Autorità di Regolazione dei Trasporti

Delibera n.78/2020

Misure organizzative e conferimento di compiti e funzioni del titolare del trattamento dei dati, ai sensi del Regolamento (UE) 2016/679 e delle relative norme di adeguamento dell'ordinamento nazionale.

L'Autorità, nella sua riunione del 26 marzo 2020

VISTO l'articolo 37 del decreto-legge 6 dicembre 2011, n. 201, convertito, con modificazioni, dalla legge 22 dicembre 2011, n. 214, che ha istituito, nell'ambito delle attività di regolazione dei servizi di pubblica utilità di cui alla legge 14 novembre 1995, n. 481, l'Autorità di regolazione dei trasporti (di seguito: Autorità);

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (di seguito: "Regolamento"), 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);

VISTO il decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" modificato, da ultimo, dal decreto legislativo 10 agosto 2018, n. 101, recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del suddetto "Regolamento" (di seguito: "Codice");

TENUTO CONTO che, il "Regolamento", all'articolo 4, paragrafo 1, n. 7, individua il "Titolare del trattamento" come *"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*" e che, nel caso di specie, tale qualifica è rivestita dall'Autorità, unitariamente considerata, quale organismo istituzionale che si identifica nel Consiglio (di seguito anche "Titolare");

VISTI l'articolo 4, paragrafo 1, n. 10, del "Regolamento", il quale prevede che l'accesso e il trattamento di dati personali è consentito anche a *"persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile"* e l'articolo 2-*quaterdecies*, comma 2, del "Codice", secondo cui "*Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.*";

VISTO l'articolo 2-*quaterdecies*, comma 1, del "Codice", il quale dispone 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";*

VISTI gli articoli 29 e 32, paragrafo 4, del **"**Regolamento", secondo cui il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, non può trattare dati personali *"se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri";*

VISTI l'articolo 24, paragrafo 1, del "Regolamento", secondo il quale "*Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario*" e l'articolo 32, paragrafo 1, dello stesso "Regolamento", ai sensi del quale, *"Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento*";

CONSIDERATO che il "Regolamento", nel disciplinare *ex novo* l'intera materia del trattamento dei dati personali e della tutela dei diritti riconosciuti agli interessati, rimette a ciascun titolare, e nella specie al Consiglio, la determinazione di misure in grado di assicurare che il trattamento stesso avvenga conformemente alle regole e ai principi fissati dalla nuova normativa;

CONSIDERATO che, a tal fine, occorre procedere, fra l'altro, ai seguenti adempimenti:

- attribuzione, nell'ambito del complessivo sistema di trattamento e protezione dei dati, di specifici compiti e funzioni a soggetti espressamente designati, che operano sotto l'autorità del Titolare (art. 2-*quaterdecies*, comma 1, del "Codice");
- autorizzazione al trattamento dei dati del personale e dei collaboratori dell'Autorità, in connessione con l'esercizio delle competenze assegnate a ciascuna struttura secondo il vigente ordinamento dell'Autorità (art. 2-*quaterdecies*, comma 2, del "Codice" e art. 4, par. 1, n. 10, del "Regolamento");
- definizione delle principali istruzioni cui devono attenersi tutti i soggetti comunque autorizzati al trattamento dei dati personali (artt. 29 e 32, par. 4, del "Regolamento");

VISTO il Regolamento concernente l'organizzazione e il funzionamento dell'Autorità, approvato con delibera n. 61/2016 del 23 maggio 2016 e successive modificazioni (di seguito: "ROF");

VISTA la delibera n. 35/2020 del 12 febbraio 2020, con la quale è stato designato l'attuale Responsabile della protezione dei dati personali per l'Autorità (di seguito: RPD), ai sensi dell'articolo 37 del "Regolamento";

TENUTO CONTO che, nell'ambito di tale designazione, l'Autorità ha ritenuto che la delibera n. 137/2019, adottata in data 24 ottobre 2019, con la quale sono stati attribuiti specifici compiti e funzioni connessi al trattamento di dati personali di cui al "Regolamento", "*possa beneficiare dell'individuazione di differenti misure di sicurezza tecniche e organizzative*" affidando, per le anzidette finalità, al Responsabile della protezione dei dati personali "*l'elaborazione della proposta di revisione dei contenuti della delibera n. 137/2019 da sottoporre all'Autorità entro il 31 marzo 2020*";

VISTA la relazione presentata, a tal fine, dal RPD, e il documento ad essa allegato, relativo alle "*Misure organizzative e conferimento di compiti e funzioni, ai sensi del regolamento (UE) 2016/679 e delle relative norme di adeguamento dell'ordinamento nazionale"*;

TENUTO CONTO delle proposte ivi formulate, e in particolare, che:

1. ai fini dell'attribuzione a soggetti designati di specifici compiti e funzioni del "Titolare" connessi al trattamento di dati personali, ai sensi dell'articolo 2-*quaterdecies*, comma 1, del "Codice", e tenuto conto del vigente assetto organizzativo dell'Autorità, siano individuati i seguenti soggetti e i rispettivi compiti:

   I. il *Segretario generale* che, nell'ambito delle proprie funzioni, come declinate dal "ROF",

      - coordina l'attività degli Uffici e vigila sul corretto adempimento degli obblighi in materia di trattamento dei dati personali e adotta i provvedimenti volti a dare attuazione concreta alle misure organizzative e tecniche approvate dal Consiglio anche con riferimento alle materie oggetto della presente delibera;
      - previa dettagliata informativa al Titolare del trattamento e al RPD, notifica al Garante per la protezione dei dati personali le eventuali violazioni dei dati personali;
      - approva le specifiche attività di aggiornamento e formazione del personale in materia di tutela dei dati personali, proposte del Responsabile dell'Ufficio Affari generali, amministrazione e personale d'intesa con il RPD;

   II. il *Referente privacy* - incarico attribuito al Responsabile dell'Ufficio *Information and Communication Technology* - quale nuova figura che,

      – collabora con il Segretario generale nell'esercizio delle funzioni di vigilanza e coordinamento delle attività dei soggetti autorizzati al trattamento dei dati personali, anche al fine di garantire l'uniforme applicazione delle misure tecniche e organizzative adottate dal Consiglio;

- acquisisce le informazioni necessarie per l'aggiornamento del "Registro delle attività di trattamento dei dati personali" e del "Registro delle richieste di esercizio dei diritti degli interessati" e le trasmette al RPD, per l'annotazione nei relativi registri, tenuti dallo stesso RPD;
- verifica eventuali esigenze di aggiornamento degli ordini di servizio e degli altri atti di autorizzazione al trattamento dei dati personali;
- acquisisce gli elementi informativi utili a valutare la necessità di notifica dei *data breach* al Garante ed agli interessati e collabora con il Segretario generale nei conseguenti adempimenti;

III. il *Responsabile dell'Ufficio* Information *and Communication Technology* (ICT), quale figura dirigenziale di riferimento in materia di trattamento dei dati personali, preposto altresì alla realizzazione e alla gestione dell'architettura informatica dell'Autorità e del sito web, che,

- verifica l'adeguatezza dei sistemi informativi in uso presso l'Autorità alle esigenze di garanzia e di sicurezza di cui al Regolamento, e, se necessario, si attiva per conformarli a quanto ivi previsto;
- sulla base del "Registro delle attività di trattamento dei dati personali", predispone, sentito il RPD, l'analisi dei rischi per i diritti e le libertà degli interessati prevista dall'art. 35 del Regolamento e, ove ne ricorrano i presupposti, la valutazione dell'impatto dei trattamenti, di cui al successivo art. 36;
- in materia di *whistleblowing*, rende disponibile la procedura informatica di raccolta delle segnalazioni, assicurando la riservatezza dei dati personali del segnalante;
- Individua il personale con mansioni di manutenzione e conduzione applicativa del sistema (Amministratori di sistema);

IV. il *Responsabile dell'Ufficio Affari generali, amministrazione e personale*, che, nell'ambito delle proprie funzioni,

- d'intesa con il RPD, programma e organizza le specifiche attività di aggiornamento e formazione del personale in materia di tutela dei dati personali, previa approvazione del Segretario generale;
- quale soggetto preposto alla sottoscrizione dei contratti, individua gli elementi di esperienza e affidabilità di cui all'art. 28, par. 1, del Regolamento, assicura che i contratti o gli altri atti giuridici che disciplinano i rapporti con i Responsabili del Trattamento dei dati siano conformi a quanto previsto dall'art. 28 del Regolamento e che contengano misure specifiche in merito alla scelta tra cancellazione, oppure restituzione di tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e contestuale cancellazione delle copie esistenti;

- verifica il rispetto delle regole definite contrattualmente con il Responsabile esterno, onde assicurare il corretto trattamento dei dati, secondo quanto previsto dal Regolamento;

V. il *Responsabile della prevenzione della corruzione e della trasparenza*, che, nell'ambito delle proprie funzioni,

- cura il rispetto della normativa in materia di tutela dei dati personali nell'adempimento degli obblighi di pubblicazione nella sezione "amministrazione trasparente" del sito web dell'Autorità;
- in tema di whistleblowing, in collaborazione con il Responsabile dell'Ufficio ICT, adotta e/o promuove le misure necessarie a garantire l'anonimato del segnalante, assicurando la conservazione anonima delle segnalazioni;

VI. il *Responsabile della conservazione documentale* che, quale soggetto cui è demandata la definizione e l'attuazione delle politiche del sistema di conservazione dei documenti dell'Autorità,

