REPUBBLICA ITALIANA

Regione Siciliana
Assessorato regionale dell'Agricoltura, dello Sviluppo rurale
e della Pesca mediterranea
Dipartimento regionale dell'Agricoltura

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 dell'Agricoltura

Anno 2024

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 personali effettuato per conto dell'Amministrazione deve avvenire nel rispetto dei principi del Regolamento UE 2016/679, del D.lgs. 101 del 10 agosto 2018 e delle altre disposizioni vigenti in materia.
Il trattamento dei dati personali per conto dell'Amministrazione viene effettuato se:
- previsto da obblighi di legge cui è soggetta l'Amministrazione;
- riguarda l'interesse pubblico o esercizio di pubblici poteri propri dell'Amministrazione;
- è necessario per l'adempimento di obblighi contrattuali stipulati dall'Amministrazione;
- l'interessato, nei casi previsti, ha espresso il consenso esplicito in favore dell'Amministrazione;
- è necessario a garantire gli interessi vitali della persona interessata o di terzi;
- è necessario per tutelare l'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 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' vietato accedere a dati personali non necessari al compito amministrativo che deve svolgersi.
Nell'ambito del Dipartimento regionale dell'Agricoltura i dati personali devono essere trattati per le finalità istituzionali, con le modalità di cui alle presenti istruzioni ed alle eventuali ulteriori specifiche disposizioni emanate dal Titolare del trattamento di dati personali.
Il Titolare del trattamento è l'Assessorato regionale per l'Agricoltura, lo Sviluppo rurale e la Pesca mediterranea, rappresentato dall'Assessore pro tempore.
Il Responsabile del trattamento, definito all'art. 4 del GDPR come la persona fisica, giuridica, PA o ente che elabora i dati personali per conto del Titolare del trattamento, è il Dirigente Generale del Dipartimento regionale dell'Agricoltura.
Inoltre il Responsabile si avvale dei sub-Responsabili, ovvero dei dirigenti di strutture intermedie o Unità Operative che nell'ambito delle rispettive competenze e prerogative effettuano il trattamento di dati personali.
Inoltre, nei casi consentiti, il trattamento dei dati personali può essere effettuato da:

1) il personale che agisce per conto dell'Amministrazione regionale, nell'ambito dei compiti assegnati (*soggetti autorizzati* al trattamento, ai sensi del D.Lgs 10 agosto 2018, art. 2-quaterdecies, e designati con provvedimento formalmente notificato);
2) le società, gli enti, i consorzi che forniscono specifici servizi o che svolgono attività connesse, strumentali o di supporto a quelle dell'Amministrazione stessa purché designati a svolgere la funzione di sub-Responsabile tecnico. Tali soggetti devono essere appositamente ed esplicitamente autorizzati dal Titolare, o dal Responsabile o dal sub-Responsabile (qualora autorizzato dal Responsabile).

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

Poiché l''accesso ai dati personali è consentito nella misura strettamente necessaria ad adempiere ai compiti assegnati, con divieto di qualunque diversa utilizzazione, funzione e divulgazione non espressamente autorizzata, il Dipartimento regionale dell'Agricoltura adotta le seguenti misure di sicurezza:

- l'accesso alle immagini riprese dalle telecamere di videosorveglianza da postazione remota è consentito solo in casi eccezionali che derivino da una specifica richiesta dell'autorità giudiziaria o di polizia giudiziaria in relazione a un'attività investigativa in corso;
- ai soggetti autorizzati al trattamento dei dati è vietato comunicare a persone non autorizzate i dati personali di qualunque genere, elementi e informazioni dei quali vengono 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 dirigente di struttura.
- è vietata l'estrazione di originali e/o copie cartacee o informatiche per uso personale di documenti, manuali, fascicoli, lettere, data base o altro.
- al termine dell'orario di lavoro 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, devono essere riposti in cartelle ed armadi chiusi in modo da evitare che, in assenza degli autorizzati, ne possano prendere visione soggetti non autorizzati;
- i documenti che contengono dati personali di cui al Reg. UE 2016/679 artt. 9 (particolari categorie di dati) e 10 (dati relativi a condanne penali e reati) devono essere riposti in archivio ad accesso controllato. I documenti contenenti dati sanitari, anche se pervenuti senza busta, devono essere conservati in buste chiuse ed in armadi chiusi e, se trasmessi, devono essere inseriti in buste chiuse con lettera di accompagnamento da cui non si evincano i dati sanitari in essa contenuti;
- per i flussi di documenti cartacei tra uffici dipartimentali, devono essere adottate idonee misure organizzative al fine di salvaguardare la riservatezza dei dati personali (es. trasmissione dei documenti in cartelle, carpette o buste chiuse, ecc.);
- non devono essere riutilizzate come carta da riciclo o da appunti copie fotostatiche di documenti contenenti dati personali, seppur non perfettamente riuscite;
- se si rende necessario trattare dati personali per telefono, si raccomanda di non parlare ad alta voce, soprattutto se si utilizzano telefoni cellulari e in presenza di terzi non autorizzati;
- in caso di eliminazione di documenti contenenti dati particolari (ex dati sensibili) o giudiziari, questi devono essere distrutti e non gettati nei cestini tal quali;
- l'accesso ai dati tramite computer deve avvenire tramite un nome utente e una password associata, attribuito al soggetto che effettua l'accesso;
- la password utilizzata deve essere di robustezza adeguata e contenere lettere maiuscole e minuscole, numeri e caratteri speciali. Non deve contenere elementi facilmente riconducibili al soggetto e deve essere cambiata periodicamente;
- il nome utente e la password, che sono personali, non devono essere condivisi con altri soggetti a meno che non sia espressamente previsto;
- non devono 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;

- nel caso di cessazione del rapporto di lavoro, il dirigente responsabile dell'Ufficio deve chiedere la disattivazione della mail aziendale gestita dall'ex dipendente e dell'account, presso qualunque sistema informativo utilizzato o server di rete;
- è vietato a tutti i dipendenti accedere ad un computer, alla rete o ad un sistema informativo utilizzando credenziali di altri;
- i documenti informatici contenenti dati personali non devono essere lasciati in cartelle di libero accesso o che consentono l'accesso a soggetti non autorizzati;
- non è consentito, a persone esterne non autorizzate per iscritto dal Titolare o dal Responsabile, l'uso di strumenti informatici, personal computer o video terminali installati negli uffici;
- ciascun dipendente, in caso di allontanamento dalla propria postazione di lavoro anche per la pausa caffè o pranzo, deve adottare tutte le accortezze e precauzioni possibili al fine di impedire l'accesso fisico a chi non è legittimato, esterno all'amministrazione o interno non specificamente autorizzato;
- alla fine della sessione di lavoro i computer, eccetto quelli in funzione "h24", devono essere spenti fisicamente;
- ciascun dipendente deve porre particolare attenzione ai programmi e ai servizi online utilizzati sul proprio pc, al fine di escludere con ragionevole certezza la diffusione, anche involontaria, di dati personali ai quali ha avuto accesso in ragione delle autorizzazioni ricevute;
- non deve essere installato ed eseguito alcun software senza previa verifica dello stesso da parte del referente informatico, a meno che il software non sia inserito in una lista dei software di uso consentito;
- non è consentito tentare di acquisire privilegi di amministratore del sistema informatico;
- non è consentito detenere chiavi di armadi o archivi ai quali non sia stato autorizzato l'accesso;
- non è consentito collegare modem o altro dispositivo che permetta un accesso non controllato alla rete informatica regionale senza apposita autorizzazione;
- ogni dipendente deve utilizzare con consapevolezza gli strumenti informatici che sono di proprietà della Regione Siciliana che gli sono stati assegnati e dei quali è personalmente responsabile. Gli strumenti informatici devono essere utilizzati esclusivamente per rendere la prestazione lavorativa. Ogni utilizzo non inerente l'attività lavorativa è vietato, in quanto può determinare disservizi o minacce alla sicurezza dei dati;
- è opportuno effettuare copie di sicurezza (backup) del lavoro svolto nell'arco della settimana, su un supporto che deve 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, devono essere criptati in maniera adeguata;

