REGOLAMENTO PRIVACY DELL'AUTOMOBILE CLUB D'ITALIA

INDICE

CAPO I - DISPOSIZIONI GENERALI

Art. 1
Finalità e oggetto

1. Il "Regolamento dell'Automobile Club d'Italia in materia di protezione dei dati personali" (di seguito, per brevità, "Regolamento Privacy ACI") costituisce misura organizzativa posta in essere dall'Ente, ai sensi e per gli effetti dell'art. 24 par. 1 del "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 e che abroga la direttiva 95/46/CE - regolamento generale sulla protezione dei dati " (di seguito, per brevità, "RGPD").

2. Il presente Regolamento, in particolare, formalizza il modello organizzativo di protezione dei dati personali nell'ACI (di seguito, per brevità, "Modello organizzativo Privacy ACI"), in conformità al RGPD ed al decreto legislativo 30 giugno 2003, n. 196 ("Codice in materia di protezione dei dati personali recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679" - come modificato dal decreto legislativo 10 agosto 2018 n. 101 e, da ultimo, dal decreto legge 8 ottobre 2021 n. 139 - di seguito, per brevità, "Codice privacy"), e definisce le politiche, di cui all'art. 24 par. 2 dello stesso RGPD, nonché le regole interne per l'adeguato svolgimento delle attività di trattamento dei dati personali da parte dell'Ente in qualità di titolare, contitolare o responsabile dello stesso trattamento secondo le disposizioni di cui al Capo IV dello stesso RGPD.

Art. 2
Principi e definizioni

1. L'ACI si conforma ai principi enunciati al Capo II del RGPD, in base ai quali i dati personali devono essere trattati nel rispetto delle prescritte regole di:

- liceità, correttezza e trasparenza;
- limitazione delle finalità;
- minimizzazione dei dati;
- esattezza;
- limitazione della conservazione;
- integrità e riservatezza;
- responsabilizzazione.

2. Qualora nel presente Regolamento ricorrano specifiche locuzioni utilizzate dal RGPD e dal Codice privacy trovano applicazione le definizioni dallo stesso adottate e, in particolare, quelle di cui all'art. 4 del medesimo RGPD.

3. Secondo le definizioni adottate dal RGPD, in particolare, ai fini del presente Regolamento si intende per:

- **«dato personale»:** qualsiasi informazione riguardante una persona fisica identificata o identificabile (**«interessato»**); 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;

- **«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;
- **«limitazione di trattamento»**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- **«profilazione»**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- **«archivio»**: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- **«titolare del trattamento»**: 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- **«responsabile del trattamento»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- **«destinatario»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi;
- **«terzo»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- **«consenso dell'interessato»**: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- **«violazione dei dati personali»**: la violazione di sicurezza che comporta 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;
- **«dati genetici»**: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- **«dati biometrici»**: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

- **«dati relativi alla salute»**: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- **«servizio della società dell'informazione»**: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio.

4. Secondo le definizioni adottate da Codice privacy, in particolare, ai fini del presente Regolamento si intende per:

- **"comunicazione"**: dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies dello stesso Codice, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
- **"diffusione"**: dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Art. 3
Ambito di applicazione

1. Il presente Regolamento si applica alle strutture centrali e territoriali dell'Ente, relativamente ai trattamenti di dati personali dei quali l'Ente sia titolare, contitolare o responsabile ai sensi delle disposizioni di cui Capo IV del RGPD.

2. Il presente Regolamento costituisce, altresì, atto di indirizzo per gli Automobile Club federati e le società controllate dall'ACI ai sensi del decreto legislativo 9 agosto 2016, n. 175 (recante "Testo unico in materia di società a partecipazione pubblica"), ferma restando la necessità che ogni Automobile Club e ogni società controllata adotti un proprio regolamento in materia di protezione dei dati personali.

CAPO II - MODELLO ORGANIZZATIVO PRIVACY ACI

Art. 4
Soggetti e ruoli del Modello organizzativo Privacy ACI

1. L'ACI, considerata la complessità della propria struttura organizzativa - sia centrale che periferica - adotta, come misura organizzativa di cui all'art. 24 par 1 del RGPD, il Modello organizzativo Privacy ACI, quale particolare assetto organizzativo che definisce i ruoli cui affidare compiti e responsabilità in ordine al trattamento ed alla tutela dei dati personali dei quali l'ACI è titolare, contitolare o responsabile del trattamento ai sensi delle disposizioni del Capo IV del RGPD.

