Autorità di Regolazione dei Trasporti

Allegato “A” alla delibera n. 78/2020

MISURE ORGANIZZATIVE E CONFERIMENTO DI COMPITI E FUNZIONI, AI SENSI DEL REGOLAMENTO (UE) 2016/679 E DELLE RELATIVE NORME DI ADEGUAMENTO DELL’ORDINAMENTO NAZIONALE

SOMMARIO

1. INTRODUZIONE

Il presente documento definisce le misure tecniche ed organizzative finalizzate a dare attuazione alla normativa vigente in materia di tutela della *privacy* di cui al Regolamento UE n. 679/2016 (di seguito Regolamento e/o RGPD) e alle relative norme di adeguamento dell'ordinamento nazionale (d.lgs. 10 agosto 2018, n. 101).

In particolare, ai sensi del richiamato d.lgs. n. 101/2018, che ha introdotto l'art. 2-*quaterdecies* del vigente "Codice in materia di protezione dei dati personali" (d.lgs. n. 196/2003, di seguito "Codice"), il documento: individua gli specifici compiti e funzioni connessi al trattamento di dati personali attribuiti dal Titolare del trattamento a soggetti, espressamente designati, che operano sotto la sua autorità (Par. 2); definisce il sistema di autorizzazione al trattamento dei dati personali del personale e dei collaboratori dell'Autorità (Par. 3); individua i principi generali e le principali istruzioni operative cui devono attenersi i soggetti autorizzati al trattamento dei dati personali (Par. 4).

A tal fine, il Regolamento UE n. 679/2016 definisce:

- il **Titolare del trattamento,** quale *"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*" (art. 4, n. 7, del Regolamento);
- il **Responsabile del trattamento,** quale *"persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*", e, dunque, estraneo alla sua struttura;
- le ***persone autorizzate al trattamento dei dati personali,*** quali soggetti che effettuano trattamenti di dati sotto l'autorità diretta del Titolare. Tali soggetti (cd. ex incaricati), richiamati dall'art. 4, par. 1, n. 10, e dagli artt. 29 e 32, par. 4, del Regolamento, non possono trattare dati personali *"se non istruiti in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri".* Nell'ambito di tali previsioni, il Codice dispone, all'art. 2-quaterdecies, comma 2, 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 responsabilità.
- le **persone designate dal Titolare o dal Responsabile allo svolgimento di specifici compiti e funzioni**, quale figura intermedia, individuata dal "Codice" (art. 2-quaterdecies, paragrafo 1), secondo il quale "*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"*;
- Il **Responsabile della protezione dei dati** (RPD o DPO), previsto dagli artt. 37 ss. del Regolamento, con compiti di consulenza, vigilanza, sensibilizzazione e formazione del personale, è anche il punto di contatto per gli interessati e per il Garante privacy rispetto a ogni questione attinente all'applicazione del Regolamento.

2. ATTRIBUZIONE DI SPECIFICI COMPITI E FUNZIONI DEL TITOLARE

Ai sensi dell'art. 2-quaterdecies, co. 1, del "Codice", sono designati allo svolgimento di specifiche funzioni e compiti del Titolare del trattamento dei dati, i seguenti soggetti, in relazione ai ruoli ricoperti in base al vigente assetto organizzativo dell'Autorità:

2.1 Il Segretario generale

Il Segretario generale, quale organo amministrativo di vertice dell'Autorità, provvede, nell'ambito delle funzioni, come declinate dal Regolamento di organizzazione e funzionamento dell'Autorità (ROF), alle seguenti funzioni, alle quali attende con il supporto del Referente privacy:

I. coordina l'attività degli Uffici e vigila sul corretto adempimento degli obblighi in materia di trattamento dei dati personali, adottando i provvedimenti di gestione necessari per dare attuazione concreta alle misure tecniche e organizzative emanate dal Consiglio;

II. 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 e provvede alle relative comunicazioni agli interessati, ai sensi degli articoli 33 e 34 del Regolamento;

III. approva le specifiche attività di aggiornamento e formazione del personale in materia di tutela dei dati personali, su proposta del Responsabile dell'Ufficio Affari generali, amministrazione e personale, formulata d'intesa con il RPD.

