere il Titolare del trattamento nel garantire il rispetto degli obblighi del GDPR;
- Garantire l'applicazione di misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- Mettere a disposizione del Titolare tutte le informazioni necessarie a dimostrare il rispetto degli obblighi normativi applicabili e a consentire/contribuire alle attività di revisione, comprese le verifiche;
- Garantire l'adozione di adeguate misure tecniche e organizzative che garantiscano un adeguato livello di protezione dei Dati Personali trattati, nel rispetto delle leggi applicabili;
- Garantire che l'eventuale dismissione di strumenti elettronici contenenti Dati Personali avvenga nel rispetto delle leggi applicabili;
- Cooperare con il Titolare del trattamento nella rilevazione e gestione di potenziali violazioni dei Dati Personali (*Data Breach*), garantendo la necessaria collaborazione nelle attività di *recovery* che dovessero rendersi necessarie;
- Non ricorrere a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare del trattamento;
- Su scelta del Titolare del trattamento, cancellare o restituire tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che legge preveda la conservazione dei dati.

L'Ente utilizza appositi modelli *standard* di nomina a responsabile forniti dal DPO dell'Automobile Club d'Italia.

2.4 Persone Autorizzate al Trattamento

Le "Persone Autorizzate al trattamento" sono soggetti all'uopo autorizzati dal Titolare o dal Responsabile del trattamento, nell'ambito dei rispettivi ruoli. Ciascuna Persona Autorizzata al trattamento opera sulla base di istruzioni fornitegli. Le suddette istruzioni possono essere differenziate e sono aggiornate nel corso della durata del rapporto in ragione di specifiche necessità (cambio mansione/responsabilità/attività).

Si indicano qui di seguito i principali obblighi in capo alla Persona Autorizzata al Trattamento:

- Eseguire le proprie attività lavorative nel rispetto delle normative applicabili e delle istruzioni ricevute dal Titolare del Trattamento in merito alle corrette modalità di gestione dei dati personali;
- Trattare e custodire i dati personali, in particolare quelli sensibili, a cui si ha accesso nell'espletamento delle mansioni lavorative, garantendo l'adozione/applicazione delle misure di sicurezza disposte dal Titolare/Responsabile del Trattamento di riferimento, al fine di evitarne la distruzione, la perdita o l'accesso da parte di persone non autorizzate;

- Trattare i dati esclusivamente al fine di adempiere alle obbligazioni conferite e, in ogni caso, per scopi determinati, espliciti e, comunque, in termini compatibili con gli scopi di riservatezza per i quali i dati sono stati raccolti;
- Verificare costantemente la correttezza dei dati trattati e, ove necessario, provvedere al loro aggiornamento;
- Garantire, in ogni operazione di trattamento, la massima riservatezza, astenendosi dal trasferire, comunicare e/o diffondere i dati a terzi, salvo preventiva autorizzazione del Titolare o del Responsabile del Trattamento di riferimento;
- Partecipare alle iniziative formative su tematiche *Privacy*;
- Segnalare al Titolare/Responsabile del Trattamento di riferimento eventuali criticità o punti di attenzione inerenti alla gestione della *Privacy* (per esempio: possibile *Data Breach*, nuovi progetti o servizi con impatti Privacy, problematiche nella gestione dei diritti degli interessati, nuove terze parti cui vengono trasferiti dati personali);
- Adottare le misure per evitare l'accesso dei dati a terze parti durante l'allontanamento, anche temporaneo, dalla postazione di lavoro.

L'Ente utilizza appositi modelli *standard* di nomina a soggetto autorizzato forniti dal DPO dell'Automobile Club d'Italia.

2.5 Amministratore di Sistema

L' "Amministratore di Sistema" è il soggetto preposto alla gestione di sistemi informatici con i quali vengono effettuati Trattamenti di Dati Personali.

Di seguito elencati i principali obblighi:

- Monitorare lo stato dei sistemi di elaborazione e delle banche dati dell'Ente e dell'ACI, con particolare e costante attenzione al profilo della sicurezza;
- Verificare che l'accesso ai sistemi e ai dati personali ivi contenuti sia debitamente protetto, nonché consentito solo quando strettamente necessario, nel pieno rispetto della legge e delle *policy* aziendali;
- Supportare la struttura di ICT nella definizione ed implementazione di misure tecniche ed organizzative tali da garantire un livello di sicurezza adeguato al rischio, tra cui, a titolo esemplificativo e non esaustivo: i) la pseudonimizzazione e la cifratura dei dati personali; ii) la capacità dell'Ente di assicurare, su base permanente, riservatezza, integrità, disponibilità e resilienza dei sistemi, oltre a quella di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico (*Data Breach*);) l'esecuzione di controlli ed *audit* per testare, verificare e valutare regolarmente l'efficacia delle misure adottate per garantire la sicurezza dei trattamenti;
- Adempiere a tutti gli obblighi stabiliti dalla normativa vigente e dalle specifiche *policy* adottate dall'ACI e dall'Automobile Club Matera;

- Effettuare gli interventi di manutenzione necessari;
- Verificare, con continuità, il corretto funzionamento dei sistemi di *backup*/*recovery*;
- Sovrintendere all'operato di eventuali tecnici esterni che, a qualunque titolo, si trovino ad operare su sistemi o archivi di dati rientranti nel proprio perimetro di competenza;
- Gestire i sistemi di autenticazione e autorizzazione, nonché l'assegnazione delle relative credenziali a tutti i dipendenti dell'ACI e dell'Automobile Club Matera;
- Avvisare senza ingiustificato ritardo l'Ente riguardo a qualsiasi violazione della sicurezza da cui possa derivare, in maniera accidentale o illecita, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trattati o conservati nei sistemi dell'Ente e dell'ACI;
- Prestare la massima collaborazione nei confronti di ogni Responsabile del Trattamento eventualmente nominato dall'Ente.

2.6 Organizzazione interna dell'Automobile Club Matera in materia di privacy

Titolare del trattamento dei dati: Titolare del trattamento ai sensi dell'art 4 del Regolamento (UE) n. 679/2016 è l'Automobile Club Matera con sede in viale delle Nazioni Unite n°47 – 75100 – Matera, rappresentato da Cosmo Damiano Pompeo quale Presidente / legale rappresentante pro tempore.

Responsabili del trattamento: i soggetti che trattano dati dei quali l'Ente è Titolare;

Incaricati/Autorizzati: soggetti opportunamente nominati.

