Automobile Club d'Italia

DELIBERAZIONE N. 79 60 DEL 2 APRILE 2019

IL PRESIDENTE

VISTO 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 e che abroga la direttiva 95/46/CE"* (GDPR – *General Data Protection Regulation*);

VISTO il Decreto Legislativo 10 agosto 2018, n.101 recante *"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679"* che ha modificato il Decreto Legislativo 30 giugno 2003, n.196 *"Codice in materia di protezione dei Dati personali";*

TENUTO CONTO che l'Ente, nell'assolvimento della propria missione istituzionale e nell'esecuzione dei servizi svolti per delega dello Stato e di altre Amministrazioni, esegue, in qualità di Titolare, trattamenti di Dati personali relativi alle persone fisiche;

RILEVATO che il citato Regolamento (UE) 679/2016 impone alle Organizzazioni pubbliche la necessità di un costante e capillare presidio dei processi di gestione dei Dati personali al fine di assicurare la tutela degli interessati non solo attraverso il puntuale rispetto delle previsioni normative, ma anche con l'adozione di interventi sulle strutture organizzative, volti al rafforzamento della cultura della tutela del trattamento e della libera circolazione dei Dati;

CONSIDERATO altresì che il Titolare del trattamento è tenuto all'adozione di politiche interne atte a garantire livelli di sicurezza adeguati ai rischi attraverso l'implementazione di specifiche misure tecniche e organizzative, al fine di mitigare l'impatto del trattamento sugli Interessati e assicurare la migliore applicazione della norma;

PRESO ATTO della necessità di assicurare, in ossequio al principio di responsabilizzazione (*accountability*), la conformità dei trattamenti alle disposizioni dettate dal citato Regolamento, dal Decreto Legislativo n. 196/2003 e s.m.i., nonché da ogni ulteriore norma a livello nazionale o sovranazionale, ivi compresi i provvedimenti adottati dal Garante per la protezione dei Dati personali;

VISTO l'articolo 2-quaterdecies del predetto Decreto Legislativo 101/2018 con specifico riferimento alla previsione che il "Titolare o il Responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di Dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità e che il Titolare o il Responsabile del trattamento individuino le modalità più opportune per autorizzare al trattamento dei Dati personali le persone che operano sotto la propria autorità";

CONSIDERATA la complessità della struttura organizzativa dell'Ente che si articola nelle Direzioni Centrali ed assicura il presidio dell'intero territorio nazionale con le Direzioni Compartimentali, le Aree Metropolitane, le Direzioni Territoriali e le Unità Territoriali;

RITENUTO opportuno delineare, nell'ambito del "Sistema Privacy ACI", un "Organigramma Privacy" articolato in diversi ruoli cui assegnare l'incarico di dare dimostrazione *per acta* che, nelle attività di trattamento dei Dati di competenza, siano rispettate le disposizioni previste dalla normativa applicabile in materia di Privacy;

ATTESA la propria competenza in qualità di Titolare del trattamento ai sensi dell'art. 24 del Regolamento (UE) 679/2016;

VISTO lo Statuto dell'ACI;

PRESO ATTO delle disposizioni dettate dal Codice di comportamento di Ente;

VISTO il Regolamento di attuazione del sistema ACI di prevenzione della corruzione;

INFORMATO il Responsabile della protezione dei Dati dell'Ente (DPO);

DELIBERA

di adottare ai sensi dell'articolo 2-quaterdecies del Decreto Legislativo 10 agosto 2018, n.101 l'Organigramma Privacy dell'Automobile Club d'Italia, definito nei documenti:

- *"Organigramma Privacy dell'Automobile Club d'Italia"*;
- *"Compiti e responsabilità correlati agli incarichi previsti nel Sistema Privacy dell'Automobile Club d'Italia"*