2.2. Il Referente privacy

Il Referente privacy collabora con il Segretario generale nell'esercizio delle funzioni di cui al precedente paragrafo e opera come referente unico degli Uffici per i trattamenti di loro spettanza. L'incarico è attribuito al Responsabile dell'Ufficio *Information and Communication Technology,* quale figura dirigenziale preposta, ai sensi del ROF, alla tutela della privacy nell'ambito dell'Autorità.

Il Referente privacy, in particolare:

I. 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. A tal fine, si rapporta con il RPD e, se del caso, ne chiede il parere;

II. 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;

III. verifica eventuali esigenze di aggiornamento degli ordini di servizio e degli altri atti di autorizzazione al trattamento dei dati personali;

IV. 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, comunicando al RPD le informazioni necessarie per l'alimentazione del "Registro dei *Data breach*".

2.3. Il Responsabile dell'Ufficio *Information and Communication Technology* (ICT)

Il Responsabile dell'Ufficio Ufficio *Information and Communication Technology* (ICT), quale soggetto che, ai sensi del ROF, è la 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:

I. 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;

II. 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;

III. in materia di segnalazione di episodi di corruzione da parte dei dipendenti (*whistleblowing*), rende disponibile la procedura informatica di raccolta delle segnalazioni, assicurando la riservatezza dei dati personali del segnalante. In particolare, provvede affinché la piattaforma per l'acquisizione e gestione delle segnalazioni:

   - preveda l'utilizzo esclusivo di protocolli sicuri di trasporto dei dati, al fine di garantire sia la riservatezza e l'integrità dei dati relativi all'identità del segnalante e al contenuto della segnalazione sia l'autenticità delle pagine web utilizzate dalla procedura informatica per l'acquisizione e la gestione delle segnalazioni;

- assicuri l'accesso selettivo ai dati delle segnalazioni, da parte dei diversi soggetti autorizzati al trattamento e non invii alcun messaggio di notifica al dipendente e al segnalante;
- tracci le attività (accessi e operazioni), effettuate dall'RPCT e dagli altri soggetti autorizzati al trattamento, al fine di garantire la correttezza e la sicurezza del trattamento.

IV. Individua il personale con mansioni di manutenzione e conduzione applicativa del sistema (Amministratori di sistema). A tal fine:

- assegna le funzioni di amministratore di sistema con ordine di servizio, previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato. La designazione è individuale e reca l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Rende nota al personale l'identità degli amministratori di sistema;
- su richiesta dei responsabili degli Uffici, o del Segretario generale per gli esperti, fornisce indicazioni agli amministratori di sistema per l'attribuzione al personale e ai collaboratori del "profilo di autorizzazione" per l'accesso al protocollo informatico, al sistema di gestione documentale e alle cartelle condivise in rete. I "profili di autorizzazione" sono l'insieme delle facoltà operative/operazioni, tecnicamente consentite dal sistema informatico/applicativo a ciascun soggetto autorizzato, in relazione all'ambito di trattamento consentito al medesimo;
- verifica l'operato degli amministratori di sistema, con cadenza almeno annuale, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

2.4. Il Responsabile dell'Ufficio Affari generali, amministrazione e personale (AGA)

Il Responsabile dell'Ufficio Affari generali, amministrazione e personale:

I. 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;

II. quale soggetto preposto alla sottoscrizione dei contratti, ai sensi del Regolamento recante la disciplina contabile dell'Autorità:

- individua gli elementi di esperienza e affidabilità di cui all'art. 28, par. 1, del Regolamento, che costituiscono il presupposto per l'affidamento dell'incarico di Responsabile del trattamento a soggetti esterni con i quali siano posti in essere rapporti contrattuali cui sia connesso il trattamento di dati personali;
- 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, verificando se il Responsabile del trattamento dati fornisca garanzie sufficienti sull'adozione di misure tecniche e organizzative adeguate all'oggetto, alla durata e alle finalità del trattamento assegnato;
- assicura in particolare che i contratti o gli altri atti giuridici sopra menzionati, contengano una misura specifica 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, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati, in conformità all'art 28 par. 3 lett. g del Regolamento;
- verifica il rispetto delle regole definite contrattualmente onde assicurare il corretto trattamento dei dati, secondo quanto previsto dal Regolamento;

2.5. Il Responsabile della Prevenzione della corruzione e della trasparenza (RPCT)

Il Responsabile della Prevenzione della corruzione e della trasparenza (RPCT), nell'ambito delle funzioni alle quali è preposto:

I. 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;

II. in tema di segnalazione di episodi di corruzione da parte dei dipendenti (*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. In particolare:

- qualora esigenze istruttorie richiedano che altri uffici, all'interno dell'amministrazione, debbano essere messi a conoscenza del contenuto della segnalazione o della documentazione ad essa allegata, si attiva affinché non sia rivelata l'identità del segnalante, verificando l'espunzione dai documenti dei dati identificativi del segnalante e ogni altro elemento che possa, anche indirettamente, consentire l'identificazione dello stesso;
- ove nella documentazione trasmessa siano presenti dati personali di altri interessati (es. soggetto cui sono imputabili le possibili condotte illecite), verifica che i soggetti che trattano i dati siano espressamente autorizzati al riguardo;
- la possibilità di associare la segnalazione all'identità del segnalante è unicamente riservata all'RPCT. Pertanto, qualora il custode dell'identità del segnalante sia soggetto diverso dall'RPCT, lo stesso deve essere espressamente autorizzato al trattamento;
- prevede una procedura selettiva per l'eventuale assegnazione della trattazione di specifiche segnalazioni al personale di supporto, con relativa corrispondente restrizione dell'accesso ai fascicoli e alla piattaforma informatica predisposta dall'Ufficio ICT;

2.6. Il Responsabile della conservazione documentale

Per le finalità di cui al Regolamento, il Responsabile della conservazione documentale, quale soggetto cui è demandata la definizione e l'attuazione delle politiche del sistema di conservazione dei documenti dell'Autorità, svolge le seguenti funzioni:

I. 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;

II. nell'affidamento del processo di conservazione ad un soggetto esterno, verifica che quest'ultimo si conformi a quanto previsto dal Manuale di conservazione;

III. 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.

2.7. Gli amministratori di sistema

I soggetti preposti alla manutenzione e alla conduzione applicativa del sistema hardware e software dell'Autorità (Amministratori di sistema), nell'ambito dei compiti del Titolare del trattamento e, in particolare, dell'obbligo di garantire un livello di sicurezza adeguato al rischio (art. 32 del Regolamento), svolgono le seguenti funzioni:

I. 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;

II. operano sui sistemi informativi in uso presso l'Autorità esclusivamente attraverso meccanismi di autenticazione, registrata e comprendente i riferimenti temporali. I Privilegi di amministratore possono essere utilizzati solo per effettuare operazioni che ne richiedano i privilegi;

III. istruiscono le persone autorizzate in merito alle cautele da adottare per assicurare la segretezza e la custodia delle credenziali;

IV. assicurano che le credenziali delle utenze vengano sostituite con sufficiente frequenza (*password aging*);

V. 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, curando interventi di conservazione dei dati attraverso debite soluzioni di "*backup*" e progettando le attività di supporto al "*disaster recovery*";

VI. ove sussistano particolari esigenze di riservatezza, verificano che sia applicata la protezione crittografica in aree di lavoro con accesso riservato e controllato, dove ogni utente entra con specifiche credenziali e con diritti definiti puntualmente;