L'Automobile Club Matera in persona del legale rappresentante è responsabile, in ultima istanza, di:

- assicurare che l'organizzazione, le misure di sicurezza e procedurali adottate e le modalità operativo/gestionali dell'Ente siano conformi ai requisiti definiti dalla Normativa *Privacy*, anche attraverso l'effettiva ed efficace attuazione delle presenti Linee Guida;
- assicurare costantemente che i compiti e le responsabilità in materia di protezione dei dati personali siano allocati in modo chiaro e appropriato, in modo coerente con le mansioni lavorative e le funzioni assegnate;
- in generale, assicurare che l'Ente adempia agli obblighi che la normativa pone in capo al Titolare e al Responsabile del trattamento, assumendo le iniziative necessarie e curando l'adozione degli atti formali (incluse la predisposizione e l'approvazione, la modifica e la conservazione della documentazione prevista dalla normativa in parola e dalle presenti Linee Guida, nonché delle Linee Guida stesse).

Le funzioni di cui sopra possono essere delegate, così da consentire una maggiore tempestività di intervento e celerità decisionale, nell'ambito dell'ordinaria gestione dell'Ente.

È compito del responsabile sovraintendere alla gestione dei processi e curare gli adempimenti previsti dalla normativa. Pertanto, gli sono affidati i seguenti compiti:

- organizzare, gestire e supervisionare tutte le operazioni di trattamento di dati personali effettuate anche di concerto con il DPO in modo che il trattamento dei dati personali sia sempre ispirato al e avvenga nel rispetto dei principi previsti dall'art. 5 del Regolamento europeo (vale a dire: liceità, correttezza e trasparenza, esattezza, integrità e riservatezza dei dati trattati, limitazione delle finalità e della conservazione, minimizzazione dei dati trattati in relazione alle attività svolte);
- valutare, di concerto con il DPO, i rischi correlati alle attività di trattamento dei dati personali, tenuto conto delle modalità operative dell'Ente, dell'organizzazione e delle misure di sicurezza implementate e, al ricorrere dei relativi presupposti, effettuare la valutazione di impatto (DPIA);
- assicurare la presenza delle misure tecniche e organizzative individuate ai sensi dell'art. 32 del Regolamento europeo, monitorandone costantemente l'adeguatezza e la corretta applicazione e di concerto con il deputato reparto tecnico/informatico e il DPO;
- gestire le attività necessarie per consentire l'esercizio dei diritti da parte degli interessati, al fine di fornire riscontro alle loro istanze, provvedendo anche all'alimentazione e conservazione dell'apposito Registro di con concerto con le posizioni operative ed il DPO;
- gestire il processo di *data breach*, provvedendo anche all'alimentazione e conservazione dell'apposito Registro e all'eventuale notifica della violazione al Garante per la protezione dei dati personali, di concerto con i dirigenti, le posizioni operative ed il DPO;

Con riferimento ai trattamenti evidenziati nell'ambito dell'Ente, censiti e rappresentati nel Registro dei Trattamenti, l'Automobile Club Matera ha individuato i seguenti Referenti in materia di Privacy, autorizzandoli al trattamento dei dati personali negli ambiti di rispettiva competenza, sulla base dei ruoli e responsabilità assegnati e in funzione delle mansioni svolte, nel rispetto dell'Organigramma a cui sono attribuiti compiti di coordinamento e supervisione.

I referenti nominati ricoprono ruoli di responsabilità per le quali è stata predisposta una apposita lettera/nomina di incarico ed autorizzazione al trattamento.

I Referenti sono tenuti ad avere una particolare attenzione in merito all'applicazione delle norme in materia di *privacy* e del presente Regolamento ed sorvegliarne l'applicazione da parte del personale che ad essi fa capo.

Persone Autorizzate al Trattamento: l'Automobile Club Matera ha provveduto ad autorizzare al trattamento dei dati personali, di cui è Titolare o che tratta in qualità di Responsabile, ciascun collaboratore al fine di garantire che, nell'ambito delle mansioni attribuite, siano adottate le misure di sicurezza a protezione dei dati personali nei termini riportati nel presente Regolamento. I soggetti in parola sono autorizzati al trattamento dei dati

per le sole finalità indicate dall'Automobile Club Matera ed è vietato qualsiasi altro uso dei dati personali trattati che non sia in linea con l'incarico ricevuto.

Le Persone Autorizzate al Trattamento sono state formalmente edotte in merito alla circostanza che:

a) il trattamento e la conservazione dei dati deve avvenire in modo lecito e proporzionato alle funzioni comunali, nel rispetto della riservatezza;

b) la raccolta, registrazione ed elaborazione dei dati, mediante strumento elettronico o cartaceo, deve essere limitata alle necessità comunali;

c) è onere dei soggetti autorizzati correggere o aggiornare i dati posseduti.

Al momento della formalizzazione della nomina, l'autorizzato ha ricevuto le idonee informazioni e istruzioni.

DPO: L'Automobile Club, ai sensi dell'art. 37 del regolamento UE n. 679/2016, ha nominato quale Responsabile della protezione dei dati (DPO - Data Protection Officer), il Dott. Mauro Annibali dirigente Generale dell'Automobile Club d'Italia che ha la funzione di affiancare il Titolare, gli Addetti e i Responsabili del Trattamento affinché assicuri una corretta gestione dei dati seguendo i principi e le indicazioni inserite nella normativa vigente, nel Regolamento UE 2016/679 e nelle presenti Linee Guida.

Il DPO è raggiungibile ai seguenti indirizzi:

Posta elettronica: **m.annibalidpo@aci.it**

Posta elettronica certificata: **DPO.AutomobileClubItalia@pec.aci.it**

3. Gestione dei dati personali

L'Automobile Club Matera garantisce che i dati raccolti sono completi, accurati e mantenuti aggiornati rispetto al proposito per cui vengono raccolti, compatibilmente con le tempistiche necessarie per gli eventuali aggiornamenti e tenuto conto del numero di dati oggetto di trattamento.

I dati personali sono raccolti solo per finalità specifiche, esplicite e legittime, mai in eccesso e comunque in coerenza con le finalità previste.

