



Policy per l'esecuzione dei controlli sull'operato dei Responsabili del trattamento

SOMMARIO

1. SCOPO E CAMPO DI APPLICAZIONE	3
2. RIFERIMENTI NORMATIVI E DOCUMENTALI	3
3. DEFINIZIONI	3
4. PROCEDURE OPERATIVE	4
5. NOMINA DEL RESPONSABILE DEL TRATTAMENTO	5
6. AGGIORNAMENTO DELLA POLICY	6
7. DOCUMENTI ALLEGATI	6

1. SCOPO E CAMPO DI APPLICAZIONE

Il Regolamento Generale sulla Protezione dei Dati (UE) 2016/679 (di seguito, GDPR) prevede che, qualora un trattamento venga effettuato per conto del titolare da parte di un soggetto esterno, quest'ultimo deve presentare 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.

A tal fine, tale soggetto deve essere conseguentemente nominato Responsabile del trattamento mediante contratto o altro atto giuridicamente valido.

La presente policy si applica a tutti i soggetti identificati come Responsabili del trattamento dei dati personali dell'Automobile Club Brescia, ai sensi dell'art. 28 del GDPR, e gli scopi principali della stessa sono i seguenti:

- verificare che i Responsabili del trattamento operino in conformità al GDPR e alle istruzioni fornite dall'Automobile Club Brescia;
- descrivere e regolamentare, secondo procedure standardizzate, le modalità operative interne per il monitoraggio periodico sull'operato dei Responsabili del trattamento dell'Automobile Club Brescia, ai sensi dell'art. 28 del GDPR.

2. RIFERIMENTI NORMATIVI E DOCUMENTALI

- Regolamento Generale sulla Protezione dei Dati (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/ce (Regolamento generale sulla protezione dei dati - RGDP);
- Decreto legislativo 30 giugno 2003, n. 196, recante il "Codice in materia di protezione dei dati personali", come modificato, da ultimo, dal Decreto legislativo 10 agosto 2018, n. 101;
- Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR;
- Decisione di esecuzione (UE) 2021/915 della Commissione del 4 giugno 2021 clausole contrattuali tipo per definire i rapporti tra titolari e responsabili del trattamento a norma dell'articolo 28 del GDPR.

3. DEFINIZIONI

"Dati personali": si intendono tutte le informazioni direttamente o indirettamente riconducibili ad una persona fisica così come definite ai sensi dell'art. 4 par. 1 del GDPR, che il Responsabile tratta per conto del Titolare allo scopo di fornire i servizi di cui al contratto.

"Categorie particolari di dati" c.d. dati sensibili: si intendono i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

"Interessato": si intende la persona fisica cui si riferiscono i dati personali.

"Servizi": si intendono i servizi resi dal responsabile oggetto del contratto o dell'atto di nomina nonché il relativo trattamento dei dati personali.

“Titolare”: si intende, ai sensi dell'art. 4, par. 7 del GDPR, 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.

“Responsabile del trattamento”: si intende, ai sensi dell'art. 4, par. 8 del GDPR, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

“Sub responsabile esterno”: si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, soggetto terzo (fornitore) rispetto alle Parti, a cui il responsabile del trattamento, previa autorizzazione del titolare, abbia, nei modi di cui al par. 4 dell'art. 28 del GDPR, eventualmente affidato parte dei servizi e che quindi tratta dati personali.

“Persona autorizzata al trattamento” o **“Autorizzato”**: si intendono le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

“Amministratore di sistema” o **“ADS”**: si intende la persona fisica dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise Resource Planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.

“Trattamento”: si intende, ai sensi dell'art. 4, par. 2 del GDPR, 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.

“Referente privacy”: soggetto formalmente designato dal responsabile della funzione per gli adempimenti privacy.

4. PROCEDURE OPERATIVE PER LO SVOLGIMENTO DEI CONTROLLI / VERIFICHE

Valutazione iniziale: prima o contestualmente alla stipula di un contratto, l'Automobile Club Brescia si assicura che il soggetto individuato quale Responsabile del trattamento si impegni a mettere in atto misure tecniche e organizzative adeguate in modo tale che i trattamenti soddisfino i requisiti del GDPR e garantiscano la tutela dei diritti degli interessati.

Clausole contrattuali: l'Automobile Club Brescia inserisce nel contratto con il Responsabile del trattamento le clausole relative alla protezione dei dati personali e designa il Responsabile del trattamento con apposito atto giuridico, che costituisce allegazione al contratto, includendo anche le necessarie istruzioni.