- predispone il "Manuale della conservazione" nel quale introduce, tra le altre: idonee misure utili alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione; l'indicazione dei tempi entro i quali le diverse tipologie di documenti devono essere scartate ovvero trasferite in conservazione; le modalità dei processi per lo scarto alla scadenza dei termini di conservazione previsti e per la produzione di duplicati informatici o di copie informatiche effettuati su richiesta degli interessati;
- verifica, nell'affidamento del processo di conservazione ad un soggetto esterno, che quest'ultimo si conformi a quanto previsto dal "Manuale di conservazione";
- d'intesa con il Responsabile dell'Ufficio ICT - e, ove presente, con il soggetto esterno cui è eventualmente affidata la conservazione dei documenti dell'Autorità - garantisce la conformità del processo di conservazione alla normativa vigente in materia di trattamento dei dati personali, verificando periodicamente l'integrità degli archivi e adottando le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;

VII. *gli Amministratori di sistema*, quali soggetti preposti alla manutenzione e alla conduzione applicativa del sistema hardware e software dell'Autorità, che, tra l'altro,

- provvedono, su indicazione del Responsabile dell'Ufficio ICT, all'attivazione e alla gestione del "profilo di autorizzazione" per l'accesso dei dipendenti e dei collaboratori dell'Autorità al protocollo informatico, al sistema di gestione documentale e alle cartelle condivise in rete, istruendo le persone autorizzate in merito alle

cautele da adottare per assicurare la segretezza e la custodia delle credenziali;
- implementano i sistemi di sicurezza del *networking* e definiscono le procedure di autenticazione alla rete e di autorizzazione all'accesso ai dati da parte gli utenti;
- ove sussistano particolari esigenze di riservatezza, verificano che sia applicata la protezione crittografica in aree di lavoro con accesso riservato e controllato;
- assicurano e gestiscono sistemi di salvataggio e di ripristino dei dati anche automatici, nonché approntano adeguate misure e/o sistemi software di salvaguardia per la protezione dei dati personali;
- curano quanto necessario per la progettazione di soluzioni applicative che tengano conto delle disposizioni in materia di *data retention* contenute nel "Manuale della conservazione", con l'obiettivo di assicurare che i "profili di autorizzazione" siano coerenti nel tempo e nei contenuti con i trattamenti formalmente autorizzati e con le connesse esigenze di cancellazione;

2. ai fini dell'autorizzazione al trattamento dei dati, ai sensi dell'articolo 2-*quaterdecies*, comma 2, del "Codice" e dell'articolo 4, par. 1, n. 10, del "Regolamento", si faccia riferimento:
   I. in generale, alle specifiche competenze alle quali il personale è preposto, avendo riguardo alle attribuzioni dell'ufficio al quale il dipendente è assegnato con ordine di servizio del Segretario generale, nonché agli specifici ulteriori ordini di servizio eventualmente adottati dai responsabili degli Uffici, nell'ambito delle rispettive competenze;
   II. per i processi che coinvolgono il trattamento in via ordinaria di "particolari categorie di dati" (art. 9 del "Regolamento"), l'assegnazione e la conseguente autorizzazione al trattamento debba essere, in ogni caso, circoscritta a dipendenti espressamente individuati attraverso specifici ordini di servizio dei dirigenti responsabili, con annotazione del nominativo dei soggetti autorizzati nel "Registro delle attività di trattamento dei dati personali";
   III. per i soggetti che collaborano con l'Autorità al di fuori di un organico rapporto di servizio, l'ambito di autorizzazione debba essere definito per iscritto nel contratto o nell'atto di conferimento dell'incarico;
3. ai fini della definizione delle istruzioni di cui agli articoli 29 e 32, par. 4, del "Regolamento", tutti i soggetti autorizzati al trattamento di dati personali, in forma digitale e/o analogica, si attengano ai criteri operativi e alle regole specificamente indicate nell'allegato "A" alla presente delibera;

RITENUTO che il complesso di misure oggetto della proposta di cui sopra sia adeguato ad assicurare il trattamento dei dati personali conformemente al "Regolamento" e alla normativa nazionale di adeguamento, nel rispetto del principio di *accountability* che vi è sotteso;

RITENUTO che l'adozione delle anzidette misure comporti una nuova ed organica disciplina della materia già oggetto della delibera n. 137/2019, approvata nella seduta del 24 ottobre 2019 e, quindi, il suo integrale superamento;

DELIBERA

1. è approvato, per le motivazioni di cui alla premessa, il documento recante "*Misure organizzative e conferimento di compiti e funzioni, ai sensi del regolamento (UE) 2016/679 e delle relative norme di adeguamento dell'ordinamento nazionale*" (Allegato "A"), che costituisce parte integrante della presente delibera;
2. la presente delibera sostituisce integralmente la delibera n. 137/2019 del 24 ottobre 2019 ed è pubblicata sul sito web istituzionale dell'Autorità.

Torino, 26 marzo 2020

Il Presidente
Andrea Camanzi

(documento firmato digitalmente ai sensi del D.Lgs 82/2005 s.m.i.)

CAMANZI
ANDREA
AUT. DI
REGOLAZ. DEI
TRASPORTI
PRESIDENTE
26.03.2020
19:09:58 UTC