Come previsto dal Regolamento GDPR, gli interessati hanno la facoltà di esercitare i seguenti diritti in merito ai propri Dati Personali:

- **diritto di accesso** (art. 15): ovvero il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati che lo riguardano e, in tal caso, di ottenere l'accesso a tali dati personali, ottenendone copia, ed alle informazioni di cui all'art. 15 del Regolamento;
- **diritto di rettifica** (art. 16): ovvero il diritto di ottenere la rettifica dei dati inesatti che lo riguardano o l'integrazione dei dati incompleti;

- **diritto alla cancellazione** (art.17): ovvero il diritto di ottenere la cancellazione dei dati che lo riguardano, se sussiste uno dei motivi indicati dall'art. 17 del Regolamento;
- **diritto di limitazione di trattamento** (art. 18): ovvero il diritto di ottenere, nei casi indicati dall'art.18 del Regolamento, la cancellazione/ pseudonimizzazione/anonimizzazione dei dati personali che lo riguardano con l'obiettivo di limitarne il trattamento;
- **diritto alla portabilità dei dati** (art. 20): ovvero il diritto, nei casi indicati dall'art. 20 del Regolamento (vale a dire il trattamento effettuato con mezzi automatizzati, basato sul consensoo sull'esecuzione di un contratto), di ricevere, in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati che lo riguardano, nonché di trasmettere tali dati ad un altro titolare del trattamento senza impedimenti;
- **diritto di opposizione** (art. 21): ovvero il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento – fondato sul perseguimento di un legittimo interesse da parte del Titolare – dei dati personali che lo riguardano, compresa la profilazione sulla base di tali disposizioni;
- **diritto ad ottenere un processo decisionale non completamente automatizzato** (art. 22): ovvero il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona, salvo i casi previsti dall'art. 22 del Regolamento.

È previsto che, in caso di esercizio da parte di un interessato di uno dei diritti appena elencati, al ricorrere dei presupposti di legge il Titolare del trattamento provveda immediatamente a dare seguito alla richiesta.

Resta inteso che le richieste di esercizio dei diritti presentate dagli Interessati non potranno riguardare Dati Personali relativi a terzi, salvo casi particolari.

3.1 Fasi del ciclo di vita del dato personale

Le operazioni di Trattamento dei Dati Personali devono essere strettamente limitate a perseguire le finalità indicate nelle informative deputate, così come pubblicate sul sito istituzionale.

Di seguito sono riportate le fasi del "ciclo di vita" del Dato Personale, nonché il dettaglio delle modalità di gestione operativa.

3.1.1 Raccolta

Per quanto concerne la raccolta dei dati, l'acquisizione – direttamente presso gli interessati, oppure mediante trasmissione/comunicazione da soggetti terzi Titolari o Responsabili del trattamento – può avvenire mediante differenti canali, digitali (siti *web*, posta elettronica) e non

digitali (Posta ordinaria, portineria, uffici, fax). L'Ente effettua operazioni di trattamento sulle categorie di Dati Personali indicate nel Registro delle Attività di trattamento predisposto ai sensi dell'art. 30, commi 1 e 2, del GDPR. Il Trattamento dei Dati Personali da parte dell'Automobile Club Matera deve avvenire per il perseguimento di finalità legittime individuate anticipatamente e comunicate agli interessati con le modalità e le tempistiche individuate dagli artt. 13 e 14 del GDPR. I principi di trattamento corretto e trasparente implicano che l'interessato sia debitamente informato, per iscritto oppure oralmente, in maniera concisa e utilizzando un linguaggio semplice e chiaro, in merito al trattamento di dati personali che lo riguardano.

3.1.2 Cessazione del trattamento e Cancellazione

Nel caso in cui l'Ente intenda cessare lo svolgimento di una o più operazioni di Trattamento, i Dati Personali precedentemente utilizzati nel contesto di tali operazioni dovranno essere distrutti, fatti salvi gli adempimenti legati ad obblighi di legge o a finalità legali/difensive. L'Ente provvede alla distruzione dei documenti e alla cancellazione dai supporti informatici che, dopo essere stati utilizzati per il Trattamento, siano destinati ad altro scopo (ad esempio: assegnazione di pc ad un diverso dipendente), in accordo a quanto previsto dalla normativa. Tale cancellazione serve a prevenire la diffusione, anche accidentale, di Dati Personali con conseguente violazione (*Data Breach*) di cui agli articoli 33 e 34 del GDPR.

Nel caso in cui i Trattamenti cessati siano stati oggetto di precedente notifica all'Autorità Garante, l'Ente dovrà prontamente provvedere ad effettuare i necessari aggiornamenti.

3.1.3 Altre operazioni di Trattamento

Le operazioni di Trattamento effettuate dall'Ente devono attenersi ai principi generali riportati di seguito:

- **Liceità, correttezza e trasparenza:** i dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato;
- **Limitazione delle finalità:** i dati devono essere raccolti per finalità esclusivamente determinate, esplicite e legittime ed utilizzati in altre operazioni del trattamento in termini compatibili con tali finalità (le finalità devono essere rese note nell'informativa);
- **Minimizzazione dei dati**: i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- **Esattezza:** i dati devono essere esatti e, se necessario, aggiornati. Si rende necessaria l'adozione di tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

- **Limitazione della conservazione:** i dati devono essere conservati in una forma che consenta l'identificazione dell'Interessato per un periodo di tempo non superiore a quello necessario e alle finalità per le quali sono stati trattati;

- **Integrità e riservatezza**: i dati devono essere trattati in maniera da garantire un'adeguata sicurezza dei Dati Personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. Per Trattamento di Dati Personali effettuato da Terze Parti, si intendono tutte le casistiche in cui i Dati Personali di titolarità dell'Ente o che la stessa tratta in qualità di responsabile del trattamento, siano resi, in qualsiasi modo, accessibili, anche tramite connessione remota, a Terze Parti.

Nella suddetta ipotesi, le Terze Parti devono essere nominate Responsabili del trattamento. Nell'ambito delle operazioni di Trattamento svolte, l'Ente deve comunque porre in essere tutte le misure necessarie per tutelare i Dati Personali, dovendo garantire:

- Riservatezza, integrità e disponibilità dei Dati Personali trattati;
- L'implementazione di misure di protezione delle reti, dei sistemi e dei *software* con i quali vengono trattati i Dati Personali, quali ad esempio la pseudonimizzazione, l'offuscamento e la cifratura dei Dati Personali, ove compatibili con il trattamento;
- Soluzioni di continuità di servizio in grado di garantire la disponibilità e l'integrità dei dati (*backup*, *Disaster Recovery*, ecc.);
- L'applicazione del principio di *Data Protection by design* e *by default* nella progettazione dei sistemi e nel disegno dei processi e delle procedure;
- L'implementazione di soluzioni in grado di rilevare tentativi non leciti di accesso ai Dati Personali in grado di garantire il rispetto delle prescrizioni del GDPR in merito alle violazioni (*Data Breach*);

3.2 Registro delle Attività di Trattamento

L'Ente è dotata di un registro delle attività di trattamento svolte sotto la propria responsabilità, che costituisce parte integrante e sostanziale del Sistema di gestione *privacy* delineato dalle presenti Linee Guida.