2. Il Modello organizzativo Privacy ACI, ed il relativo aggiornamento, sono definiti dal Presidente dell'Ente, tenuto conto del Regolamento di organizzazione adottato dall'ACI, ai sensi del'art. 27 del decreto legislativo 30 marzo 2001 n. 165 (di seguito, per brevità, "d. lgs. n. 165/2001"), e dell'assetto organizzativo generale dell'Ente, definito dall'Ordinamento dei Servizi. Detto modello si articola nei ruoli - individuatl ai sensi dell'art. 29 del RGPD e dell'art. 2-quaterdecies del Codice Privacy - di Titolare, di Referente, di Designato e di Autorizzato, ai quali sono attribuiti i compiti indicati nel presente Capo. Restano, fermi i ruoli di Responsabile del trattamento, di cui all'art. 28 del GDPR, e di Responsabile della protezione dei dati (di seguito, per brevità, RPD), di cui agli articoli 37 e seguenti dello stesso RGPD, nonché i ruoli definiti dalle "Politiche di sicurezza dei Sistemi e delle Informazioni" di cui al seguente art. 12.

Art. 5
Titolare del trattamento dei dati personali

1. L'ACI, quale ente pubblico non economico Titolare del trattamento dei dati personali di competenza (di seguito, per brevità "Titolare") ai sensi dell'art. 4 n. 7) del RGPD, determina, singolarmente o insieme ad altri soggetti, le finalità e i mezzi del trattamento degli stessi dati personali.

2. L'ACI, nella persona del Presidente quale legale rappresentante, ai sensi dell'art. 5 par. 2 del RGPD, è competente per il rispetto dei principi di cui al precedente art. 2, enunciati nel par. 1 dello stesso art. 5 del RGPD, ed è tenuto a comprovarlo secondo il principio di "responsabilizzazione" (*accountability*).

3. L'ACI assume il ruolo di Contitolare del trattamento, ai sensi dell'art. 26 del RGPD, quando determina in modo congiunto con uno o più titolari le finalità e i mezzi del trattamento dei dati personali. L'accordo interno tra Contitolari, previsto dallo stesso art. 26 del RGPD, stabilisce in modo trasparente le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dalla normativa applicabile.

4. Il Titolare può affidare ad una struttura centrale dell'Ente compiti di supporto tecnico e metodologico ai Referenti, di cui al seguente art. 6, per fornire approfondimenti specialistici e garantire coerenza generale nell'adempimento degli obblighi previsti dalla vigente normativa in materia di tutela dei dati personali.

Art. 6
Referente per il trattamento dei dati personali

1. Il Referente per il trattamento dei dati personali (di seguito, in breve, Referente) è nominato dal Presidente dell'Ente, o su delega di questi dal Segretario Generale, e, nell'ambito della struttura alla quale è preposto o alla quale è assegnato, assicura la puntuale osservanza delle disposizioni dettate dalla normativa sulla tutela dei dati personali.

2. Il Referente, a seguito dell'atto formale di nomina, in particolare, è tenuto a:

a. assicurare e comprovare che, nelle attività di trattamento dei dati di competenza della struttura alla quale è preposto, siano rispettati i principi di cui all'art. 5 del RGPD, in particolar modo, nel caso di trattamento delle categorie particolari di dati personali di cui agli artt. 9 e 10 dello stesso RGPD;
b. collaborare con il Titolare per l'adeguamento, ai sensi dell'art. 24 del RGPD, delle attività di trattamento dei dati alle disposizioni previste dalla normativa applicabile assicurando, nell'ambito delle attività di competenza della struttura alla quale è preposto, l'adempimento degli obblighi normativi in materia, anche per quanto concerne l'informativa agli interessati di cui agli artt. 13 e 14 del RGPD e, in generale, predisponendo tutti gli atti, i documenti e la modulistica necessaria nonché assicurandone l'adozione, la conservazione, la diffusione e l'aggiornamento;
c. assicurare e comprovare l'acquisizione del consenso da parte degli interessati, quando previsto e secondo le modalità indicate dall'art 7 del RGPD, nonché il corretto ed efficace esercizio da parte dell'Interessato del diritto di revoca del consenso medesimo;
d. assicurare il corretto ed efficace esercizio da parte dell'interessato dei diritti di cui agli articoli da 15 a 22 del RGPD nonché il puntuale riscontro nei termini e con le modalità prescritte dallo stesso RGPD e dal presente Regolamento; fornire, per le materie di competenza, le informazioni richieste dagli interessati attraverso i canali di comunicazione tradizionali e digitali dedicati dall'Ente alla specifica materia della tutela dei dati personali;
e. vigilare in maniera costante sugli eventuali trattamenti di competenza affidati a soggetti terzi, esterni all'Ente, nominati dal Titolare quali Responsabili del trattamento ai sensi dell'art. 28 del RGPD;
f. informare preventivamente il Titolare di ogni modifica che si rendesse necessario od opportuno apportare alle modalità di esecuzione dei trattamenti in essere e di ogni nuovo trattamento che dovesse essere eseguito nella struttura alla quale è preposto, anche previa verifica con il RPD, al fine di assicurare costantemente la conformità alla normativa applicabile, con particolare riferimento alle disposizioni di cui all'art. 25 del RGPD, in materia di protezione dei dati fin dalla progettazione (*privacy by design*) e di protezione per impostazione predefinita (*privacy by default*);
g. collaborare con il Titolare, per gli ambiti di propria competenza, nella predisposizione e aggiornamento del registro dei trattamenti di dati personali dell'Ente, di cui all'art. 30 del RGPD; in particolare, individuare e censire i trattamenti di dati personali di competenza della struttura alla quale è preposto;