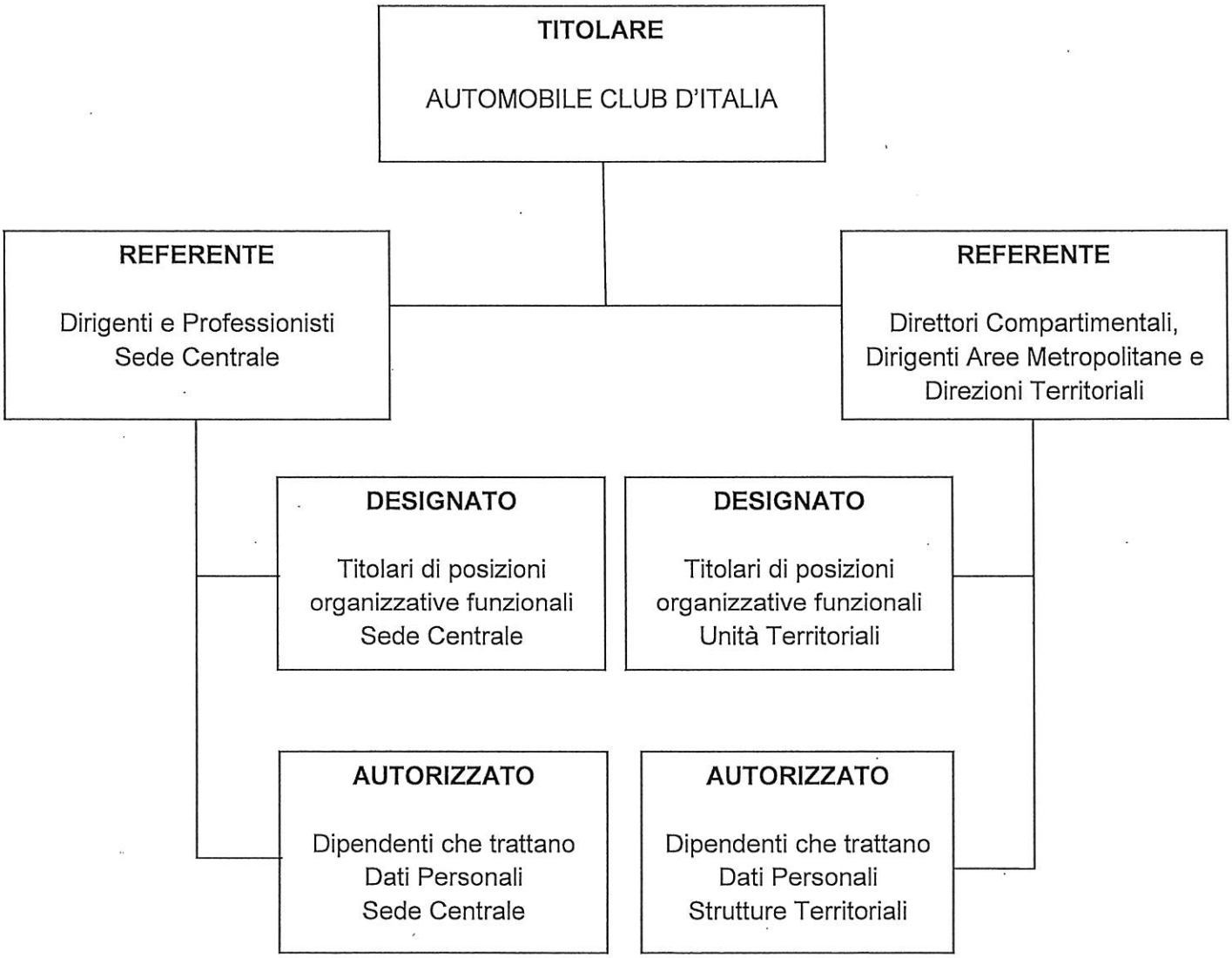
allegati n. 1) e n. 2) alla presente deliberazione di cui costituiscono parte integrante e sostanziale.

F.to

IL PRESIDENTE
(Angelo Sticchi Damiani)

Automobile Club d'Italia

ORGANIGRAMMA PRIVACY
DELL'AUTOMOBILE CLUB D'ITALIA



COMPITI E RESPONSABILITÀ CORRELATI AGLI INCARICHI PREVISTI NEL SISTEMA PRIVACY DELL'AUTOMOBILE CLUB D'ITALIA

Il presente documento illustra i compiti, gli obblighi e le responsabilità connessi agli incarichi di Referente del trattamento, Designato al trattamento e Autorizzato al trattamento dei Dati personali.

Il Referente del trattamento dei Dati personali

Sono destinatari dell'incarico di Referente del trattamento dei Dati (di seguito "***Referente***"):

- i Direttori delle Direzioni centrali e dei Servizi,
- i Dirigenti degli Uffici centrali e i Professionisti delle Aree
- i Direttori Compartimentali,
- i Dirigenti delle Aree Metropolitane e delle Direzioni territoriali;

Il Referente ha il compito di assicurare, nell'ambito della propria struttura, la puntuale osservanza delle disposizioni dettate in materia di *Privacy* dalla normativa applicabile nonché delle funzioni attribuite dal Titolare del trattamento. Il Referente ha il potere di compiere qualsiasi atto e sottoscrivere qualsiasi documento necessari per adempiere ai propri doveri.

Compiti del Referente

Il Referente effettua i trattamenti di Dati personali sulla base e nei limiti delle istruzioni ricevute dal Titolare del trattamento con la relativa nomina, in ogni caso, in conformità alla Normativa Applicabile in materia di protezione dei Dati personali garantendo la tutela dei diritti degli Interessati.