Il registro delle attività di trattamento è uno strumento che raccoglie tutte le attività di trattamento dei dati personali svolte dall'Ente, tenuto dal Titolare e/o dal Responsabile del trattamento o da suo rappresentante come stabilito dall'art. 30 del GDPR. Il registro delle attività di trattamento è, quindi, fondamentale, non soltanto per disporre di un quadro aggiornato dei trattamenti in essere all'interno dell'Ente, ma è anche indispensabile per ogni valutazione e successiva analisi del rischio. È quindi dovere dell'Ente, di concerto con il DPO,

mantenere costantemente aggiornamento il Registro con i nuovi trattamenti, nuove banche dati e nuove responsabilità, così come procedere all'eliminazione di eventuali Trattamenti cessati.

In attuazione di quanto richiesto dalla nuova normativa in materia di privacy e al fine di elaborare il Registro delle attività di trattamento, si è proceduto a una preliminare valutazione delle attività svolte dall'Automobile Club Matera, delimitando il perimetro dell'analisi alle attività ove si concentrano e circolano i dati personali relativi a dipendenti, consulenti e fornitori e soggetti che intrattengono rapporti con l'Ente.

L'Ente mette il Registro a disposizione dell'Autorità di controllo, oppure del Titolare/Responsabile del trattamento.

4. Modello di classificazione delle informazioni e gestione dei rischi connessi alla Privacy

Lo scopo del presente paragrafo è quello di fornire gli strumenti per una corretta classificazione delle informazioni a disposizione dell'Automobile Club Matera così da ingenerare una conseguente gestione efficiente del patrimonio informativo. Per "patrimonio informativo" si intende l'insieme delle informazioni necessarie allo svolgimento delle attività.

4.1 Applicabilità

Per assicurare alti *standard* qualitativi e di sicurezza, è necessario che tutte le risorse dell'organizzazione rispettino e applichino le procedure indicate all'interno del presente paragrafo.

4.2 Livelli di classificazione

Le informazioni a disposizione sono caratterizzate da diversi livelli di criticità stabiliti in base all'impatto che hanno sulle operazioni ed al danno che potrebbe causare una perdita di informazioni. È necessario per questo motivo fissare dei criteri che ne consentano una prima classificazione, così da poter stabilire il livello di protezione da attivare.

All'aumentare del livello di criticità dell'informazione, si riduce il perimetro del bacino di utenti che possono accedervi, poiché proporzionalmente alla criticità cresce anche l'intensità del danno che comporterebbe un'erronea diffusione dell'informazione stessa.

Le informazioni si classificano in:

- **Pubbliche**: possono essere diffuse a chiunque. La loro divulgazione non comporta alcun rischio;
- **Uso Interno**: la diffusione deve rimanere circoscritta all'interno del perimetro di attività dell'Ente (dipendenti, collaboratori). Il danno derivante da una divulgazione incontrollata sarebbe trascurabile;

- **Confidenziali o riservate**: la diffusione deve essere limitata a specifiche aree e agli attori esterni che vi entrano in contatto. In questo caso il danno derivante sarebbe di medio-alta entità;

Inoltre, ai fini dell'analisi si considerano i seguenti parametri di classificazione delle informazioni:

- **Riservatezza** (R): un'informazione deve essere nota solo a quanti ne abbiano diritto e siano autorizzati ad accedervi;
- **Integrità** (I): un'informazione deve essere intatta e invariata, così come viene consolidata dal suo proprietario;
- **Disponibilità** (D): un'informazione deve essere sempre disponibile per quanti hanno diritto di accedervi e prenderne conoscenza.

Dopo aver definito i parametri di classificazione, si identificano tre tipologie di minacce che potrebbero arrecare un danno all'Ente:

- l'accesso non autorizzato e illecita divulgazione delle informazioni viola il parametro di riservatezza provocando il rischio di un utilizzo non autorizzato dell'informazione;
- la modifica/distruzione non controllata/autorizzata delle informazioni viola il parametro di integrità provocando il rischio di cancellazione o alterazione dell'informazione;
- l'impossibilità di accesso e utilizzo delle informazioni viola il parametro di disponibilità comportando l'impossibilità di utilizzare l'informazione.

4.3 Criteri e misure adottati per assicurare l'integrità e la protezione dei dati

In questa sezione sono riportati i criteri definiti e le misure adottate per contrastare i rischi individuati in relazione alle attività e modalità di trattamento dei dati personali.

Per "misura" si intende lo specifico intervento tecnico od organizzativo posto in essere (per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia), come pure quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia.

In relazione al trattamento dei dati personali è, quindi, costantemente in atto un procedimento di controllo e di verifica della sicurezza del sistema informatico attraverso l'utilizzo di appositi strumenti a livello di sistema, di gestione delle basi dati e di applicativo, effettuato anche mediante l'ausilio di soggetti terzi.

MISURE ORGANIZZATIVE

Misure valide per tutto il personale:

È necessario procedere all'identificazione del personale addetto a ciascun trattamento e limitare delle attività di trattamento al solo personale così identificato, e fornire istruzioni operative al personale, nel rispetto dei seguenti principi:

- Trattamento dei dati esclusivamente per le finalità e con le modalità individuate dall'Ente, riportate nel Registro delle attività di trattamento, nel rispetto delle disposizioni di legge vigenti;limitazione del trattamento dei dati alle seguenti attività: raccolta, registrazione, organizzazione, elaborazione, archiviazione, consultazione, estrazione, utilizzo, comunicazione / trasmissione nei limiti individuati, cancellazione;trattamento limitato ai dati strettamente necessari in relazione alle finalità individuate;
- rispetto delle misure di sicurezza per la conservazione / archiviazione della documentazione cartacea, in particolare l'obbligo di chiusura a chiave degli armadi e rimozione delle chiavi prima della chiusura quotidiana degli uffici;
- divieto di comunicazione a terzi di *password* e credenziali di accesso personali;
- divieto di comunicazione/trasmissione di dati a terzi in assenza di identificazione e di accertamento dell'esistenza di una causa giustificativa di detta comunicazione/trasmissione (destinatario pre-individuato, adempimento di un obbligo di legge, esecuzione di un rapporto contrattuale, delega dell'interessato);
- divieto di divulgazione di dati;
- divieto di installazione di applicazioni e/o *software* senza previa autorizzazione;
- divieto di utilizzo di dispositivi mobili personali per il trattamento dei dati.
- utilizzo dei dispositivi elettronici (anche mobili) assegnati dal'Ente esclusivamente per finalità lavorative, nel rispetto delle istruzioni ricevute.