h. predisporre misure tecniche e organizzative idonee a garantire, ai fini di cui all'art. 32 del RGPD, un livello di sicurezza adeguato al rischio, secondo quanto previsto dalla normativa applicabile nonché dalle procedure interne stabilite dall'ACI in tema di sicurezza dei dati, segnalando al Titolare eventuali specifiche esigenze;
i. coordinare e controllare, secondo le politiche definite dalla struttura centrale competente per la gestione dei sistemi informativi, la tenuta delle banche dati e degli archivi, informatici e cartacei, necessari allo svolgimento delle attività della struttura alla quale è prepostoo alla quale è assegnato;
j. informare immediatamente il Titolare e il RPD di ogni questione concernente la protezione dei dati ed, in particolare, di ogni violazione *(data breach)* di cui sia venuto a conoscenza, ed assisterli, se del caso, nelle eventuali attività di notifica al Garante e di comunicazione agli interessati, ai sensi e per gli effetti degli artt. 33 e 34 del RGPD;
k. collaborare con il Titolare nell'esecuzione delle attività connesse alla valutazione d'impatto sulla protezione dei dati personali (*Data Protection Impact* Assessment - DPIA), in relazione ai trattamenti che presentino un rischio elevato per i diritti e le libertà delle persone fisiche, secondo le previsioni dell'art. 35 del RGPD e in coerenza con le linee guida emanate dal Garante per la protezione dei dati personali di cui all'art. 153 del Codice (di seguito, per brevità, "Garante");
l. collaborare con il RPD e il Titolare in occasione di ispezioni o in caso di richieste da parte del Garante, mettendo a disposizione degli stessi tutte le informazioni necessarie per dimostrare il rispetto della normativa applicabile;
m. nominare i Designati e gli Autorizzati al trattamento, in base alla funzione ricoperta all'interno della struttura alla quale è preposto o alla quale è assegnato; in particolare il Referente deve impartire, per iscritto, ai Designati idonee istruzioni circa le modalità di esecuzione delle attività demandate e vigilare sul rispetto delle stesse, nonché informare adeguatamente i Designati e gli Autorizzati dell'obbligo di mantenere riservati i dati oggetto dei trattamenti;
n. organizzare, se ritenuti utili per i Designati ed Autorizzati della struttura alla quale è preposto o alla quale è assegnato, interventi formativi ed informativi, ulteriori rispetto a quelli organizzati ai sensi dell'art. 20 del presente Regolamento.

3. Il Referente, a seguito dell'atto formale di nomina, ha il potere di adottare qualsiasi atto necessario per l'esecuzione dei compiti attribuiti.

4. I Referenti preposti alle strutture o funzioni centrali dell'Ente possono adottare, nelle materie di rispettiva competenza a carattere trasversale, indicazioni generali per orientare il trattamento dei dati personali presso le altre strutture centrali e presso le strutture periferiche dell'Ente stesso. Dette indicazioni sono da considerare misure tecniche e organizzative predisposte dal Titolare ai sensi dell'art. 24 del RGPD.

Art. 7
Designato al trattamento dei dati personali

1. Il Designato al trattamento dei dati personali (di seguito, in breve, Designato) è nominato dal Referente preposto alla struttura centrale o periferica di competenza, o alla quale è assegnato, e, nell'ambito della stessa struttura e nei limiti delle istruzioni impartite dallo stesso Referente, lo coadiuva nell'esecuzione dei compiti indicati nel precedente art. 6.