- le copie di backup possono essere utilizzate esclusivamente per il fine per cui sono state effettuate e non possono essere utilizzate, per accedere ai dati ivi contenuti, tramite computer non autorizzati dall'Amministrazione;
- la consultazione della posta elettronica deve essere sempre improntata alla massima prudenza, evitando di aprire file allegati ai messaggi di posta non richiesti o provenienti da soggetti sconosciuti o con elementi che tradiscano comportamenti dubbi. Tali file potrebbero

essere portatori di virus e compromettere la funzionalità del pc in dotazione, l'integrità dei dati in esso contenuti e soprattutto l'integrità dei sistemi collegati al pc stesso;
- nell'ipotesi in cui, per gli scambi di documenti informatici tra un ufficio dipartimentale e un altro, debba effettuarsi la trasmissione di categorie particolari di dati personali via mail, gli autorizzati devono prestare la massima attenzione a che:
  - l'indirizzo del destinatario sia correttamente digitato;
  - l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura particolare;
  - nel corpo del messaggio sia presente la seguente dicitura standardizzata in cui si avverte della riservatezza del messaggio: "*Questo messaggio di posta elettronica e il suo contenuto sono riservati e confidenziali e destinati esclusivamente al soggetto indicato nell'indirizzo. Se per errore ricevete questo messaggio o non siete il soggetto destinatario o delegato dal destinatario alla lettura qualsiasi uso, diffusione, inoltro, stampa o copia di questa email è rigorosamente proibito. In questo caso Vi preghiamo di notificare l'errore al mittente e cancellare definitivamente il messaggio di posta elettronica.*" ;
- la navigazione su internet è consentita solo sui siti connessi alla attività lavorativa svolta e deve essere posta particolare attenzione a non condividere dati personali propri o altrui ed evitare 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.

Nel caso in cui sul proprio PC risulti impossibile aprire i file, staccare immediatamente il cavo di rete del personal computer e richiedere l'intervento dell'amministratore di rete (Sicilia digitale).

Tutti i soggetti autorizzati al trattamento dei dati personali sono tenuti a collaborare, nell'ambito delle rispettive competenze, con il Titolare, il Responsabile e il Referente privacy (dirigente responsabile dell'UO A6.04 "Trasparenza e semplificazione"), *fornendo loro il supporto e l'assistenza necessaria allo svolgimento dei loro compiti nel rispetto del Regolamento UE 2016/679, del D.lgs. 101 del 10 agosto 2018 e delle ulteriori disposizioni vigenti in materia.*

Gestione della violazione dei dati personali (data breach)

L'art. 4 del Reg. UE 2016/679 definisce la **violazione dei dati personali** (*data breach*) come "*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*".
Quindi, un data breach può essere un evento doloso, come un attacco informatico, oppure un evento accidentale come un accesso abusivo, un incidente, la semplice perdita di una chiavetta USB, un malfunzionamento hardware o software.
Per stabilire cosa fare in caso di violazione dei dati personali occorre una valutazione del rischio, cioè dei possibili effetti. Il rischio viene valutato tenendo in considerazione natura, sensibilità e volume dei dati personali violati, numero degli interessati, grado di possibilità che si verifichino effetti dannosi sui diritti e le libertà personali degli interessati o eventuali ripercussioni di carattere economico-finanziario dovute a pretese risarcitorie nei confronti dell'Amministrazione regionale.

Una volta scoperta la violazione dei dati, qualora si potesse determinare un rischio alle libertà personali della persona a cui si riferiscono i dati, sarà necessario informare prontamente il Titolare e il Responsabile del trattamento, anche per il tramite dei Sub-Responsabili del Dipartimento regionale dell'Agricoltura. Il Titolare, così come stabilisce il GDPR, deve quindi notificare l'evento all'Autorità di controllo (Garante della privacy), tranne nel caso in cui "*sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche*" (es. perdita di dati già pubblici). La notifica deve avvenire "*senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza*" il Titolare. Qualora la notifica non avvenga nelle 72 ore, il Titolare dovrà precisare anche i motivi del ritardo. La norma prevede anche la possibilità di allegare ulteriori informazioni in un momento successivo.
Nel caso di necessaria notifica all'Autorità, questa deve essere effettuata in modo telematico seguendo le istruzioni disponibili nel sito del Garante:
https://servizi.gpdp.it/databreach/s/istruzioni

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO DEL DIPARTIMENTO

In adempimento al GDPR 2016/679 il Dipartimento dell'Agricoltura, provvede periodicamente ad aggiornare il proprio Registro del Responsabile dei trattamenti e, per i processi di propria competenza, quello del Titolare.
Il registro contiene, tra l'altro, le seguenti informazioni:

- il nome e i dati di contatto del titolare, del responsabile e del sub-responsabile del trattamento e del responsabile della protezione dei dati;
- le finalità del trattamento;
- le categorie di interessati;
- le categorie di dati personali trattati;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- i termini previsti per la cancellazione delle diverse categorie di dati;
- le misure di sicurezza tecniche e organizzative adottate.