Come descritto in precedenza, è necessario fornire agli interessati le dovute informazioni in merito al trattamento dei dati personali, mediante sottoposizione/consegna/invio della documentazione appositamente predisposta [Informative *ex* artt. 13 e 14 Reg. (UE) 2016/679].

MISURE TECNICHE

Misure dei sistemi:

L'accesso ai sistemi informatici è concesso solo agli amministratori di sistema ed ai dipendenti nominati. Il sistema prevede:

- abilitazione di accesso ai sistemi informatici tramite l'utilizzo di identificativi univoci per ciascun utente;
- adozione di *password* di complessità adeguata (lunghezza minima di 8 caratteri, contenenti lettere maiuscole e minuscole, numeri e caratteri speciali);
- Attribuzione a ciascun profilo di utenza dei soli permessi di accesso ai sistemi.

Misure di sicurezza dei *personal computer*

- Attivazione del blocco automatico dei PC dopo un determinato intervallo temporale di inutilizzo;

- Installazione, configurazione e aggiornamento dei *software firewall* e *antivirus* sui PC;
- Installazione periodica degli aggiornamenti di sicurezza del sistema operativo sui PC;
- Effettuazione periodica del *backup* per i dati eventualmente presenti sui PC;
- Disabilitazione della modifica delle impostazioni di sicurezza dei PC per gli utenti.

Sicurezza di smartphone e tablet(se presenti)

- Attivazione del blocco automatico dei dispositivi dopo un determinato intervallo temporale di inutilizzo;
- Accesso alle funzionalità e applicazioni tramite PIN o *password*;
- Selezione/impostazione di blocchi per l'accesso ai dati e/o la condivisione tramite applicazioni gestite da soggetti terzi, con riferimento alla rubrica e alle e-mail;
- Connessione mobile ad *internet* sicura (*sim card* dedicata o reti Wi-Fi private, protette da*password*);
- Impostazione per la connessione di IP statico.

Sicurezza della rete

- Adozione di impostazioni di sicurezza adeguate per la connessione tramite LAN e limitare la possibilità di installazione di *software* e di *download di* file da parte degli operatori;
- Adozione di impostazioni di sicurezza adeguate perle connessioni Wi-Fi, quali l'utilizzo di protocolli di criptazione aggiornati, l'utilizzo di IP statici e connessioni riservate agli ospiti isolate dal resto della rete locale;
    - Blocco del traffico in ingresso ed in uscita dalla rete locale per i servizi non necessari (es. *peer to peer*) tramite l'impiego di appositi dispositivi di sicurezza;
    - Accesso da remoto alla rete locale sicuro e profilato;
    - Installazione periodica degli aggiornamenti per la sicurezza dei sistemi.

Sicurezza dei dati

- Effettuazione periodica di copie di *backup* dei dati memorizzati sui sistemi informatici centralizzati (es. *server*) o sui singoli PC e verifica della loro integrità;
- Archiviazione di copie di *backup* dei dati presso un sito esterno, differente da quello nel quale risiedono i sistemi centralizzati;
- Adozione di adeguate misure di sicurezza fisica per il sito presso il quale sono custodite le copie di *backup* (es. controllo accessi fisici ai locali, misure antincendio);

- Cancellazione sicura o distruzione dei dati su supporto informatico o cartaceo quando il loro trattamento non è più necessario o in occasione della dismissione dei dispositivi informatici (es. PC, *smartphone*, *hard-disk*);
- Utilizzo di e-mail *provider* che garantisca adeguati livelli di sicurezza e adozione di*antivirus* e *antispam* per le caselle e-mail.

Sicurezza fisica

- Protezione degli uffici con sistemi di chiusura (porte) in grado di impedire o comunque rendere difficoltoso l'accesso, se non mediante forzatura, a soggetti estranei non muniti di chiave;
- Identificazione dei visitatori all'ingresso della struttura e separazione degli ambienti di lavoro da quelli destinati all'accesso al pubblico;
- Custodia dei documenti cartacei e dei dispositivi di memorizzazione contenenti dati personali in spazi chiusi (es. archivi, armadi), in locali con accesso consentito al solo personale precedentemente autorizzato;
- Corretta identificazione delle fonti di calore, controllo periodico e manutenzione all'occorrenza dei locali in cui si trovano documenti cartacei e/o dei relativi impianti (per tali intendendosi anche le sole tubature di passaggio) elettrico, idraulico e del gas.
- Accesso ai locali tecnici presso i quali sono ospitati i sistemi informatici centralizzati (es. *server*) al solo personale precedentemente autorizzato.

INDICAZIONI SUGLI STRUMENTI RISPETTO ALLA FORMA DEI DATI TRATTATI
Dati elettronici

I dati di tipo informatico vengono trattati attraverso PC protetti tramite l'utilizzo di *password*, gestite dagli amministratori di sistema: dette *password* sono costituite da almeno 8 caratteri alfanumerici e devono essere periodicamente cambiate, a cadenza prestabilita. Ogni dipendente ha unicamente la *password* del PC e/o dei sistemi gestionali e/o delle aree *intranet* che utilizza e/o al cui accesso è abilitato.

Le banche dati/accessi alle *directory* dei sistemi gestionali sono suddivisi in base ai ruoli e ai compiti affidati ad ogni dipendente/collaboratore, a seconda dell'area/ufficio di appartenenza. Chi ha accesso ad una banca dati/*directory* non ha accesso alle altre che non gli competono; in altri termini, ognuno, a seconda delle mansioni svolte, può accedere solo a determinate cartelle, create e conservate sui *computer* locali, contenenti alcune tipologie di documenti e dati personali.

La configurazione dei sistemi prevede l'utilizzo di cartelle installate su *server* interno oppure presenti su Piattaforme condivise con soggetti terzi (anche in *cloud*), con profilazione degli accessi da parte dei diversi operatori (*public folder* + cartella riservata alle singole aree); gli accessi

dall'esterno e verso l'esterno sono "ristretti", con possibilità di visualizzare soltanto i dati di interesse, e veicolati tramite VPN.

Tutte le credenziali di accesso sono custodite da ciascun affidatario con la massima attenzione e, in caso di loro furto o smarrimento, è previsto l'immediato intervento dell'Amministratore di sistema affinché blocchi le credenziali oggetto di furto e/o smarrimento, verificando l'assenza *medio tempore* di eventuali accessi non autorizzati e fornisca nuove credenziali di autenticazione che, al primo accesso da parte dell'incaricato, dovranno essere modificate a sua cura e sotto la sua esclusiva responsabilità.