2. Il Designato, a seguito dell'atto formale di nomina, in particolare, è tenuto a:

a. assistere il Referente per le attività relative al riscontro all'esercizio dei diritti degli interessati, di cui agli articoli da 15 a 22 del RGPD, ed alla richiesta di informazioni in materia di tutela dei dati personali;
b. mettere in atto, secondo le politiche definite dalla struttura centrale competente per la gestione dei sistemi informativi, tutte le misure tecniche e organizzative, ai fini di cui agli articoli 24 e 32 del RGPD, necessarie a prevenire i rischi connessi all'esecuzione delle attività di trattamento svolte per conto del Titolare e ad assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi con cui i trattamenti sono effettuati, avvalendosi di adeguati processi e di ogni altra misura tecnica idonea ad attuare le istruzioni fornite e dai Referenti, ivi inclusa l'adozione di:
    - procedure idonee a garantire il rispetto dei diritti e delle richieste formulate dagli Interessati al Titolare;
    - adeguate interfacce o sistemi di supporto informatici che consentano di garantire e fornire informazioni agli interessati, così come previsto dalla normativa applicabile;
    - procedure atte a garantire l'aggiornamento, la modifica e la correzione, su richiesta del Titolare, dei dati di ogni interessato;
    - procedure atte a garantire la cancellazione o il blocco dell'accesso ai dati, su richiesta del Titolare;
    - misure che consentano di contrassegnare i dati dei singoli Interessati, per consentire al Titolare di poter applicare particolari regole, quale la differenziazione dei consensi;
    - procedure atte a garantire il diritto degli interessati alla portabilità dei dati e alla limitazione di trattamento, su richiesta del Titolare;
c. collaborare con il Referente nell'aggiornamento costante e tempestivo del registro delle attività di trattamento di cui all'art. 30 del RGPD;
d. informare immediatamente il Referente e il RPD di ogni questione concernente la protezione dei dati personali, con particolare riferimento alle eventuali violazioni (*data breach*) di cui sia venuto a conoscenza, ed assisterli nelle attività di notifica al Garante e di comunicazione agli interessati, ai sensi e per gli effetti degli artt. 33 e 34 del RGPD;
e. collaborare con il Referente nell'esecuzione delle attività connesse alla valutazione d'impatto sulla protezione dei dati personali (*Data Protection Impact* Assessment - DPIA) di cui all'art. 35 del RGPD;
f. collaborare con i Referenti e con il RPD in occasione di ispezioni o in caso di richieste da parte del Garante, mettendo a loro disposizione tutte le informazioni necessarie per dimostrare il rispetto della normativa applicabile;
g. verificare che gli Autorizzati rispettino le istruzioni ricevute e mantengano riservati i dati oggetto dei trattamenti.

Art. 8
Autorizzato al trattamento dei dati personali

1. L'Autorizzato al trattamente dei dati personali (di seguito, in breve, Autorizzato) è nominato dal Referente preposto alla struttura centrale o periferica di competenza, o alla quale è assegnato, ed effettua, nell'ambito della stessa struttura, i trattamenti operativi dei dati personali sulla base e nei limiti delle istruzioni impartite dal Referente. L'autorizzato ha accesso ai soli dati la cui conoscenza sia strettamente necessaria allo svolgimento dei compiti assegnati.

2. L'Autorizzato, a seguito dell'atto formale di nomina, in particolare, è tenuto a:

a. assicurare la conformità delle attività di trattamento svolta alla normativa sulla tutela dei dati personali;
b. eseguire le attività di trattamento sulla base e nei limiti delle istruzioni ricevute;
c. assistere i Referenti e i Designati nelle attività di riscontro alle richieste per l'esercizio dei diritti degli interessati, di cui agli articoli da 15 a 22 del RGPD, ed alle richieste di informazioni in materia di tutela dei dati personali;
d. eseguire tutte le misure tecniche e organizzative, introdotte dal Referente e dal Titolare ai fini di cui all'art. 24 del RGPD, per prevenire i rischi connessi all'esecuzione delle attività di trattamento e assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi con cui i trattamenti sono effettuati, dando puntuale attuazione alle istruzioni ricevute;
e. informare immediatamente i Referenti, i Designati e il RPD di ogni questione concernente la protezione dei dati personali, ed, in particolar modo di ogni violazione di dati personali (*data breach*) di cui sia venuto a conoscenza, ed assisterli nelle eventuali attività di notifica al Garante e di comunicazione agli interessati ai sensi e per gli effetti degli artt. 33 e 34 del RGPD;
f. collaborare con i Referenti, i Designati nell'esecuzione delle attività propedeutiche alla valutazione d'impatto sulla protezione dei dati personali (*Data Protection Impact Assessment* - DPIA) di cui all'art. 35 del RGPD;
g. fornire ogni utile supporto in occasione di ispezioni o in caso di richieste da parte del Garante, mettendo a disposizione tutte le informazioni necessarie per dimostrare il rispetto della normativa applicabile.

Art. 9
Responsabile del trattamento

1. L'ACI, quale Titolare, ricorre al Responsabile di cui all'art. 28 c. 1 del RGPD, qualora ritenga che il trattamento di specifici dati personali di competenza, per la particolare finalità o tipologia del trattamento, debba essere effettuato, per conto dell'Ente stesso, da soggetti esterni che presentino adeguate garanzie per mettere in atto misure tecniche e organizzative idonee al rispetto del RGPD ed alla tutela dei diritti dell'interessato.

