Repubblica Italiana

Regione Siciliana

Misure attuative del Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016

Istruzioni e norme comportamentali di carattere generale
per il trattamento dei dati personali di competenza del Dipartimento
Regionale Autorità di Bacino del Distretto Idrografico della Sicilia

Il trattamento dei dati personali effettuato per conto del Dipartimento Regionale Autorità di Bacino dovrà avvenire nel rispetto dei principi del Regolamento UE 2016/679, del D. lgs 101/2018 e delle altre disposizioni vigenti in materia.

Per trattamento di dati personali si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, 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.

Il trattamento dei dati per conto del Dipartimento Regionale Autorità di Bacino può avvenire nei seguenti casi:

- sia previsto da obblighi di legge cui è soggetta l'Amministrazione;
- riguardi l'interesse pubblico o esercizio di pubblici poteri propri dell'Amministrazione;
- sia necessario per l'adempimento di obblighi contrattuali stipulati dall'Amministrazione;
- sia necessario a garantire gli interessi vitali della persona interessata o di terzi;
- l'interessato abbia espresso il consenso esplicito in favore dell'Amministrazione;
- sia necessario per tutelare interesse legittimo prevalente dell'Amministrazione o di terzi cui i dati vengono comunicati.

Il trattamento dei dati avviene mediante documentazione cartacea, strumenti informatici e telematici, con modalità strettamente correlate alle finalità stesse e comunque in modo da garantire la sicurezza e la riservatezza adeguata.

Nel trattamento dei dati personali va osservato il principio di pertinenza e di non eccedenza, limitando i dati trattati a quelli strettamente necessari ed attinenti al compito da svolgere.

E' pertanto vietato accedere a dati personali non necessari al compito amministrativo che deve svolgersi.

I dati personali devono essere trattati per le finalità istituzionali del Dipartimento Regionale Autorità di Bacino secondo le modalità di cui alle presenti istruzioni e di ogni ulteriore specifica dis posizione in merito emessa dal Titolare del trattamento di dati personali (Presidente pro-tempore della Regione Sicilia), dal Responsabile del trattamento (il Dirigente Generale pro-tempore del Dipartimento Regionale Autorità di Bacino, nominato dal Titolare) e da tutti i sub-Responsabili (i Dirigenti pro-tempore delle Aree, dei Servizi o delle Unità Operative del Dipartimento Regionale Autorità di Bacino) nell'ambito delle rispettive competenze e prerogative.

Il trattamento dei dati personali, che rientri nei suddetti casi consentiti, potrà essere effettuato da:

1) il personale che agisce per conto del Dipartimento Regionale Autorità di Bacino, nell'ambito dei compiti assegnati;

2) le società, gli enti, i consorzi che forniscono specifici servizi al Dipartimento Regionale Autorità di Bacino o che svolgono attività connesse, strumentali o di supporto a

quelle dell'Amministrazione regionale stessa purché designati a svolgere la funzione di sub-Responsabile tecnico. Tali soggetti dovranno essere stati appositamente ed esplicitamente autorizzati dal Titolare o dal Responsabile o dai sub-Responsabili, qualora autorizzati dal Responsabile.

3) i soggetti a cui la facoltà di accedere ai dati personali sia riconosciuta da disposizioni di legge o di normativa comunitaria.

L'accesso ai dati è consentito nella misura strettamente necessaria ad adempiere ai compiti assegnati, con divieto di qualunque diversa utilizzazione, funzione e divulgazione non espressamente autorizzata.

In particolare i soggetti autorizzati che trattano i dati per conto del Dipartimento Regionale Autorità di Bacino osserveranno almeno le seguenti misure di sicurezza:

- è vietato comunicare a persone non autorizzate i dati personali di qualunque genere (giudiziari, sanitari o altri dati), elementi e informazioni dei quali il soggetto autorizzato viene a conoscenza nell'esercizio delle proprie funzioni e mansioni. In caso di dubbio, è necessario accertarsi che la persona a cui devono essere comunicati i dati sia o meno autorizzato a riceverli, mediante richiesta preventiva al proprio dirigente;

- è vietata l'estrazione di originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, fascicoli, lettere, data base o altro;

- la documentazione cartacea, compresi i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali, gli atti e i documenti contenenti i dati personali, al termine dell'orario di lavoro, dovrà essere riposta in cartelle ed armadi chiusi in modo da evitare che, in assenza degli autorizzati, altri soggetti non autorizzati ne possano prenderne visione;

- qualora i documenti contengano dati sensibili o giudiziari essi dovranno essere riposti in archivio ad accesso controllato. I documenti contenenti dati sanitari, anche se pervenuti senza busta, dovranno essere conservati in buste chiuse ed in armadi chiusi e, se trasmessi, andranno inseriti in buste chiuse con lettera di accompagnamento, da cui non si evincano i dati sanitari in essa contenuti;

- per quanto riguarda i flussi di documenti cartacei all'interno degli uffici regionali del Dipartimento Regionale Autorità di Bacino dovranno essere adottate idonee misure organizzative per salvaguardare la riservatezza dei dati personali (es. trasmissione dei documenti in cartelle, carpette o buste chiuse ecc.);