In particolare, il Referente deve:

1. individuare e censire i trattamenti di Dati personali di competenza della Direzione/Servizio/Ufficio/Area cui è preposto, nonché coordinare e controllare la gestione delle banche dati e degli archivi, informatici e cartacei, necessari allo svolgimento delle attività della struttura;

2. 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 GDPR e in coerenza con le linee guida emanate dall'Autorità di controllo;

3. assicurare e comprovare che nelle attività di trattamento dei Dati di competenza della Direzione/Servizio/Ufficio/Area cui è preposto siano rispettati i principi di cui all'art. 5 del GDPR e in particolare la liceità, correttezza e trasparenza, la limitazione delle finalità, la minimizzazione dei dati, l'esattezza, la limitazione della conservazione, l'integrità e la riservatezza, in particolar modo nel caso di trattamento delle categorie particolari di dati personali degli artt. 9 e 10 del GDPR;

4. predisporre misure tecnico/organizzative idonee a garantire un livello di sicurezza adeguato al rischio secondo quanto previsto dalla normativa applicabile nonché dalle procedure interne stabilite da A.C.I. in tema di sicurezza dei Dati, segnalando al Titolare eventuali esigenze;

5. collaborare con il Titolare per l'adeguamento delle attività di trattamento dei Dati alle disposizioni previste dalla Normativa Applicabile, assicurando nell'ambito delle attività di competenza della Direzione/Servizio/Ufficio/Area cui è preposto, l'adempimento degli obblighi normativi in materia anche per quanto concerne l'informativa agli interessati (artt. 13 e 14 del GDPR) e, in generale, predisponendo tutti gli atti, i documenti e la modulistica necessaria, assicurandone l'adozione, la conservazione, la diffusione e l'aggiornamento;

6. assicurare e comprovare l'acquisizione del consenso da parte degli Interessati quando previsto e secondo le modalità indicate dall'art 7 del GDPR, nonché il corretto ed efficace esercizio da parte dell'Interessato del diritto di revoca del consenso medesimo;

7. assicurare il corretto ed efficace esercizio da parte dell'Interessato dei diritti di cui agli artt. da 15 a 22 del GDPR e in particolare: a) accesso; b) rettifica; c) cancellazione; d) limitazione del trattamento; e) portabilità; f) opposizione al trattamento; g) non sottoposizione a processi decisionali automatizzati, compresa la profilazione;

8. 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 Direzione/Servizio/Ufficio/Area cui è preposto, anche previa verifica con il D.P.O., al fine di assicurare costantemente la conformità alla Normativa

Applicabile ai sensi dell'art. 25 del GDPR (es. *Privacy by Design, Privacy by Default*);

9. vigilare in maniera costante sugli eventuali trattamenti di competenza affidati a Soggetti terzi, esterni all'organizzazione del Titolare, nominati dal Titolare stesso Responsabili "esterni" del Trattamento ai sensi dell'art. 28 del GDPR;

10. collaborare con il Titolare per gli ambiti di propria competenza nella predisposizione e aggiornamento del Registro dei trattamenti di Dati personali del Titolare (art. 30 GDPR);

11. informare immediatamente il Titolare e il DPO di ogni questione concernente la protezione dei Dati ed in particolar modo di ogni violazione (*data breach*) di cui sia venuto a conoscenza, assistendoli, se del caso, nell'esecuzione delle attività di notifica al Garante per la protezione dei dati personali e di comunicazione agli interessati, che dovessero eventualmente rendersi necessarie;

12. collaborare con il DPO e il Titolare in occasione di ispezioni o in caso di richieste da parte del Garante per la protezione dei dati personali, mettendo a disposizione degli stessi tutte le informazioni necessarie per dimostrare il rispetto della Normativa Applicabile;

13. nominare i Designati al trattamento (di seguito, i "***Designati***") e gli Autorizzati al trattamento (di seguito, gli "***Autorizzati***"), in base alla funzione ricoperta all'interno della struttura organizzativa di competenza. In particolare deve:

    - impartire, per iscritto, ai Designati idonee istruzioni circa le modalità di esecuzione delle attività demandate e vigilare sul rispetto delle stesse;
    - informare adeguatamente i Designati e gli Autorizzati dell'obbligo di mantenere riservati i Dati oggetto dei trattamenti;
    - attuare, d'intesa con il DPO, idonee azioni di informazione e formazione dei Designati e degli Autorizzati.