2. Il contratto o altro atto giuridico, stipulato tra l'ACI e il Responsabile di cui al presente articolo, deve essere conforme alle prescrizioni contenute nell'art. 28 del RGPD. Il Presidente dell'Ente può delegare ai Referenti, di cui al precedente art. 6, la predisposizione e sottoscrizione, per quanto di competenza, del contratto con lo stesso Responsabile. In ogni caso, detto Responsabile è scelto secondo i criteri di selezione e le modalità di affidamento degli incarichi o servizi previsti dalla vigente normativa applicabile alle amministrazioni pubbliche; l'esecuzione dell'incarico o servizio affidato viene periodicamente controllata dal Referente preposto alla struttura competente.

3. L'ACI può essere individuato, da altro Titolare, quale Responsabile di cui all'art. 28 c. 1 del RGDP, per il trattamento di specifici dati personali, previa stipula del contratto o altro atto giuridico di cui al precedente comma 2. Il Presidente dell'Ente può delegare ai Referenti, di cui al precedente art. 6, la predisposizione e la sottoscrizione, per quanto di competenza, del contratto stipulato dall'Ente con il Titolare.

4. Nel caso in cui l'Ente, come Titolare o Responsabile, trasmette dati personali di propria competenza ad un soggetto terzo, in qualità di incaricato o fornitore di un servizio affidato dall'Ente stesso, a detti fornitori o incaricati sono applicate le politiche di tutela dei dati personali previste nel presente Regolamento. Nel caso in cui il Referente ritenga necessario discostarsi dalle predette politiche, è tenuto, oltre che ad informare il Presidente dell'Ente, alla previa consultazione del RPD.

Art. 10
Responsabile della protezione dei dati (RPD)

1. L'ACI, quale amministrazione pubblica, è obbligato, ai sensi del'art. 37 par. 1 lett. a) del RGPD, a designare il RPD per lo svolgimento dei compiti indicati dall'art. 39 dello stesso RGPD.

2. Il RPD è designato dal Presidente dell'Ente, con apposito atto di nomina, in funzione delle qualità professionali, con particolare riferimento alla conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati nonché alla capacità di assolvere i compiti di cui all'art. 39 dello stesso RGPD. Il RPD designato deve essere un dipendente dell'Ente.

3. L'Amministrazione supporta lo svolgimento dei compiti attribuiti al RPD anche attraverso l'assegnazione, ad un'apposita struttura di supporto, di adeguate risorse finanziarie e organizzative. In ogni caso l'Ente, riconoscendo la rilevanza del ruolo affidato al RPD dalla normativa sulla tutela dei dati personali nonché la particolare incidenza dell'incarico nell'ambito della propria organizzazione, ne agevola i compiti attraverso la collaborazione di Referenti, Designati ed Autorizzati.

Art. 11
Help desk Privacy

1. L'Help desk Privacy è un gruppo di lavoro permanente interdirezionale, con funzioni di supporto ai Referenti, nominato dal Direttore della struttura di cui all'art. 5 c. 4 del presente

Regolamento e composto da risorse interne all'Ente in possesso delle competenze adeguate allo svolgimento dei compiti di cui al seguente comma 2.

2. L'Help Desk Privacy svolge, in particolare, i compiti di:

- assistere i Referenti, di cui al precedente art. 6, nell'approfondimento delle problematiche inerenti al trattamento dei dati personali, anche conseguenti all'esercizio dei diritti degli Interessati, con particolare riferimento ai temi multidisciplinari;
- contribuire a garantire omogeneità di comportamento dei Referenti rispetto alle soluzioni adottate quanto al trattamento dei dati personali da parte dell'Ente ed all'adempimento dei compiti attribuiti agli stessi Referenti, con specifico riferimento alle misure tecniche ed organizzative, da predisporre ai sensi e per gli effetti di cui all'art. 24 dello stesso RGPD, ed alla compilazione del registro dei trattamenti di cui all'art. 30 del RGPD;
- facilitare la diffusione all'interno dell'Ente di una "cultura per la privacy", anche attraverso la conoscenza delle disposizioni normative in materia nonché delle indicazioni operative formulate dal Garante italiano e del Comitato europeo per la protezione dei dati, in modo tale da garantire il costante aggiornamento dei Designati e degli Autorizzati.

3. L'Amministrazione assicura ai componenti dell'Help desk Privacy, per l'adeguato svolgimento dei compiti assegnati, i necessari strumenti logistici e informatici.

Art. 12
Ruoli in materia di sicurezza dei sistemi e delle informazioni

1. I ruoli, ed i relativi compiti, dedicati alla gestione della sicurezza delle informazioni, sono individuati nelle "Politiche di sicurezza dei Sistemi e delle Informazioni" predisposte, e periodicamente aggiornate dalla struttura centrale competente per la gestione dei sistemi informativi. Dette politiche sono da considerare misure tecniche e organizzative predisposte dal Titolare ai sensi dell'art. 24 del RGPD.