VII. 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 (*antivirus, firewall, Intrusion Detection System*, ecc.);

VIII. 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.

2.8. Il Responsabile della protezione dei dati personali

Con delibera n. 35/2020, il Consiglio ha nominato il Responsabile della protezione dei dati. Lo stesso, ai sensi del RGPD, svolge i seguenti compiti:

I. coopera e funge da punto di contatto con il Garante per la protezione dei dati personali, anche con riguardo alla consultazione preventiva di cui all'articolo 36 del Regolamento;

II. informa e coadiuva il Titolare del trattamento e, in merito agli obblighi derivanti dal Regolamento e dalle altre disposizioni in materia di protezione dei dati e relative modifiche;

III. vigila sull'osservanza del Regolamento e delle altre disposizioni relative alla protezione dei dati nonché delle disposizioni della presente delibera e e ne riferisce periodicamente al Titolare del trattamento;

IV. collabora con il Responsabile dell'Ufficio Affari generali, amministrazione e personale, nell'elaborazione dei piani di aggiornamento e formazione del personale in materia di trattamento dei dati personali;

V. costituisce il punto di contatto per gli interessati per l'esercizio dei loro diritti. Prende in carico le richieste di esercizio dei diritti degli interessati a lui eventualmente pervenute, le inoltra al Referente privacy e lo coadiuva nei conseguenti adempimenti da parte degli uffici;

VI. custodisce e aggiorna il "Registro delle attività di trattamento dei dati personali", il "Registro delle richieste di esercizio dei diritti degli interessati" e il "Registro dei *data breach*", sulla base delle informazioni acquisite dal Referente privacy;

VII. partecipa alle procedure in materia di violazioni di dati personali, coadiuvando il Segretario generale nelle decisioni afferenti alla gestione delle notificazioni dei *data breach* di cui agli artt. 33 e 34 del Regolamento;

VIII. Collabora con il Responsabile dell'Ufficio ICT nell'elaborazione dell'analisi dei rischi di cui all'art. 35 del Regolamento e, se del caso, nella valutazione d'impatto sulla protezione dei dati, di cui all'art. 36 del Regolamento.

3. AUTORIZZAZIONE AL TRATTAMENTO DEI DATI PERSONALI

Il personale in servizio è autorizzato al trattamento di dati personali funzionali all'esercizio delle specifiche competenze alle quali è preposto. A tal fine, si ha 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.

Resta inteso che, nei processi che coinvolgono il trattamento in via ordinaria di "particolari categorie di dati" (quelli di cui all'art. 9 del Regolamento, quali, ad esempio, i dati biometrici, genetici e relativi alla salute, i dati giudiziari, etc.), l'assegnazione e la conseguente autorizzazione al trattamento è ogni caso circoscritta a dipendenti espressamente individuati attraverso specifici ordini di servizio dei dirigenti responsabili. Il nominativo dei soggetti autorizzati è annotato nel "Registro delle attività di trattamento dei dati personali".

Per i soggetti che collaborano con l'Autorità al di fuori di un organico rapporto di servizio, l'ambito di autorizzazione è definito per iscritto nel contratto o nell'atto di conferimento dell'incarico.

L'autorizzazione al trattamento dei dati personali ha validità limitatamente al periodo di dipendenza/collaborazione e si intende revocata alla sua cessazione, ferma restando la facoltà di revoca in caso di inadempimento, violazione e/o utilizzo arbitrario dei dati o anche per ragioni di carattere organizzativo.

4. PRINCIPI E CRITERI PER IL TRATTAMENTO DEI DATI PERSONALI

Nell'ambito del delineato modello organizzativo, i soggetti autorizzati al trattamento dei dati personali si attengono alla normativa vigente in materia, nel rispetto dei principi generali e delle istruzioni operative di seguito riportate.