- l’accesso ai dati tramite computer dovrà avvenire tramite un nome utente e una password associata, attribuiti al soggetto che effettua l’accesso;

- la password utilizzata dovrà essere di robustezza adeguata e contenere lettere maiuscole e minuscole, numeri e caratteri speciali. Non dovrà contenere elementi facilmente riconducibili all’utente;

- il nome utente e la password sono personali e non dovranno essere condivisi con altri soggetti (a meno che non sia espressamente previsto);

- non dovranno essere inseriti dati personali in sistemi informativi non protetti da nome utente e password associata o protetti dal solo nome utente o dalla sola password;

- la password dovrà essere cambiata periodicamente con una diversa;
- nel caso di cessazione del rapporto di lavoro il dirigente dell'Ufficio dovrà chiedere la disattivazione dell'account presso qualunque sistema informativo utilizzato o server di rete;
- dovrà essere vietato accedere ad un computer, alla rete o ad un sistema informativo utilizzando credenziali di altre persone;
- i documenti informatici contenenti dati personali non dovranno lasciati in cartelle di libero accesso o che consentono l'accesso a soggetti non autorizzati;
- non dovrà essere consentito a persone non autorizzate per iscritto dal Titolare o dal Responsabile di utilizzare gli strumenti informatici, personal computers o video terminali, installati negli uffici;
- alla fine della sessione di lavoro i computer, eccetto quelli in funzione "h24", dovranno essere spenti fisicamente;
- non si dovrà accedere a servizi online non consentiti;
- nei computer nei quali vengono utilizzati dati personali, ciascun dipendente dovrà porre particolare attenzione ai programmi e ai servizi online utilizzati, al fine di escludere con ragionevole certezza la diffusione, anche involontaria, di dati personali ai quali ha avuto accesso in ragione delle autorizzazioni;
- non dovrà essere installato ed eseguito alcun software senza previa verifica dello stesso da parte del proprio referente informatico, a meno che il software non sia inserito in una lista dei software di uso consentito;
- non si dovrà tentare di acquisire privilegi di amministratore di sistema informatico;
- non si dovranno detenere chiavi di armadi o archivi ai quali non sia stato consentito l'accesso;
- non si dovrà collegare modem o altro dispositivo che consenta un accesso non controllato alla rete informatica regionale;
- il dipendente dovrà utilizzare con consapevolezza gli strumenti informatici di proprietà della Regione siciliana e dovranno essere utilizzati esclusivamente per rendere la prestazione lavorativa. Ogni dipendente sarà responsabile dell'utilizzo degli strumenti informatici che gli sono stati assegnati. Ogni utilizzo non inerente l'attività lavorativa è vietato, in quanto può determinare disservizi o minacce alla sicurezza dei dati;
- si dovranno effettuare copie di sicurezza (backup) settimanale del lavoro svolto nell'arco della settimana su un supporto che dovrà essere custodito separatamente dal computer ovvero su una cartella di un computer diverso, purché questa sia protetta da password personale che abiliti l'accesso esclusivo ai dati contenuti; nel caso di memorizzazione in servizi di cloud (ad es. Dropbox, Google Drive, One Drive, WeTransfer ecc.) i documenti, ed in particolare quelli contenenti dati sensibili, dovranno essere criptati in maniera adeguata;
- le copie di backup dovranno essere utilizzate esclusivamente per il fine per cui sono state effettuate, evitando di utilizzarle per accedere ai dati ivi contenuti tramite computer non autorizzati dall'Amministrazione;

- si dovranno informare prontamente il Titolare e il Responsabile del trattamento, anche per il tramite dei Sub-Responsabili del Dipartimento Regionale Autorità di Bacino, qualora si dovesse verificare una perdita di dati ovvero un accesso non autorizzato ai dati personali

detenuti con consapevolezza, determinandosi un rischio alle libertà personali della persona a cui si riferiscono i dati;

- la consultazione della posta elettronica dovrà sempre essere improntata alla massima prudenza, non aprendo allegati ai messaggi di posta non richiesti o provenienti da soggetti sconosciuti o con elementi che tradiscano comportamenti dubbi;

- la navigazione su internet sarà consentita solo sui siti connessi alla attività lavorativa svolta, facendo attenzione a non condividere dati personali propri o altrui ed evitando di collegarsi a siti tramite link non richiesti;

- è vietato compiere azioni che potrebbero mettere a rischio i dati personali o creare falle nella sicurezza della rete o del computer utilizzato: ad esempio scaricando file, programmi, audio o video non connessi all'attività lavorativa e di provenienza dubbia o non verificata.

I soggetti autorizzati al trattamento dei dati saranno tenuti a collaborare, nell'ambito delle rispettive competenze, con il Titolare, il Responsabile, i sub-Responsabili e il Referente privacy del Dipartimento Regionale Autorità di Bacino, fornendo loro il supporto e l'assistenza necessaria allo svolgimento dei loro compiti, nel rispetto del Regolamento UE 2016/679, del D. lgs. 101/2018 e delle ulteriori disposizioni vigenti in materia.

Il Segretario Generale
Francesco Greco
F/to

Il Referente Privacy
del Dipartimento
Raffaele Greco
F/to

Originale agli atti d'ufficio