CAPO III - OBBLIGHI DEL TITOLARE E DIRITTI DELL'INTERESSATO

Art. 13
Informativa

1. L'Ente, quale Titolare, ha l'obbligo di fornire all'Interessato le informazioni di cui agli articoli 13 e 14 del RGPD, in caso di raccolta dei dati personali presso lo stesso interessato o presso altri soggetti. L'informativa deve essere fornita qualunque siano le condizioni di liceità, o basi giuridiche, del trattamento di cui all'art. 6 del RGPD.

2. Le informazioni di cui al precedente comma, ai sensi dell'art.12 del RGPD, devono avere caratteristiche di intelligibilità, accessibilità e semplicità, in particolare, nel caso in cui siano destinate specificamente ai minori. L'Ente comunica le informazioni per iscritto o in formato elettronico, anche a mezzo del sito web o di *app* istituzionali, in particolare qualora i servizi offerti siano resi in modalità *on line*. In ogni caso, sono adottate modalità di comunicazione dell'informativa in grado di tracciare la presa visione della stessa da parte dell'interessato.

Art. 14
Richiesta del consenso

1. L'ACI deve acquisire il consenso da parte dell'interessato come condizione di liceità del trattamento dei dati personali comuni, rispettando le prescrizioni di cui agli artt. 5 e 7 del RGPD, qualora non ricorrano le altre condizioni di liceità, o basi giuridiche, di cui allo art. 6 ovvero previste dal diritto interno in base alle disposizioni di cui alla Parte II del Codice privacy. Resta fermo che l'Ente, quale amministrazione pubblica di cui all'art. 1 c. 2 del d. lgs. n. 165/2001, ai sensi dell'art. 6 c. 1 lett. e) del RGDP e dell'art. 2-ter del Codice privacy è legittimato a trattare i dati personali comuni per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esso attribuiti, sempreché il compito o l'esercizio del potere siano previsti da una norma di legge o di regolamento ovvero da atti amministrativi generali.

2. Per i trattamenti delle categorie particolari di dati personali, di cui all'art. 9 par. 1 del RGPD, il consenso da parte dell'interessato è necessario qualora non ricorrano le altre condizioni previste dal par. 2 dello stesso art. 9, ovvero non ricorrano le circostanze previste dall'art. 2-sexies Codice privacy nel caso di trattamento necessario per motivi di interesse pubblico. In particolare, per il trattamento dei dati genetici, biometrici e relativi alla salute, devono essere osservate anche le misure di garanzia previste dall'art. 2-septies dello stesso Codice.

3. Per il trattamento dei dati personali relativi a condanne penali e reati, di cui all'art. 10 del RGPD, devono essere comunque rispettate le regole previste dallo stesso art. 10 ed i principi fissati dall'art. 2-octies del Codice privacy.

4. Per il trattamento di dati personali di minori, in relazione ai servizi della società dell'informazione, nell'acquisizione del consenso dello stesso minore si applicano le disposizioni di cui all'art. 8 del RGPD e dell'art. 2-quinquies del Codice privacy

5. L'interessato ha diritto di revocare il consenso, in qualsiasi momento, senza alcun condizionamento e con la stessa facilità con cui lo ha prestato (diritto di revoca di cui all'art. 7 c. 3 del RGPD);

Art.15
Esercizio dei diritti da parte dell'interessato

1. L'ACI, in qualità di Titolare, è tenuto, ai sensi dell'art. 12 del RGPD, ad agevolare l'esercizio dei seguenti diritti, riconosciuti all'interessato dagli articoli da 15 a 22 dello stesso GDPR, fornendo le comunicazioni previste dai medesimi articoli:

a. diritto ad ottenere la conferma che sia in corso un trattamento di dati che riguardano l'interessato e, in tal caso, di accesso ai dati personali ed alle informazioni indicate dall'art. 15 par. 1 del RGPD;
b. diritto ad ottenere, ai sensi dell'art. 16 del RGPD, la rettifica dei dati personali inesatti che riguardano l'interessato, senza ingiustificato ritardo, nonché ad ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa;
c. diritto ad ottenere la cancellazione dei dati personali che riguardano l'interessato (cd. diritto all'oblio), senza ingiustificato ritardo, nel rispetto delle condizioni e secondo le modalità indicate dall'art. 17 del RGPD;
d. diritto ad ottenere la limitazione (temporanea) del trattamento, al ricorrere di una delle ipotesi indicate dall'art. 18 del RGPD, secondo le modalità indicate nello stesso articolo;
e. diritto ad ottenere, ai sensi dell'art. 19 del RGPD, la comunicazione, a ciascuno dei destinatari cui sono trasmessi i dati personali dell'interessato, di eventuali rettifiche, cancellazioni o limitazioni del trattamento, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato;
f. diritto di ricevere, ai sensi dell'art. 20 del RGPD in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che riguardano l'interessato, forniti dallo stesso al Titolare, nei soli casi in cui il trattamento si basa sul consenso o su un contratto ed è effettuato con mezzi automatizzati, e diritto a trasmettere i medesimi dati ad un altro Titolare senza impedimenti (cd. portabilità dei dati); qualora tecnicamente possibile, il diritto alla portabilità dei dati comprende anche il diritto di ottenere la trasmissione diretta dei dati personali da un Titolare del trattamento all'altro Titolare;
g. diritto di opporsi, alle condizioni e nel rispetto dei limiti previsti dall'art. 21 del RGPD, al trattamento dei dati personali che riguardano l'interessato; in caso di opposizione, il Titolare si deve astenere dal trattare ulteriormente i dati salvo che dimostri l'esistenza di motivi legittimi oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, secondo le previsioni di cui allo stesso art. 21;
h. diritto a non essere sottoposto, ai sensi dell'art. 22 del RGPD, a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che riguardano l'interessato o che incida in modo analogo significativamente sulla sua persona, salvo quanto previsto dallo stesso art. 22.