Server

Vengono utilizzati *server* locali (*server* principale e *server* di *back-up*) e *server* virtuali in *cloud*, messi a disposizione e gestiti da società terze, i cui *Data Center* sono collocati all'interno dell'Unione Europea o che, comunque, offrono adeguate garanzie di sicurezza e conformità al Regolamento e alla normativa di riferimento.

I sistemi sono generalmente ospitati su *server* (sia locali che in *cloud*) ad alta disponibilità che offrono una buona resilienza a situazioni di normali guasti tecnici e con dischi ridondati che permettono di ripristinare la disponibilità dei dati in caso di guasto.

Back-up

Vengono effettuati *back-up* periodici su *server* dedicati (locale e in *cloud*) e su supporti magnetici removibili, custoditi in appositi locali. L'amministratore di sistema verifica che il *backup* sia andato a buon fine.

***Computer* e supporti informatici:**

1. L'introduzione di *password* all'accensione del *personal computer* determina un livello di sicurezza, circa i dati contenuti nei PC, ritenuto più che soddisfacente. L'introduzione di dette *password* inibisce ad estranei l'uso dei personal computer, attraverso i quali, si accede alla posta elettronica;
2. In merito a messaggi e-mail inviati a più destinatari, quale mittente dovrà essere indicato il l'Automobile Club Matera in persona del soggetto che invia la e-mail, ed in Ccn i destinatari (che in tal modo non possono individuare gli indirizzi e-mail degli altri destinatari, attraverso la funzione di proprietà) salvo richieste esplicite dei soggetti terzi.
3. Nei messaggi di posta inviati viene inserita di *default* la seguente dicitura: "*Avviso di riservatezza: Il presente messaggio, inclusi eventuali allegati, contiene informazioni riservate esclusivamente ai destinatari indicati nel messaggio ed è protetto dalla legge. La diffusione, distribuzione e/o copia del contenuto del presente messaggio da parte di qualsiasi soggetto*

diverso dal destinatario è proibita. Se non siete il destinatario del presente messaggio, vi preghiamo di distruggerlo e di darcene immediata comunicazione inviando un messaggio all'indirizzo e-mail del mittente. Confidentiality notice: This message, including any attachment, contains confidential information intended only for the recipients named above, and is protected by law. Any disclosure, distribution and/or copying of this message by any subject different from the named recipients is prohibited. If you are not the intended recipient, you are pleased to delete this message and inform us immediately by sending an e-mail to the address of the sender.". (Avviso di riservatezza: questo messaggio, compresi eventuali allegati, contiene informazioni riservate destinate esclusivamente ai destinatari sopra indicati ed è protetta dalla legge. È vietata qualsiasi divulgazione, distribuzione e/o copia del presente messaggio da parte di soggetti diversi dai destinatari indicati. Se non sei il destinatario previsto, ti preghiamo di cancellare questo messaggio e di informarci immediatamente inviando una e-mail all'indirizzo del mittente.)"

4. I supporti magnetici contenenti dati possono essere riutilizzati esclusivamente previa formattazione irreversibile, in modo da impedire la lettura dei dati precedenti;
5. Dopo 15 minuti di inattività i PC vanno in modalità *stand-by*: dunque per la riattivazione è necessaria la *password*.
6. I *Personal Computer* sono dotati di *antivirus*, che vengono aggiornati automaticamente. Anche il server di rete è dotato di un *antivirus*, questo per avere un doppio controllo e una maggiore sicurezza;

Dati cartacei

Le aree e gli ambienti dove si trovano documenti contenenti dati su supporto cartaceo sono strutturate in modo tale che ciascun addetto possa rilevare a vista il tentativo di accesso da parte di persone estranee e, di conseguenza, impedirne l'accesso stesso.

L'ubicazione di stampanti e scanner non consente ad estranei di leggere o asportare eventualmente documenti.

Vi sono diversi armadi per l'archiviazione di documenti contenenti dati personali.

Supporti cartacei

Relativamente ai supporti cartacei, i criteri di protezione dei dati debbono essere ricercati nelle seguenti indicazioni:

- Qualsiasi documento in entrata/uscita dell'Ente, appartenente a fornitori/consulenti/dipendenti/ecc., viene inserito in apposite cartelline, raccoglitori o buste;

- Le eventuali rubriche telefoniche in utilizzo su supporto cartaceo sono richiuse dopo la consultazione in armadi o cassettiere, che dopo l'orario di lavoro saranno chiuse a chiave;
- Le copie delle e-mail inviate e ricevute dovranno essere archiviate in appositi raccoglitori che successivamente verranno archiviati in armadi;
- Tutti gli archivi cartacei sono chiusi all'interno di raccoglitori inseriti in armadi chiusi.
- i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali e, nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento;
- i faldoni contenenti i dati sono archiviati in una forma che non consenta l'identificazione dell'interessato a chi non autorizzato e comunque per un periodo di tempo non superiore a quello necessario agli scopi per i quali i dati sono stati raccolti e successivamente trattati;
- per tutto il periodo in cui i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici sono al di fuori dei locali individuati per la loro conservazione, il Responsabile o l'Incaricato del trattamento non dovrà lasciarli mai incustoditi;
- il soggetto autorizzato al trattamento deve, inoltre, controllare che i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, composti da numerose pagine o più raccoglitori, siano sempre completi e integri;
- al termine dell'orario di lavoro tutti i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, devono essere riportati nei locali individuati per la loro conservazione;
- i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere mai lasciati incustoditi nelle postazioni di lavoro durante l'orario di lavoro;
- si deve adottare ogni cautela affinché ogni persona non autorizzata non venga a conoscenza del contenuto di documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici;
- per evitare il rischio di diffusione dei dati personali trattati senza l'ausilio di strumenti elettronici, si deve limitare l'utilizzo di copie fotostatiche;
- particolare cautela deve essere adottata quando i documenti sono consegnati in originale a un altro incaricato debitamente autorizzato;
- è tassativamente proibito utilizzare copie fotostatiche di documenti (anche se non perfettamente riuscite) all'esterno del luogo di lavoro.