Restano fermi gli obblighi di riservatezza cui è soggetto tutto il personale dell'Autorità in forza di quanto previsto dall'articolo 2, comma 10, della legge n. 481 del 1995 (obbligo del segreto di ufficio), dall'articolo 23, comma 1, del Regolamento sul trattamento giuridico ed economico del personale dell'Autorità, dall'articolo 7 del Codice etico e dagli altri atti di organizzazione interna dell'Autorità. In tale ambito, si rinvia, in particolare, alle indicazioni contenute nel Manuale di gestione.

4.1. Principi generali

In base al principio dell'*accountability* di cui all'artt. 5 e 24 del RGPD, il Titolare del trattamento, e dunque tutti i soggetti autorizzati al trattamento dei dati, ispirano il proprio operato al rispetto dei principi generali di cui all'art. 5, par.1, del Regolamento, ai sensi del quale i dati personali devono essere:

I. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (**principio di liceità, correttezza e trasparenza**): un trattamento si considera "lecito" quando è conforme alla legge in generale e "corretto" quando avviene in maniera tale da rispettare la finalità di tutela delle persone con riferimento al trattamento dei relativi dati personali;

II. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità (**principio di limitazione della finalità**). Conseguenza di questo principio è il divieto di trattare i dati raccolti per finalità ulteriori e/o diverse da quelle ordinarie, di norma oggetto dell'informativa all'interessato e per cui è stato prestato, nei casi in cui le norme lo prevedono, il consenso dell'interessato;

III. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (**principio di minimizzazione dei dati**). I dati raccolti non devono essere superflui rispetto alla finalità del trattamento dichiarata, occorre pertanto verificare se tutti i dati raccolti rispondono alla finalità

perseguita;

IV. esatti e, se necessario, aggiornati (**principio di esattezza**). Devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

V. conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (**principio di limitazione della conservazione dei dati**);

VI. trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (**principio di integrità e riservatezza**).

4.2. Istruzioni operative

Premesso l'obbligo, per tutti i soggetti autorizzati, di operare nel rispetto dei principi sopra enucleati, le indicazioni che seguono espongono, più in dettaglio, le corrette modalità operative da utilizzare per la gestione dei dati personali:

I. rispettare le disposizioni impartite dal Titolare e dai soggetti designati allo svolgimento dei relativi compiti;

II. non diffondere (in forma cartacea, elettronica o verbale) informazioni che contengano dati personali né comunicarle a persone non autorizzate al trattamento;

III. integrare i documenti informatici e analogici con le informative privacy, di cui agli artt. 13 e 14 del Regolamento, in conformità delle indicazioni impartite;

IV. comunicare al Referente privacy e al RPD ogni notizia utile ai fini della tutela dei dati personali degli interessati e, in particolare, di eventuali violazioni dei dati personali che possano esporre a rischio le libertà ed i diritti degli interessati ovvero la sicurezza, integrità e disponibilità dei dati trattati (*data breach*);

V. partecipare ai programmi di aggiornamento organizzati all'interno dell'Autorità, in materia di tutela dei dati personali;

VI. nell'ambito dei trattamenti operati tramite i sistemi informativi, i soggetti autorizzati al trattamento sono tenuti a:

- utilizzare esclusivamente i sistemi informativi, i terminali e i *software* messi a disposizione dall'Autorità o da questa approvati e attenersi alle istruzioni impartite;
- custodire con cura e diligenza le proprie credenziali per l'accesso e l'utilizzo dei sistemi informativi e non cederle o divulgarle;
- non utilizzare sistemi di memorizzazione automatica delle credenziali di accesso, specie nell'ipotesi in cui venga utilizzato un terminale di proprietà;
- non lasciare incustodito e/o liberamente accessibile, anche se all'interno dei locali dell'Autorità, il terminale tramite il quale si sta svolgendo il trattamento;
- non realizzare *backup* dei dati in *cloud* o su supporti di proprietà;
- evitare l'utilizzo di connessioni non protette derivanti (ad esempio) dalla connessione internet da computer condivisi (ad esempio PC degli alberghi o degli Internet Point) o attraverso reti (fisse o wi-fi) che non siano dell'Autorità; tali connessioni potrebbero comportare rischi di sicurezza di dati e informazioni trattate e quindi possono essere utilizzate solo se non si trattano dati personali;

