Accordo tra il Titolare e il Responsabile esterno del trattamento ai sensi dell'art. 28 del Regolamento generale sulla protezione dei dati (UE) 2016/679

Oggetto: disciplina dei rapporti tra la Regione Abruzzo e l'Automobile Club d'Italia in materia di trattamenti di dati personali nell'ambito delle attività previste dall'Accordo di Cooperazione in materia di tasse automobilistiche in ordine a: istruzioni, natura e finalità del trattamento, tipo di dati personali e categorie di interessati, obblighi e diritti del titolare del trattamento, compiti e responsabilità del responsabile del trattamento in osservanza dell'articolo 28 paragrafo 3) del Regolamento Europeo n. 679/2016.

PREMESSE

- Con DGR n. 935 del 30.12.2024, è stato approvato lo schema di Accordo di Cooperazione in materia di tasse automobilistiche per il periodo 01.01.2025-31.12.2025 tra la Regione Abruzzo (di seguito anche "Regione") e l'Automobile Club d'Italia (di seguito anche "ACI"), di cui il presente atto ne costituisce parte integrante.

Ciò premesso,

TRA

Regione Abruzzo, codice fiscale n. 80003170661, legalmente rappresentata dalla Dott.ssa Lorenza De Antoniis, nella sua qualità di Dirigente del Servizio Entrate della Regione Abruzzo incaricato con Deliberazione di Giunta Regionale n. 119 del 15.02.2024, ai sensi dell'art. 24 L.R. 14-9-1999 n. 77 "Norme in materia di organizzazione e rapporti di lavoro della Regione Abruzzo", domiciliato presso la sede dell'Ente, autorizzato alla stipula dell'Accordo di Cooperazione ai sensi della DGR n. 935 del 30.12.2024.

E

l'Automobile Club d'Italia - ACI, codice fiscale 00493410583, con sede legale in via Marsala, 8, 00185 Roma, legalmente rappresentato dal Presidente Ing. Angelo Sticchi Damiani,

si conviene quanto segue:

Articolo 1
Definizioni

Ai fini della presente disciplina valgono le seguenti definizioni:

- Per "Legge Applicabile" o "Normativa Privacy", si intende il Regolamento 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 (di seguito, per brevità, "GDPR") a far data dal 25.05.2018, il D. Lgs. 196/2003 e s.m.i. e i suoi allegati (di seguito, per brevità, anche "Codice della Privacy"), nonché qualsiasi altra normativa sulla protezione dei dati personali applicabile in Italia, ivi compresi i provvedimenti dell'Autorità Garante per la Protezione dei dati personali (di seguito, per brevità, "Garante");

- per "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 ai fini dell'espletamento delle attività previste dall'Accordo di Cooperazione;

- per "Interessato": si intende la persona fisica cui si riferiscono i dati personali;

- per "Attività": si intendono le attività rese dal Responsabile nell'ambito dell'Accordo di Cooperazione oggetto del presente contratto, nonché il relativo trattamento dei dati personali;

- per "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. Il Titolare del Trattamento sono rispettivamente ACI e Regione Abruzzo;

- per "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. Il Responsabile del trattamento dei dati personali" ai sensi dell'art. 28 dell'GDPR sono rispettivamente ACI e Regione Abruzzo;

- per "Ulteriore Responsabile": 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 lo svolgimento di parte delle attività di cui all'Accordo o concesso l'accesso all'Archivio delle tasse automobilistiche in sola visualizzazione.

- per "Misure di Sicurezza": si intendono le misure di sicurezza di all'art. 32 del GDPR;

- per "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;

- per “Violazione di Dati personali” (c.d. Data Breach), si intende ai sensi dell'art. 4, par. 12 del GDPR, la violazione di sicurezza che comporta anche 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;
- per “Amministratore di Sistema” si intende la figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti; è altresì considerato tale anche altra figura equiparabile dal punto di vista dei rischi relativi alla protezione dei dati, quale l’amministratore di basi di dati, l’amministratore di reti e di apparati di sicurezza e l’amministratore di sistemi software complessi utilizzati in grandi organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali;
- per “Responsabile della protezione dei dati (Data Protection Officer – DPO)” si intende la figura di cui all’articolo 37 e seguenti del GDPR, nominato, per quanto concerne la Regione Abruzzo, con decorrenza dal 1 dicembre 2023, con determinazione dirigenziale n. 12 /CAP del 16/11/2023 nella società Pluconform s.r.l.s. che ha indicato il DPO designato quale referente da rendere alla Giunta Regionale D’Abruzzo, nella persona fisica dell’Avv. Alberto Faccini Caroppo; per quanto concerne ACI, l'incarico è stato confermato al Dott. Mauro Annibali, con deliberazione del Presidente ACI n.8214 del 09/02/2024 e con decorrenza dal 09/02/2024.