AZIONI E MISURE DA IMPLEMENTARE SU BASE CONTINUATIVO - PERIODICA O ALL'OCCORRENZA

- Analisi e valutazione dell'effettività ed efficacia delle misure adottate, da effettuarsi su base continuativa (attraverso lo svolgimento di attività di *audit*);
- Responsabilizzazione massima di tutti gli operatori, tramite controlli e istruzioni per la gestione delle attività che comportano il trattamento dei dati personali, periodicamente e all'occorrenza;
- Formazione del personale: in seguito all'adozione del presente Regolamento e della connessa documentazione e, successivamente, con cadenza periodica (almeno biennale), in particolar modo in caso di modifiche normative, organizzative e tecniche; l'articolo 32 del GDPR insiste sull'importanza della formazione come misura tecnica e organizzativa atta a garantire un livello di sicurezza adeguato al rischio.

5. Politica per la gestione delle terze parti

L'obiettivo del presente paragrafo è quello di definire e identificare le norme e i requisiti da tenere in considerazione nell'ambito del trattamento dei dati personali, in relazione ai rapporti dell'Automobile Club Matera con le "terze parti".

Il paragrafo, in particolare, si riferisce alle "terze parti" che, in virtù delle attività e delle prestazioni svolte, entrano in contatto con le informazioni riservate in possesso dell'Ente.

Specificatamente, per "terze parti", si intende la totalità di persone fisiche esterne. Con il termine "terze parti", dunque, si fa riferimento alla categoria dei fornitori/collaboratori, ossia tutti gli attori da cui l'Ente, nell'ambito dello svolgimento dei propri processi, acquista beni e servizi.

Il presente paragrafo si applica a tutte le funzioni interne coinvolte nel processo di approvvigionamento di beni e servizi e di contrattualizzazione delle "terze parti", secondo quanto previsto dal Regolamento GDPR. In particolare l'Automobile Club Matera si impegna a predisporre clausole contrattuali relative alla sicurezza e al trattamento dei dati relativamente alla gestione di rapporti con le "terze Parti".

5.1 Contratti con "terze parti"

'Automobile Club Matera, intrattiene numerose relazioni contrattuali con "terze parti" con le quali condivide dati, informazioni e risorse. Tutto ciò espone l'Ente a numerosi rischi derivanti dall'accesso e utilizzo da parte di "terzi" di dati personali. L'Automobile Club Matera è tenuto a richiedere che tutti i soggetti con possibilità di accesso ai dati rispettino le regole di comportamento adeguate ai propri requisiti di sicurezza. Spetta, dunque, all'Ente il compito di:

- identificare i livelli di sicurezza in funzione della rilevanza delle informazioni condivise;

- definire i requisiti di sicurezza opportuni per tutelare le informazioni condivise con le "terze parti;
- considerare e valutare, nel processo di selezione delle "terze parti" e nella definizione dei requisiti di sicurezza da formalizzare nei contratti, le politiche di sicurezza già poste in essere da terze parti.

5-1-2 Rispetto delle norme di legge

Al fine di rispondere agli obblighi di legge, come previsto dal regolamento GDPR, garantendo dunque da eventuali ripercussioni in termini legali, economici e di immagine, le "terze parti" devono analogamente adeguarsi ai requisiti imposti dalle normative che si occupano di sicurezza aziendale e di protezione dei dati e che disciplinano le relazioni tra le parti. L'Automobile Club Matera, di concerto con il DPO ove necessario, definisce contrattualmente le normative cui devono attenersi le "terze parti".

5-1-3 Clausole con "Terze Parti"

Il livello di sicurezza richiesto alle "terze parti" è direttamente correlato alla prestazione fornita e, quindi, alla criticità delle informazioni condivise. Per questo motivo, le clausole contrattuali da considerare nella definizione del contratto possono essere molteplici e devono essere adattate al caso concreto.

5-1-4 Clausole contrattuali relative alla sicurezza

L'attività di predisposizione delle clausole contrattuali *standard* relative alla Sicurezza e al Trattamento dei dati, da applicare nella gestione dei rapporti con le "terze parti", è condotta dall'Automobile Club Matera. Esistono, tuttavia alcuni fornitori che, proprio per la peculiare tipologia di prestazione fornita, richiedono un particolare livello di attenzione. Rientrano in questa casistica i fornitori di soluzioni *software*. Per i contratti che regolano tali approvvigionamenti, infatti, si può rivelare necessaria la richiesta di specifici requisiti di controllo e diritti di accesso.

5.2 Ruoli e responsabilità

L'Automobile Club Matera, a garanzia di una corretta e omogenea gestione delle relazioni contrattuali con le "terze parti" identifica, al proprio interno, ruoli e responsabilità specifici, così da salvaguardare la sicurezza delle attività svolte dai soggetti coinvolti nei processi di Pianificazione, Realizzazione e Controllo.

Qualora la terza parte effettui un trattamento dei dati, in nome o per conto dell'Automobile Club Matera, la stessa deve essere nominata "Responsabile del trattamento", ai sensi dell'art.

28 del GDPR. A tal fine, l'Automobile Club Matera provvede a formalizzare apposito atto di nomina.

6. Politica per la gestione dei *Data Breach*

Il presente paragrafo e la Procedura qui menzionata sono redatti:

- nel rispetto di quanto previsto dal Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (GDPR), della normativa italiana di adeguamento nonché dei Provvedimenti dell'Autorità Garante per la protezione dei dati personali applicabili al contesto dell'Automobile Club Matera (complessivamente, la "Normativa *Privacy*");

- ai sensi degli art. 33 e 34 del GDPR, tenendo conto di quanto definito nei *Considerando* C85, C86, C87, C88;

- recepiscono le definizioni di cui all'art. 4 del GDPR.

Scopo della definizione di una Politica per la gestione dei *Data Breach* è quello di fornire al personale dell'Automobile Club Matera chiare indicazioni da seguire per una gestione efficace ed efficiente delle eventuali violazione dei dati trattati in possesso dell'azienda. Il GDPR descrive e regola, al riguardo, gli obblighi di notifica in caso di violazione dei dati personali. In particolare:

- Obbligo di notifica da parte del Titolare del trattamento verso l'Autorità di Controllo;
- Obbligo di notifica da parte del Titolare del trattamento verso il Soggetto Interessato;
- Obbligo di notifica da parte del Responsabile del trattamento verso il Titolare del trattamento.

Si definisce *Data Breach* una "violazione di dati personali", cioè ogni evento che comporti 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, ai sensi dell'art. 4 del Regolamento UE 2016/679 ("*General Data Protection Regulation*" o GDPR). Si possono distinguere tre categorie di violazioni:

- **Violazione di riservatezza**: divulgazione o accesso a dati personali non autorizzato o accidentale;
- **Violazione di integrità**: alterazione di dati personali non autorizzata o accidentale;
- **Violazione di disponibilità**: perdita, inaccessibilità o distruzione, accidentale o non autorizzata, di dati personali.