2. La struttura centrale di cui all'art. 5 c. 4 del presente Regolamento, d'intesa con la struttura competente per la gestione dei sistemi informativi, e consultato il RPD, predispone le indicazioni operative utili per assicurare omogeneità procedurale nella ricezione delle richieste relative all'esercizio dei diritti di cui al precedente comma 1 e nel riscontro all'interessato.

3. I diritti, di cui al precedente comma 1, riferiti ai dati personali concernenti persone decedute, ai sensi dell'art. 2-terdecies del Codice privacy, possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario o per ragioni familiari meritevoli di protezione.

Art. 16
Responsabilità del Titolare, misure tecniche ed organizzative adeguate e sicurezza del trattamento

1. L'ACI, quale Titolare, ai sensi e per gli effetti dell'art. 24 par. 1 del RGPD, ha la responsabilità di individuare e porre in essere nonché, se necessario, di aggiornare le misure tecniche ed organizzative adeguate per garantire che il trattamento dei dati di competenza sia effettuato conformemente allo stesso RGDP (principi di *accountability* e di *compliance* alla normativa sulla tutela dei dati personali) e deve essere in grado di dimostrare il rispetto dei predetti principi.

2. L'ACI, quale Titolare, nell'individuazione ed applicazione delle misure di cui al precedente comma, osserva le disposizioni, di cui all'art. 25 par. 1 e 2 del RGPD, relative alla protezione dei dati fin dalla progettazione (*privacy by design*) ed alla protezione per impostazione predefinita (*privacy by default*).

3. L'ACI, quale Titolare o quale Responsabile di cui all'art. 9 del presente Regolamento, deve individuare e porre in essere misure tecniche ed organizzative tali da garantire, ai sensi dell'art. 32 del RGPD, un livello di sicurezza adeguato al rischio. La struttura centrale competente per la gestione dei sistemi informativi assicura al Titolare il necessario supporto per conformarsi a detta disposizione, fermi restando i compiti attribuiti a Referenti, Designati ed Autorizzati ai sensi degli articoli 6, 7 e 8 del presente Regolamento.

4. L'adesione ai codici di condotta, di cui all'art. 40 del RGPD, o a un meccanismo di certificazione di cui all'art. 42 dello stesso RGPD può essere utilizzata dall'Ente per dimostrare il rispetto dei principi e delle disposizioni di cui ai precedenti commi del presente articolo.

Art. 17
Registro delle attività di trattamento

1. L'ACI, ai sensi e per gli effetti dell'art. 30 c. 1 del RGPD, predispone e tiene aggiornato il registro delle attività di trattamento (di seguito, per brevità, "Registro") svolte sotto la propria responsabilità, in qualità di Titolare. Qualora l'ACI rivesta il ruolo di Responsabile del trattamento, di cui all'art. 9 c. 3 del presente Regolamento, deve tenere, ai sensi e per gli effetti dell'art. 30 c. 2 del RGPD, un registro di tutte le categorie di attività relative al trattamento svolte per conto di un altro Titolare.

2. La struttura centrale competente per la gestione dei sistemi informativi fornisce il necessario supporto per garantire l'adeguata tenuta, in modalità elettronica, dei registri di cui al precedente comma 1, fermi restando i compiti attribuiti a Referenti, Designati ed Autorizzati, ai sensi degli articoli 6, 7 e 8 del presente Regolamento, per quanto attiene al trattamento dei dati personali effettuati nell'ambito delle attività di competenza della struttura di riferimento.

3. La struttura centrale di cui all'art. 5 c. 4 del presente Regolamento, d'intesa con la struttura competente per la gestione dei sistemi informativi, e consultato il RPD, predispone le indicazioni operative utili per assicurare l'omogenea compilazione del Registro.