Verifiche periodiche: le verifiche sull'operato dei Responsabili del trattamento (Società in house, Delegazioni ACI/ACI Point, fornitori di servizi, e professionisti) possono essere eseguite con periodicità annuale, su almeno un campione pari al 15%, ovvero ogniqualvolta venga ritenuto opportuno dal Titolare del Trattamento. Tali controlli sono effettuati dal Direttore pro-tempore, nonché referente privacy, ovvero da un dipendente autorizzato.

Le verifiche e i controlli sull'operato dei Responsabili del trattamento possono avvenire anche attraverso la compilazione della “check list” (*all. n. 1*) sia da remoto, con riunioni online, sia in presenza presso la sede del Responsabile esterno (previo preavviso) oppure presso la sede

dell'Automobile Club Brescia, nonché mediante richiesta di informazioni e documenti. Tali verifiche riguardano l'accertamento sulla conformità alle disposizioni del GDPR e alle istruzioni ricevute delle operazioni di trattamento di dati personali eseguite per conto dell'Automobile Club Brescia.

In particolare, a seconda della categoria di Responsabile del trattamento dei dati personali dell'Automobile Club Brescia, sono posti in essere controlli e verifiche differenti, come di seguito specificato:

- SOCIETA' IN HOUSE
 - verifica della presenza del contratto/nomina a Responsabile esterno del trattamento, ai sensi dell'art. 28 GDPR;
 - verifica presenza del Registro dei Trattamenti e nomine ai dipendenti quali incaricati al trattamento dei dati.
- DELEGAZIONI e ACI Point
 - verifica della presenza del contratto/nomina a Responsabile esterno del trattamento, ai sensi dell'art. 28 GDPR;
 - verifica corretto trattamento dei dati personali e corretta detenzione e utilizzo dell'informativa Privacy relativi al Data Base associativo dell'AC;
 - attestazione da parte del Delegato che i supporti cartacei relativi al rilascio/rinnovo delle tessere ACI sono custoditi correttamente;
- FORNITORI / PROFESSIONISTI
 - verifica della presenza del contratto/nomina a Responsabile esterno del trattamento, ai sensi dell'art. 28 GDPR;
 - richiesta annuale di una sintetica relazione in merito al trattamento dei dati per conto dell'Automobile Club Brescia, ovvero compilazione della check list allegata alla presente policy;
- AMMINISTRATORE DI SISTEMA INFORMATICO
 - verifica della presenza del contratto/nomina a Responsabile di sistema informatico dell'Ente;
 - richiesta annuale di una sintetica relazione in merito all'attività svolta sul sistema informativo dell'Automobile Club Brescia, con indicazione del personale incaricato ad operare sul sistema informatico dell'Ente.

Tutti i controlli sono documentati da apposito verbale (check list) per le successive ed eventuali ulteriori verifiche.

Una volta cessato, per qualsiasi motivo, il rapporto contrattuale con il fornitore, bisognerà procedere con l'aggiornamento dell'elenco dei responsabili del trattamento.

5. NOMINA DEL RESPONSABILE DEL TRATTAMENTO

Prima o contestualmente all'affidamento e alla sottoscrizione del contratto, si dovrà procedere alla formalizzazione della nomina del Responsabile del trattamento ai sensi dell'art. 28 GDPR. A tal fine, l'ufficio incaricato della formalizzazione del rapporto contrattuale, al momento della sottoscrizione del contratto, utilizzerà l'atto di nomina, secondo i modelli in uso presso l'Automobile Club Brescia, il quale dovrà contenere almeno:

- oggetto, durata e natura del trattamento;
- tipologia di dati trattati e categorie di interessati;
- obblighi del responsabile (riservatezza, sicurezza, sub-responsabili) (art. 28, par. 3 GDPR);
- istruzioni del titolare e modalità di assistenza per l'esercizio dei diritti degli interessati (art. 28, par. 3, lettera e GDPR);

- misure di sicurezza tecniche e organizzative (art. 32 GDPR);
- obbligo di notificare eventuali violazioni di dati (art. 33 e 34 GDPR).

Copia dell'atto firmato andrà conservato agli atti dell'Ente.

6. Aggiornamento della Policy

La presente policy entra in vigore alla data di approvazione e può essere aggiornata periodicamente in caso di modifiche organizzative o normative.

7. Documenti Allegati

Allegato 1: Check list verifica fornitore