Articolo 2
Oggetto

1. La presente disciplina riguarda le operazioni di trattamento dei dati personali contenuti nell’archivio regionale delle Tasse Automobilistiche rientranti nella sfera di titolarità di Regione Abruzzo effettuate da ACI nell’ambito delle attività previste dall’Accordo di Cooperazione, e le operazioni di trattamento dei dati personali contenuti nell'archivio Nazionale della Tassa Automobilistica rientranti nella sfera di titolarità ACI, effettuate da Regione Abruzzo nell’ambito delle attività dell’Accordo di Cooperazione il cui schema è stato approvato con DGR n. 935 del 30.12.2024. Il trattamento dei dati dovrà limitarsi alle operazioni strettamente necessarie allo svolgimento delle attività indicate nell’Accordo di Cooperazione e relativi allegati, ai quali si rimanda.

2. I dati saranno trattati soltanto dai soggetti che dovranno utilizzarli per l’esecuzione delle attività previste dall’Accordo di Cooperazione. ACI e Regione Abruzzo nell’ambito dei reciproci ruoli di responsabili esterni del trattamento non potranno comunicare ad altri soggetti i dati personali di cui venga a conoscenza, né utilizzarli autonomamente, per scopi diversi da quelli sopra menzionati.

Articolo 3
Durata e finalità

1. La presente disciplina rimarrà in vigore fino alla cessazione delle attività svolte da ACI, in riferimento al

trattamento dei dati personali rientrati nella sfera della titolarità di Regione Abruzzo e da Regione Abruzzo in riferimento al trattamento dei dati rientranti nella sfera della titolarità di ACI.

2. Resta fermo il diritto del Titolare, in qualsiasi momento, di revocare e/o modificare rispettivamente la nomina di ACI e di Regione Abruzzo quale responsabile del trattamento dei dati personali, ivi compresi i relativi compiti e responsabilità, salvo ogni eventuale obbligo di legge.

3. I trattamenti dei dati personali saranno effettuati dall'ACI e dalla Regione Abruzzo per il tempo strettamente necessario al conseguimento della finalità per le quali i dati sono raccolti e successivamente trattati in relazione alle attività previste dal Accordo di Cooperazione.

Articolo 4
Tipologie di dati e Categorie di interessati

1.ACI per conto della Regione Abruzzo effettua operazioni di trattamento aventi ad oggetto tutte le categorie di dati personali rientranti nella titolarità dell'Archivio regionale (cittadini, utenti, etc.), Regione Abruzzo per conto di ACI effettua operazioni di trattamento aventi ad oggetto tutte le categorie di dati personali rientranti nella titolarità dell'archivio nazionale (cittadini, utenti, etc.), relativamente alle attività previste dall'Accordo di Cooperazione.

Articolo 5
Modalità e istruzioni

1.Le modalità e le istruzioni per il Trattamento dei dati personali impartite dal Titolare al Responsabile sono contenute nella presente disciplina, come riportate nei successivi articoli e nell'allegato "INFORMAZIONI E ISTRUZIONI AGLI AUTORIZZATI".

Articolo 6
Obblighi e doveri del Responsabile del trattamento

1.Il Responsabile è obbligato a mettere in atto misure tecniche ed organizzative atte a garantire un livello di sicurezza adeguato al rischio, a salvaguardare la riservatezza, l'integrità e la disponibilità dei dati trattati (comprese la cifratura e la pseudonimizzazione, effettuazione di *back up* o di *restore*, di un piano di *Disaster Recovery* e di *Business Continuity*, nonché di controlli atti a testare l'efficacia delle misure adottate), in modo tale che i trattamenti effettuati nell'ambito dello svolgimento delle attività di competenza previste dall'Accordo di Cooperazione, soddisfi i requisiti di cui al GDPR, nonché tuteli i diritti degli interessati al trattamento. In particolare, il Responsabile si impegna a mantenere una struttura ed una organizzazione adeguata per la corretta esecuzione delle attività di cui al Accordo di Cooperazione (per sé e per i propri dipendenti e collaboratori interni ed esterni), nel rispetto delle disposizioni normative, nonché nel rispetto delle istruzioni specificatamente impartite dal Titolare nel presente atto e/o di volta in volta impartite in riferimento allo svolgimento delle attività di cui trattasi.