Art. 18
Valutazione d'impatto sulla protezione dei dati personali (*Data Protection Impact Assessment* - DPIA)

1. L'ACI, quale Titolare, ai sensi dell'art 35 del RGPD è tenuto ad effettuare la valutazione di impatto dei trattamenti previsti sulla protezione dei dati nei casi in cui, in presenza delle circostanze indicate dallo stesso art. 35, un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Se necessario, quantomeno quando insorgano variazioni del rischio rappresentato dalle attività relative al trattamento, il Titolare procede ad un riesame per verificare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati.

2. L'ACI è tenuto, ai sensi dell'art. 36 del RGPD, a consultare il Garante prima di procedere al trattamento, qualora la valutazione di impatto sulla protezione dei dati, di cui al comma precedente, indichi che il trattamento può presentare un rischio elevato in assenza di misure adottate dal Titolare per attenuare il rischio.

3. La struttura centrale competente per la gestione dei sistemi informativi fornisce il necessario supporto informatico e tecnologico per effettuare la valutazione d'impatto di cui al comma 1, fermi restando i compiti attribuiti a Referenti, Designati ed Autorizzati, ai sensi degli articoli 6, 7 e 8 del presente Regolamento, per quanto attiene al processo di valutazione d'impatto per i trattamenti di competenza della struttura di riferimento.

4. La struttura centrale di cui all'art. 5 c. 4 del presente Regolamento, d'intesa con la struttura competente per la gestione dei sistemi informativi, e consultato il RPD, predispone le indicazioni operative utili per assicurare omogeneità procedurale nella valutazione di impatto dei trattamenti di cui l'Ente è Titolare.

Art. 19
Notifica e comunicazione in caso di violazione dei dati personali (*data breach*)

1. L'ACI, quale Titolare, in caso di violazione dei dati personali, è tenuto a darne notifica al Garante, ai sensi e per gli effetti dell'art. 33 del RGPD, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento della conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e libertà delle persone fisiche cui

i dati violati si riferiscono. Qualora la notifica non sia effettuata entro le 72 ore dalla conoscenza, deve essere corredata dei motivi del ritardo.

2. L'ACI è tenuto a comunicare anche all'interessato, ai sensi e per gli effetti dell'art. 34 del RGPD, la violazione, di cui al precedente comma 1, quando la stessa è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Detta comunicazione non è richiesta se sussistono le condizioni indicate nel par. 3 dello stesso art. 34.

3. L'ACI, quale Responsabile di cui all'art. 9 c. 3 del presente Regolamento, è tenuto ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

4. La struttura centrale di cui all'art. 5 c. 4 del presente Regolamento, d'intesa con la struttura competente per la gestione dei sistemi informativi, e consultato il RPD, predispone le indicazioni operative utili per assicurare omogeneità procedurale alla rilevazione della violazione dei dati personali ed alla conseguente notifica e comunicazione, di cui ai precedenti commi 1 e 2, anche al fine di garantire la certezza del momento iniziale della conoscenza, la tempestività delle trasmissioni e l'acquisizione della documentazione prevista dall'art. 33 par. 5 del RGPD. Restano fermi i compiti attribuiti a Referenti, Designati ed Autorizzati, ai sensi degli articoli 6, 7 e 8 del presente Regolamento, per quanto attiene al processo di rilevazione della violazione dei dati personali relativamente ai trattamenti di competenza della struttura di riferimento.

Art. 20
Formazione

1. L'ACI, in qualità di Titolare, ai sensi dell'art. 39 par. 1 lett. b) del RGPD, è tenuto ad organizzare interventi formativi ed informativi specifici in materia di trattamento e protezione dei dati personali, rivolti al personale che partecipa ai trattamenti ed alle connesse attività di controllo. Detti interventi formativi ed informativi sono da considerare misure organizzative predisposte dal Titolare ai sensi dell'art. 24 del RGPD e danno, altresì, attuazione alla prescrizione di cui all'art. 32 c. 4 dello stesso RGDP, in base alla quale il personale che ha accesso a dati personali può trattarli solo se è a tal fine istruito dal Titolare.

2. L'ACI, in particolare, riconosce l'importanza di promuovere la cultura della protezione delle persone fisiche riguardo al trattamento dei dati personali e, a tal fine, avvalendosi della struttura centrale competente per la gestione delle risorse umane e consultato il RPD, organizza specifiche iniziative di formazione e aggiornamento rivolte ai Referenti, Designati ed Autorizzati, di cui agli articoli 6, 7 e 8 del presente Regolamento, nonché, eventualmente, a particolari categorie di soggetti esterni, quali i Responsabili del trattamento di cui all'art. 9 del presente Regolamento, che siano autorizzati al trattamento di dati personali per conto dello stesso Titolare. L'Ente organizza, inoltre, specifiche attività di formazione per i componenti del gruppo Help desk privacy di cui all'art. 11 del presente Regolamento.

3. Resta ferma la possibilità di azioni formative ed informative sussidiarie, organizzate dai Referenti, ai sensi dell'art. 6 c. 2 lett. n del presente Regolamento, per il personale assegnato alle rispettive strutture.