Il GDPR prevede e regolamenta specifici obblighi di notifica all' Autorità di controllo e, ricorrendone i presupposti, anche agli interessati in caso di violazione dei dati personali che presenti profili di rischio per i diritti e le libertà delle persone fisiche. Per gestire il processo di rilevazione di una violazione di dati personali e di valutazione della sua portata e per adempiere ai connessi obblighi di notifica, l'Ente ha elaborato una apposita procedura.

In caso di data breach, l'Automobile Club Matera si impegna ad avvisare immediatamente il DPO.

7. Gestione dei Rapporti con l'Autorità Garante

Nell'ottica di garantire l'efficacia del modello sviluppato e raggiungere i requisiti di *compliance* imposti dalla normativa *Privacy*, risulta necessario prevedere un processo di gestione dei rapporti con l'Autorità Garante che includa almeno:

- la consultazione preventiva (art. 36 del GDPR);
- il riscontro alle richieste dell'Autorità Garante;
- la notifica in caso di violazione dei dati personali;

Con riguardo alla consultazione preventiva ai sensi dell'art. 36 del GDPR, il Titolare del trattamento consulta l'Autorità Garante in via preventiva e qualora, all'esito della valutazione d'impatto sulla protezione dei dati di cui all'art. 35 del GDPR, risulti che il trattamento presenta un rischio elevato in assenza di misure adottate dall'Ente.

La comunicazione trasmessa all'Autorità Garante deve contenere almeno:

- la responsabilità degli attori coinvolti nel trattamento (titolari, contitolari, responsabili, ecc.);
- le finalità e i mezzi del trattamento previsto;
- le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati;
- i risultati della valutazione d'impatto effettuata;
- ogni altra informazione richiesta dall'Autorità Garante.

L'Autorità Garante può richiedere informazioni relativamente a segnalazioni o ricorsi degli Interessati oppure, nell'ambito di indagini conoscitive, richiedere contributi informativi specifici; inoltre può, anche in occasione delle verifiche ispettive, raccogliere documentazione relativamente alle misure tecniche e organizzative implementate a protezione dei Dati Personali trattati, documentazione contrattuale, modelli e documenti *privacy* estendendo l'analisi a qualsiasi altro processo, misura o trattamento effettuato da parte del Titolare.

In generale, tali richieste di informazioni hanno un termine che deve essere rispettato poiché la mancata esibizione o messa a disposizione delle informazioni richieste può originare una sanzione.

Nei casi di violazione dei Dati Personali, l'Automobile Club Matera deve notificare l'evento all'Autorità Garante senza ingiustificato ritardo, e ove possibile, entro 72 ore dal momento in cui viene rilevato l'evento di violazione dei Dati Personali.

A titolo esemplificativo e non esaustivo, gli eventi di possibile violazione dei Dati Personali possono essere costituiti da:

- **Distruzione di dati informatici o documenti cartacei** – intesa come indisponibilità irreversibile di dati con accertata impossibilità di ripristino degli stessi – conseguente ad eliminazione logica (ad esempio errata cancellazione dei dati nel corso di un intervento manuale o automatizzato) o fisica (ad esempio rottura di dispositivi di memorizzazione

informatica, incendio/allagamento locali dove sono archiviati i contratti ed altri documenti dei clienti);

- **Perdita di dati**, conseguente a smarrimento/furto di supporti informatici (ad esempio *Laptop*, *hard-disk*, *memory card*) o di documentazione contrattuale o altri documenti cartacei (in originale o in copia);
- **Accesso non autorizzato** o **intrusione a sistemi informatici**, tramite lo sfruttamento di vulnerabilità dei sistemi interni e delle reti di comunicazione oppure attraverso la compromissione o rilevazione abusiva di credenziali di autenticazione (ad esempio *user id* e *password*) per l'accesso ai sistemi;
- **Modifica non autorizzata di dati**, derivante ad esempio da un'erronea esecuzione di interventi sui sistemi informatici o intervento umano;
- **Rivelazione di dati e documenti a soggetti terzi non legittimati**, anche non identificati, conseguenti ad esempio alla fornitura di informazioni, anche verbali, a persone diverse dal soggetto legittimato (in assenza di delega formale di quest'ultimo), all'invio di fatture o altri documenti di valore contrattuale o esecutivo a soggetti diversi dall'effettivo destinatario o errata gestione di supporti informatici.

Descrizione delle misure adottate.

Nel caso in cui la violazione esponga gli Interessati a particolari rischi, in vista dei dati oggetto della stessa, dovrà essere prevista una notificazione diretta a ciascuno degli stessi salvo casi particolari di esclusione.

L'Autorità Garante e le altre autorità di vigilanza competenti possono effettuare ispezioni finalizzate a verificare l'effettiva implementazione da parte dell'Ente delle tutele previste dalle Normativa *Privacy*.

Nel corso delle ispezioni svolte dalle autorità di vigilanza, l'Ente adotterà le cautele e i presidi previsti dalle proprie *policy* interne riguardanti i rapporti con autorità di pubblica vigilanza.

Il DPO, ha il compito di interfacciarsi con i soggetti esterni in caso di ispezioni e dovrà gestire e coordinare la cooperazione tra le autorità e il Titolare.

Le Persone Autorizzate al trattamento dovranno prestare la massima collaborazione ai funzionari dell'autorità di vigilanza che effettuino le suddette ispezioni e fornire tutte le informazioni attinenti alle operazioni di Trattamento di Dati Personali svolte che siano richieste dagli stessi.

Sanzioni

L'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'Autorità di controllo ai sensi dell'art. 58, par. 2

(GDPR), o il negato accesso in violazione dell'art. 58, par. 1 (GDPR), comporta sanzioni pecuniarie.

Inoltre, la violazione della Normativa *Privacy* può avere impatti reputazionali negativi, anche rilevanti, sull'Ente.

Pertanto, il Titolare, avvalendosi dell'ausilio del *Data Protection Officer (DPO)*, attua, ove ritenuto necessario, i controlli sul processo di gestione degli adempimenti *Privacy*, con l'obiettivo di rilevare lo stato di conformità rispetto alla Normativa *Privacy*, nonché alle disposizioni contenute nel presente documento.

L'accertamento di determinate violazioni può anche comportare l'emissione, da parte delle autorità competenti nei confronti dell'Ente, di ordini finalizzati alla cancellazione dei Dati Personali raccolti o all'interruzione di determinate operazioni di Trattamento che si assumono illecite.

Regolamento adottato con Delibera Presidenziale n° 1 del 08-04-2025