Il Designato al trattamento dei Dati personali

Sono destinatari dell'incarico di Designato al trattamento dei Dati (di seguito ***"Designato"***):

- i titolari di posizione organizzativa funzionale della Sede Centrale
- i titolari di posizione organizzativa di Responsabile di Unità Territoriale di livello non dirigenziale
- i titolari di posizione organizzativa di Vicario delle Unità Territoriali di livello dirigenziale;

Compiti del Designato

Il Designato effettua i trattamenti dei Dati personali sulla base e nei limiti delle istruzioni impartite dal Referente, in conformità alla Normativa Applicabile in materia di protezione dei Dati personali e garantendo la tutela dei diritti degli Interessati.

In particolare, il Designato deve:

1. collaborare con il Referente nell'aggiornamento costante e tempestivo del Registro delle attività di trattamento del Titolare (art. 30 GDPR);

2. collaborare con il Referente 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 GDPR e in coerenza con le linee guida progressivamente emanate dall'Autorità di controllo;

3. mettere in atto tutte le misure tecniche e organizzative 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 dal Titolare e dai Referenti, ivi incluso l'adozione di:

    a. procedure idonee a garantire il rispetto dei diritti e delle richieste formulate al Titolare dagli Interessati relativamente ai loro Dati;

    b. adeguate interfacce o sistemi di supporto informatici che consentano di garantire e fornire informazioni agli Interessati così come previsto dalla normativa applicabile;

    c. procedure atte a garantire l'aggiornamento, la modifica e la correzione, su richiesta del Titolare, dei Dati di ogni Interessato;

d. procedure atte a garantire la cancellazione o il blocco dell'accesso ai Dati, su richiesta del Titolare;

e. misure che consentano di contrassegnare i Dati dei singoli Interessati, per consentire al Titolare di poter applicare particolari regole come ad esempio, la differenziazione dei consensi;

f. procedure atte a garantire il diritto degli Interessati alla portabilità dei dati e alla limitazione di trattamento, su richiesta del Titolare;

4. informare immediatamente il Referente e/o il Titolare e il DPO di ogni questione concernente la protezione dei Dati personali ed in particolar modo di ogni violazione (*data breach*) di cui sia venuto a conoscenza assistendoli, se del caso, nell'esecuzione delle attività di notifica al Garante per la protezione dei dati personali e di comunicazione agli Interessati, che dovessero eventualmente rendersi necessarie;

5. verificare che i gli Autorizzati al trattamento rispettino le istruzioni ricevute e mantengano riservati i Dati oggetto dei trattamenti;

6. assistere il Referente per le attività relative al riscontro di richieste di l'esercizio dei diritti degli Interessati come previsto, dagli artt. da 15 a 22 del GDPR e in particolare: a) – accesso; b) – rettifica; c) - cancellazione ; d) - limitazione del trattamento; e) – portabilità; f) - opposizione al trattamento: g) – di non essere sottoposto a processi decisionali automatizzati, compresa la profilazione, anche in base alle indicazioni fornite dal DPO;

7. collaborare con i Referenti e con il DPO in occasione di ispezioni o in caso di richieste da parte del Garante per la protezione dei dati personali, mettendo a loro disposizione tutte le informazioni necessarie per dimostrare il rispetto della normativa applicabile;

L'Autorizzato al trattamento dei Dati personali

Sono destinatari dell'incarico di Autorizzato al trattamento dei Dati (di seguito ***"Autorizzato"***) i dipendenti che effettuano il trattamento operativo di Dati personali nel rispetto della Normativa Applicabile in materia di protezione dei Dati personali e delle istruzioni ricevute garantendo la tutela dei diritti degli Interessati

Compiti dell'Autorizzato

In particolare, l'Autorizzato deve:

1. assicurare la conformità delle attività di trattamento alla Normativa Applicabile;

2. eseguire le attività di trattamento sulla base e nei limiti delle istruzioni ricevute;

3. informare immediatamente i Referenti, i Designati e il DPO 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 assistendoli, se del caso, nell'esecuzione delle attività di notifica al Garante per la protezione dei dati personali e di comunicazione agli interessati, che dovessero eventualmente rendersi necessarie;

4. eseguire tutte le misure tecniche e organizzative introdotte dal Referente e dal Titolare 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;

5. assistere i Referenti e i Designati nelle attività di riscontro alle richieste per l'esercizio dei diritti degli interessati previsti dalla Normativa Applicabile, anche in base alle indicazioni fornite dal DPO;

6. collaborare con i Referenti, i Designati e con il DPO nell'esecuzione delle attività propedeutiche alla valutazione d'impatto sulla protezione dei Dati personali (*Data Protection Impact Assessment*) in relazione ai trattamenti che presentino un rischio elevato per i diritti e le libertà delle persone fisiche;

7. fornire ogni utile supporto in occasione di ispezioni o in caso di richieste da parte del Garante per la protezione dei dati personali, mettendo a disposizione tutte le informazioni necessarie per dimostrare il rispetto della Normativa Applicabile.