- nella trasmissione elettronica di dati personali (e-mail, servizi web, trasferimento file, instant messaging, ecc.), individuare correttamente i destinatari della trasmissione, evitando di coinvolgere persone non autorizzate;

VII. ove il trattamento di dati personali sia effettuato in forma analogica, devono essere osservate, in particolare, le seguenti disposizioni finalizzate al controllo ed alla custodia degli atti e dei documenti contenenti dati personali, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento:

- custodire con cura e diligenza gli atti e i documenti contenenti dati personali, in modo che ad essi non accedano persone prive di autorizzazione;
- adottare le opportune cautele in caso di allontanamento dalla propria postazione, riponendo i documenti di lavoro negli armadi o nei cassetti chiusi a chiave o in altro luogo sicuro;
- eventuali copie analogiche di documenti dovranno essere distrutte al termine del procedimento o dell'attività, ove la conservazione in forma analogica non sia strettamente necessaria per esigenze d'ufficio;

Ferme le indicazioni di cui sopra, i soggetti preposti all'assegnazione dei documenti e dei fascicoli al personale, verificano la presenza di "particolari categorie di dati personali", limitando, conseguentemente, l'assegnazione del documento ai dipendenti e ai collaboratori effettivamente preposti allo svolgimento delle corrispondenti attività lavorative.

Specifiche istruzioni per il personale che svolge il proprio servizio in telelavoro o lavoro agile sono contenute, quanto alla tutela della privacy, nell'art, 2, commi 14 e 15, del regolamento recante la "Disciplina del telelavoro e del lavoro agile" (delibera n. 39 del 5 aprile 2018 e successive modificazioni).

5. TERMINI E DEFINIZIONI

Anonimizzazione: tecnica di trattamento dei dati personali tramite la quale i dati personali non possano più essere attribuiti a un interessato specifico, nemmeno attraverso l'utilizzo di informazioni aggiuntive.

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

Data Protection by-design/by-default: l'incorporazione della privacy a partire dalla progettazione di un processo, con le relative applicazioni informatiche di supporto. La prima introduce la protezione dei dati fin dalla progettazione per caso specifico, la seconda per impostazione predefinita di una pluralità di casi tra loro omogenei.

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.

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;

DPR o DPO: Responsabile della protezione dei dati personali/*Data Protection Officer* designato dal titolare del trattamento

RGPD o Regolamento: Regolamento Europeo sulla protezione dei dati personali 679/2016 – General Data Protection Regulation.

Interessato: persona fisica identificata o identificabile. 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.

Misure di sicurezza: misure tecniche ed organizzative adeguate a garantire un livello di sicurezza dei dati trattati adeguato al rischio.

Persone Autorizzate (già Incaricati): persone fisiche autorizzate al trattamento dei dati personali sotto la diretta autorità del Titolare e/o del Responsabile ex artt. 4(10) e 29 del RGPD.

Processo: sequenza di sottoprocessi/attività, poste in essere da persone o soggetti organizzativi diversi (strutture organizzative, enti), tra loro interrelate e finalizzate al conseguimento di un obiettivo comune, che creano valore trasformando delle risorse (input del processo) in un prodotto (output del processo).

Pseudonimizzazione: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo esterno che tratta dati personali per conto del titolare del trattamento;

Responsabile della Conservazione documentale: figura preposta alla gestione e supervisione del processo di conservazione dei documenti (digitali o cartacei);

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;

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. Per quanto riguarda l'Autorità di regolazione dei trasporti, il Titolare del trattamento è il Consiglio;

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;

Violazione dei dati personali (cd. Data breach): 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.