2.In particolare, ACI e Regione Abruzzo in qualità di Responsabile sono rispettivamente obbligati a:

- effettuare le operazioni di trattamento dei dati relative alle attività di competenza previste dall'Accordo di Cooperazione, nel rispetto delle disposizioni normative vigenti;

- adottare le misure tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio in osservanza delle disposizioni di cui agli articoli 32 e 35 del GDPR, al fine di garantire il rispetto del principio della "Protezione dei dati fin dalla progettazione e protezione predefinita cui all'art. 25 del GDPR, già in fase contrattuale ";
- nominare un responsabile della protezione dei dati (Data Protection Officer) nei casi previsti dalla normativa vigente;
- eseguire i trattamenti connessi alle attività espletate nell'ambito dell'Accordo di Cooperazione, compatibilmente e nei limiti delle finalità perseguite. Qualora sorgesse la necessità di effettuare trattamenti su dati personali diversi ed eccezionali rispetto a quelli normalmente eseguiti, ACI e Regione Abruzzo dovranno informare il Titolare del trattamento ed il Data Protection Officer (DPO) di Regione Abruzzo e di ACI.
- adottare le misure organizzative e procedurali necessarie al fine di autorizzare il personale preposto alle operazioni di trattamento, nonché impartire allo stesso le necessarie istruzioni in materia di privacy nel rispetto delle disposizioni normative, nonché delle condizioni e dei termini contemplati nel presente atto, ivi compresi le istruzioni impartite di volta in volta, quando necessarie. Il Responsabile ha l'obbligo di garantire che il personale autorizzato al trattamento sia vincolato legalmente al rispetto degli obblighi di riservatezza.
- garantire l'adozione delle misure di sicurezza di cui all'articolo 32 del GDPR. In particolare - tenuto conto dello stato dell'arte delle misure di sicurezza adottate a protezione dei trattamenti dei dati per conto di Regione Abruzzo e di ACI come previste dal contratto vigente, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento e, sulla base delle risultanze dell'analisi dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati - porre in essere le opportune azioni organizzative per l'ottimizzazione di tali misure, per garantire un livello di sicurezza adeguato al rischio. Tali misure comprendono, tra le altre:

- la cifratura dei dati personali;
- misure idonee a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- misure idonee a garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico;
- procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento e predisporre, a cadenza annuale, un rapporto scritto in merito agli adempimenti eseguiti ai fini della legge ed alle conseguenti risultanze, da consegnare al Titolare e permettere eventuali controlli concordati rispettivamente da parte di Regione Abruzzo o di Aci o loro delegato;

- distruggere, ovvero riconsegnare i dati personali al Titolare, secondo le indicazioni impartite da Aci o da Regione Abruzzo, alla cessazione del trattamento, a meno che non sia previsto per legge un termine di conservazione di dati.
- trasmettere al Titolare del trattamento la documentazione tecnica relativa sia alle misure di sicurezza in atto sia alle modifiche in seguito applicate; inoltre renderà disponibili al Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli adempimenti normativi previsti dal GDPR, consentendo di effettuare periodicamente attività di verifica, comprese ispezioni realizzate dal Titolare stesso o da un altro soggetto da questi incaricato.
- adottare le politiche interne e impegnarsi ad attuare le misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure (privacy by design); adottare ogni misura adeguata a garantire che i dati personali siano trattati in ossequio al principio di necessità, ovvero che siano trattati solamente per le finalità previste e per il tempo strettamente necessario al raggiungimento delle stesse (privacy by default);
- tenere, ai sensi dell'art. 30 del GDPR e nei limiti di quanto esso prescrive, un Registro delle attività di Trattamento effettuate sotto la propria responsabilità rispettivamente per conto di Regione Abruzzo o di Aci e cooperare con il Titolare e con l'Autorità Garante per la protezione dei dati personali, laddove ne venga fatta richiesta ai sensi dell'art. 30, comma 4 del GDPR;
- assistere il Titolare, ove richiesto, nello svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente a quanto prescritto dall'art. 35 del GDPR e nella eventuale consultazione del Garante per la protezione dei dati personali, prevista dall'art. 36 del GDPR;
- soddisfare le richieste ritenute legittime, qualora riceva istanze degli interessati in esercizio dei loro diritti di cui dall'art. 15 all'art. 22 del GDPR;
- garantire gli adempimenti e le incombenze anche formali verso l'Autorità Garante, quando richieste e nei limiti dovuti, disponendosi a collaborare tempestivamente, per quanto di competenza, sia con il Titolare sia con l'Autorità. In particolare, ACI dovrà:

a) fornire informazioni sulle operazioni di trattamento svolte;

b) consentire l'accesso alle banche dati oggetto delle operazioni di trattamento;

c) consentire l'effettuazione di controlli;

d) mettere in atto quanto necessario per una tempestiva esecuzione dei provvedimenti inibitori, di natura temporanea.

- garantire l'applicazione in merito alle misure di sicurezza da adottare al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati personali, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, secondo quanto prescritto dagli artt. 25 e 32 del GDPR EU 2016/679 in materia di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (Privacy by Design) e in materia di misure di sicurezza;
- informare il Titolare tempestivamente ove riscontri carenze sulle misure di sicurezza o su qualunque aspetto relativo ai trattamenti che dovesse comportare responsabilità penale, civile e ammnistrativa del medesimo Titolare. In particolare, è tenuta altresì ad informate periodicamente il

Titolare sullo stato dell'arte relativo agli obblighi e alle prescrizioni contemplate dal GDPR, segnalando contestualmente le eventuali azioni da intraprendere;

- permettere lo svolgimento dei controlli previsti dall'art. 28, par. 3 lett. h) del RGPD 2016/679 da parte di Aci o Regione Abruzzo o da altro soggetto da essi incaricato;
- non trasferire i dati personali verso un paese terzo o un'organizzazione internazionale, salvo che non abbia preventivamente ottenuto l'autorizzazione scritta da parte del Titolare e nel rispetto della normativa applicabile.

Articolo 7

Ulteriori Obblighi del Responsabile in materia di Amministratore di Sistema

1. Laddove le prestazioni previste nell'Accordo di Cooperazione implichino l'erogazione di servizi di amministrazione di sistema, ACI e Regione Abruzzo, in qualità di Responsabile del trattamento, si impegnano a:

- individuare i soggetti ai quali affidare il ruolo di Amministratori di Sistema (System Administrator), Amministratori di Base Dati (Database Administrator), Amministratori di Rete (Network Administrator) e/o Amministratori di Software Complessi e, sulla base del successivo atto di designazione individuale, impartire le istruzioni a detti soggetti, vigilando sul relativo operato;
- assegnare ai suddetti soggetti una *user id* che contenga riferimenti agevolmente riconducibili all'identità degli Amministratori e che consenta di garantire il rispetto delle seguenti regole:

a) divieto di assegnazione di *user id* generiche e già attribuite anche in tempi diversi;

b) rimozione dei privilegi di Amministratore delle *user id* attribuite alle figure di Amministratori che non necessitano più di accedere ai dati;

c) associare alle *user id* assegnate agli Amministratori una password di adeguata complessità nel rispetto delle "*best practices*" vigenti;

d) assicurare la completa distinzione tra utenze privilegiate e non privilegiate di amministratore, alle quali devono corrispondere credenziali diverse;

e) assicurare che i profili di accesso, in particolare per le utenze con privilegi amministrativi, rispettino il principio del need-to-know, ovvero che non siano attribuiti diritti superiori a quelli realmente necessari per eseguire le normali attività di lavoro. Le utenze con privilegi amministrativi devono essere utilizzate per il solo svolgimento delle funzioni assegnate;

f) mantenere aggiornato un inventario delle utenze privilegiate (Anagrafica AdS), anche attraverso uno strumento automatico in grado di generare un alert quando è aggiunta una utenza amministrativa e quando sono aumentati i diritti di una utenza amministrativa.