Per le attività di trattamento del Dipartimento dell'Agricoltura con Titolarità a carico dell'Assessore al ramo, l'interessato può esercitare i propri diritti trasmettendo la richiesta a dpo@regione.sicilia.it oppure dpo@certmail.regione.sicilia.it.

TRATTAMENTO DEI DATI PER LE ATTIVITA' DELEGATE DA AGEA

Per le attività effettuate dalla Regione Siciliana - Dipartimento regionale dell'Agricoltura per conto di AGEA, Organismo Pagatore, il Dipartimento mantiene il ruolo di Responsabile del trattamento dei dati personali, mentre il Titolare del trattamento, in questo caso, è AGEA.
I trattamenti effettuati dal Dipartimento in ragione delle attività delegate da AGEA hanno ad oggetto essenzialmente dati personali identificativi, giudiziari, finanziari. Le categorie di interessati sono i soggetti che chiedono il pagamento di aiuti, contributi, premi o sussidi comunitari in attuazione di misure relative al fondo comunitario FEASR di cui AGEA è competente, nonché i soggetti connessi ai predetti, identificati ai fini dell'applicazione della vigente normativa antimafia.
Il Dipartimento dell'Agricoltura, che ha sottoscritto un'apposita convenzione con AGEA, in adempimento a quest'ultima deve assicurare l'adozione di misure di sicurezza a protezione del

trattamento dei dati e rendere disponibili al Titolare (AGEA) tutte le informazioni necessarie per dimostrare il rispetto degli adempimenti normativi previsti dal GDPR anche attraverso periodiche attività di verifica, comprese le ispezioni realizzate dal Titolare stesso (AGEA) o da un altro soggetto da questi incaricato.
Il Dipartimento autorizza i dipendenti ad effettuare il trattamento dei dati per conto di AGEA, assegnando credenziali specifiche per l'abilitazione ai servizi del portale del SIAN. Tutti i soggetti autorizzati al trattamento dei dati per conto di AGEA sono tenuti a rispettare le stesse misure di sicurezza precedentemente citate con accortezza e, nel caso in cui si palesi una violazione di dati personali (cd. *data breach*) darne comunicazione, tempestivamente e senza ingiustificato ritardo, al Responsabile - Dirigente Generale e al Referente privacy. Il Dipartimento dovrà, quindi, inviare al Titolare AGEA ed al Responsabile della Protezione dei Dati di AGEA, **entro 24 ore dall'avvenuta conoscenza dell'evento**, la documentazione inerente la violazione. A seguito della notifica, da inviare sia all'indirizzo PEC protocollo@pec.agea.gov.it che all'indirizzo email ageaprivacy@agea.gov.it, AGEA valuterà se comunicare la violazione all'Autorità Garante per la protezione dei dati personali e, nel caso di rischio per i diritti e le libertà dell'interessato, darne comunicazione anche a quest'ultimo.
Qualora per le attività delegate al Dipartimento da AGEA, un ufficio riceva istanza dall'interessato in esercizio dei propri diritti previsti dal GDPR, (richieste di informazioni sul trattamento dei dati personali, accesso, modifica, cancellazione, limitazione, ecc.), è tenuto a darne tempestiva comunicazione al Responsabile - Dirigente Generale e al Referente privacy affinché si possa avviare la seguente procedura prevista dalla convenzione:
– trasmettere comunicazione al Titolare AGEA o al Responsabile della Protezione dei Dati (RPD) di AGEA, allegando copia della richiesta;
– valutare con il Titolare AGEA e con il RPD di AGEA la legittimità della richiesta e soddisfare la richiesta ritenuta legittima.

Palermo, 23 ottobre 2024

f.to. Il Titolare del Trattamento
L'Assessore
(on. Salvatore Barbagallo)

f.to: Il Responsabile del Trattamento
Dirigente Generale
Dario Cartabellotta