Articolo 8

Violazione dei Dati personali

1. IL responsabile è tenuto il Titolare ed il Data Protection Officer, tempestivamente e senza ingiustificato ritardo, al fine di rispettare i termini di cui all'articolo 33 GDPR, di ogni violazione di dati personali (cd. data breach) derivante dall'esecuzione delle attività previste dall'Accordo di Cooperazione. Tale notifica – da effettuarsi tramite PEC alla Direzione regionale competente in materia e contestualmente al DPO di Regione Abruzzo e/o di ACI - deve essere accompagnata da ogni documentazione utile, ai sensi degli artt. 33e 34 del GDPR, per permettere al Titolare, ove ritenuto necessario, di notificare la violazione all'Autorità Garante per la protezione dei dati personali e/o darne comunicazione agli interessati, entro il termine di 72 ore da quando il Titolare ne è venuto a conoscenza.

Nel caso in cui il Titolare debba fornire informazioni aggiuntive alla suddetta Autorità Garante, ACI o Regione Abruzzo supporteranno il Titolare nella misura in cui le informazioni richieste e/o necessarie per l'Autorità Garante siano esclusivamente in possesso del Responsabile e/o di suoi ulteriori Responsabili.

Articolo 9

Nomina di ulteriori responsabili (sub-Responsabili)

1. In esecuzione e nell'ambito di quanto previsto dall'Accordo di Cooperazione, ACI e/o Regione Abruzzo, ai sensi dell'art. 28 comma 2 del GDPR, è autorizzata, salva diversa comunicazione scritta del Titolare, a ricorrere alla nomina di Ulteriori Responsabili.

2. La nomina di Ulteriori responsabili da parte di ACI e/o di Regione Abruzzo sarà possibile a condizione che sull'Ulteriore Responsabile siano imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel presente Atto, incluse garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti richiesti dalla Normativa Privacy.

4. Qualora gli Ulteriori responsabili omettano di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi dell'Ulteriore Responsabile.

Articolo 10

Responsabilità

1.Il Responsabile ha la piena responsabilità diretta verso gli Interessati per i danni subiti derivanti da inadempimento o da violazione delle istruzioni legittime del Titolare con riferimento alle attività affidate attraverso l'Accordo di Cooperazione, ai sensi dell'art. 82 del RGPD 2016/679 e ai servizi in cooperazione.

2.Le Parti del presente Atto sono soggette, a cura dell'Autorità di controllo, alle sanzioni pecuniarie ai sensi dell'art. 83 del GDPR. Ferma restando l'applicazione di tale norma e, in generale, della Normativa Privacy, il mancato rispetto delle funzioni delegate e delle istruzioni impartite al Responsabile ovvero la violazione delle condizioni prescritte, darà luogo all'applicazione di penali e/o alla risoluzione della cooperazione.

3. Il Responsabile si obbliga a manlevare il Titolare e tenere quest'ultimo indenne da qualsiasi tipo di conseguenza, sia civile che amministrativa, responsabilità, perdita, onere, spesa, danno o costo da quest'ultimo sopportato per comportamenti attribuibili al Responsabile, ovvero di violazioni agli obblighi o adempimenti prescritti dalla Normativa Privacy, ovvero di inadempimento delle pattuizioni contenute nel presente Atto, ovvero dei compiti assegnati dal Titolare. Letto, approvato e sottoscritto

Per la Regione Abruzzo

Dirigente del Servizio Entrate della Regione Abruzzo

Dott.ssa Lorenza De Antoniis

LORENZA DE ANTONIIS
DIRIGENTE REGIONE
ABRUZZO
13.01.2025 11:10:25
GMT+02:00

Per l'Automobile Club d'Italia

Il Presidente

Ing. Angelo Sticchi Damiani

Firmato da Angelo Sticchi Damiani il 05-02-2025

INFORMAZIONI E ISTRUZIONI AGLI AUTORIZZATI

In ottemperanza alle disposizioni del Codice in materia di protezione dei dati personali (D.Lgs 196/03) e s.m.i. recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 (GDPR) ed in relazione alle attività svolte nell'ambito dell'Accordo di cooperazione in materia di tasse automobilistiche per il periodo 01.01.2025-31.12.2025 tra la Regione Abruzzo e l'Automobile Club d'Italia, il cui schema è stato approvato con DGR n. 935 del 30.12.2024, l'autorizzato, dovrà effettuare i trattamenti di dati personali di competenza attenendosi scrupolosamente alle seguenti istruzioni e ad ogni ulteriore indicazione, anche verbale, che potrà essere fornita dal *Titolare del Trattamento* o dal *Responsabile del Trattamento* presso il quale opera.
I dati personali devono essere trattati:

a) in osservanza dei criteri di riservatezza;
b) in modo lecito e secondo correttezza;
c) per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati;
d) nel pieno rispetto delle misure di sicurezza definite, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Le misure di sicurezza definite sono obbligatorie, e sono state anche distinte in funzione delle seguenti modalità di trattamento dei dati:

1. senza l'ausilio di strumenti elettronici (es. dati in archivi cartacei o su supporti magnetici/ottici);
2. con strumenti elettronici (es. PC, tablet o smartphone)
3. generali

Trattamenti dati con Strumenti Elettronici
Gli autorizzati al trattamento dovranno attenersi alle seguenti misure di sicurezza:

- accedere ai sistemi informativi esclusivamente per mezzo di credenziali di autenticazione personali; le credenziali di autenticazione consistono in un codice (user id o username) per l'identificazione dell'autorizzato, associato ad una parola chiave (password) conosciuta solo dall'autorizzato;
- utilizzare la password con una lunghezza minima di otto caratteri, composte sia da numeri che lettere (o, se il sistema informativo in uso non lo permette, dal numero massimo di caratteri consentito) e differente dallo user id;
- nella generazione della password non utilizzare elementi o notizie facilmente riconducibili all'autorizzato e non utilizzare password simili alla precedente;
- modificare la password al primo utilizzo del sistema informativo, quindi ogni volta che viene richiesto dal sistema (al massimo 6 mesi, 3 mesi se i dati trattati sono particolari - ad. es. di salute - e/o giudiziari) e <u>nel caso vi sia il dubbio che la stessa password abbia perso il carattere di segretezza</u>;
- qualora il sistema non renda obbligatoria la modifica della password nel rispetto dei predetti termini, provvedere autonomamente a tale variazione;
- adottare particolari cautele per assicurare la segretezza della password (evitare la digitazione in presenza di terzi, conservarne i riferimenti in luogo non accessibile a terzi) custodendola con diligenza e riservatezza;
- per le banche dati automatizzate che utilizzano il proprio codice di accesso personale, evitare di operare su postazioni di lavoro al fine di non incorrere in trattamenti non autorizzati;
- tenere un comportamento corretto durante la navigazione in internet, così come previsto dalle disposizioni interne sulla modalità di utilizzo dei servizi di rete.
- non aprire messaggi di posta provenienti da soggetti esterni *non accreditati*;
- non comunicare la mail istituzionale a siti per i quali non siete interessati per fini lavorativi;
- non trasmettere dati particolari (ex sensibili) via e-mail. Nel caso in cui sia strettamente necessaria tale forma di trasmissione per ragioni d'ufficio, occorrerà porre in essere gli accorgimenti atti ad impedire la visione del contenuto del file da parte di soggetti non autorizzati o non legittimati al trattamento,

che siano diversi dai destinatari delle comunicazioni elettroniche. In particolare, si raccomanda il ricorso all'uso di tecniche di criptazione o di cifratura dei messaggi, ovvero il ricorso all'uso di codificazione dei dati contenuti nel testo delle comunicazioni;

- bloccare la propria stazione di lavoro durante la pausa pranzo, ovvero in tutte le occasioni in cui ci si assenti o ci si allontani anche temporaneamente dalla propria postazione di lavoro; nel caso in cui fosse necessario mantenere accesa la postazione di lavoro, utilizzare i metodi messi a disposizione dal sistema per bloccare la stessa, come ad esempio il blocco sessione o il salvaschermo con password;
- adottare tutte le cautele necessarie atte ad evitare l'accesso ai dati personali trattati o in trattamento sia cartaceo anche se dipendenti o altri autorizzati;
- non lasciare la propria stazione di lavoro incustodita e collegata alla rete e/o ai sistemi informativi con il proprio account (nome utente) e password;
- non alterare in alcun modo la configurazione software della stazione di lavoro, evitando di installare qualunque software sconosciuto o non approvato;
- non utilizzare la rete dell’Amministrazione per fini non espressamente autorizzati;

Trattamenti senza l’ausilio di Strumenti Elettronici
Gli autorizzati al trattamento dovranno attenersi alle seguenti istruzioni:

- garantire sempre la corretta custodia dei dati personali; i documenti non devono essere lasciati incustoditi sulla propria scrivania e/o in luoghi aperti al pubblico in assenza di altri autorizzati addetti al medesimo trattamento; non devono essere consultati da altri autorizzati non abilitati al trattamento; non possono essere riprodotti o fotocopiati se non per esigenze connesse alla finalità del trattamento;
- per il tempo necessario allo svolgimento delle operazioni di trattamento si dovrà diligentemente controllare e custodire gli atti e documenti contenenti dati personali per evitare visione, possesso, utilizzo non autorizzati; conservare i documenti o gli atti che contengono dati particolari (ex dati sensibili) e/o giudiziari in archivi ad accesso controllato (armadi/schedari/contenitori chiusi da apposita serratura oppure soggetti a sorveglianza da parte di personale preposto);
- al termine delle operazioni di trattamento, restituire tempestivamente la documentazione prelevata dagli archivi ed assicurarsi che questa venga opportunamente risposta;
- in caso di utilizzo di stampante, fotocopiatrice o fax condivisi da vari utenti e collocati al di fuori dei locali ove è posta la singola postazione di lavoro, le stampe devono essere immediatamente raccolte e custodite con le modalità sopra descritte; Qualora i documenti da stampare contengano dati particolari è necessario, nei limiti del possibile, presenziare la fase di stampa;
- non gettare via copie cartacee contenenti dati personali, senza averle distrutte prima in modo opportuno o comunque avere reso l’identificazione dell’interessato impossibile;
- adottare misure che siano idonee a limitare la conoscenza dei dati personali e/o particolari qualora essi siano presenti nei flussi documentali dell'Amministrazione garantendo il rispetto della riservatezza dei dati degli interessati ad esempio riponendo i documenti in cassetti o armadi debitamente chiusi a chiave.
- è vietato cedere ad altri dati personali di cui si è venuti a conoscenza durante lo svolgimento dell’incarico;

Misure di carattere generale
Gli autorizzati al trattamento dovranno attenersi alle seguenti istruzioni:

- assicurare la riservatezza opportuna e necessaria affinché il trattamento dei dati, sia effettuato in conformità alle disposizioni del GDPR e del D.lgs 196/2003 s.m.i.;
- assicurare la somministrazione dell’informativa al trattamento dati ogni qual volta venga coinvolto un nuovo interessato;
- assicurarsi, quando previsto, che sia stata rilasciato il consenso al trattamento dati da parte dell’interessato;
- rispettare, se presente, il documento sulla sicurezza dei dati, predisposto dall’Amministrazione;
- è vietato l’utilizzo improprio di documenti, dati, informazioni a qualsiasi titolo posseduti, ricevuti o trasmessi;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli e nei supporti informatici avendo cura che l’accesso ad essi sia possibile solo ai soggetti autorizzati;

- è vietato cedere ad altri dati personali di cui si è venuti a conoscenza durante lo svolgimento dell'incarico;
- informare tempestivamente il proprio referente di ogni questione rilevante in relazione al trattamento di dati personali effettuato e di eventuali richieste pervenute dagli interessati;
- nel caso in cui si constati o si sospetti un disguido o un incidente che abbia messo o possa mettere a repentaglio la sicurezza e/o la riservatezza dei dati trattati, darne immediata comunicazione al proprio referente;
- segnalare al proprio referente eventuali circostanze, che richiedano il necessario ed opportuno aggiornamento delle misure di sicurezza adottate, al fine di ridurre al minimo i rischi di diffusione, distruzione o perdita anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- fornire al Titolare o al Responsabile del Trattamento, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire loro una adeguata azione di controllo e verifica di eventuali incidenti che possano essersi verificati;
- eseguire qualsiasi operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge;
- recepire nuove indicazioni fornite dal Titolare del Trattamento o dal Responsabile del Trattamento anche partecipando a percorsi formativi quando previsti;
- trattare i dati personali, eventualmente riferiti a categorie particolari (art. 9) o relativi a condanne penali e reati (art. 10) è ammesso se lecito (art. 6) e cioè quando:
    - l'interessato ha espresso il consenso al trattamento dei propri dati personali;
    - il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
    - il trattamento è necessario per adempiere ad un obbligo di legge cui è tenuto il Titolare o per salvaguardare gli interessi vitali dell'interessato;
    - il trattamento è necessario per il perseguimento del legittimo interesse del Titolare;
- garantire all'interessato l'esercizio dei diritti sui propri dati secondo quanto previsto dal GDPR (es: diritto di accesso, di rettifica, di limitazione, di portabilità, di opposizione, ecc.) segnalando al proprio referente qualsiasi richiesta in questo senso.