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 2020

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 per conto dell'Amministrazione può avvenire nei seguenti casi:

- sia previsto da obblighi di legge cui è soggettal'Amministrazione;
- riguardi l'interesse pubblico o esercizio di pubblici poteri propri dell'Amministrazione;
- sia necessario per l'adempimento di obblighi contrattuali stipulati dall'Amministrazione;
- l'interessato, nei casi previsti, abbia espresso il consenso esplicito in favore dell'Amministrazione;
- sia necessario a garantire gli interessi vitali della persona interessata o di terzi;
- sia necessario per tutelare l'interesse legittimo prevalente dell'Amministrazione o di terzi cui idati 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, secondo le modalità di cui alle presenti istruzioni e di ogni ulteriore specifica disposizione emessa dal Titolare del trattamento di dati personali (l'Assessore regionale per l'Agricoltura, lo Sviluppo rurale e la Pesca mediterranea), dal Responsabile del trattamento (il Dirigente Generale,

incaricato dal Titolare) e dal sub-Responsabile (dirigente della struttura intermedia o dell'unità operativa) nell'ambito delle rispettive competenze e prerogative.

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

1) il personale che agisce per conto dell'Amministrazione regionale, nell'ambito dei compiti assegnati;

2) le società, gli enti, i consorzi che forniscono specifici servizi al Dipartimento 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 dovranno essere stati 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.

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.

I soggetti autorizzati che trattano i dati per conto del Dipartimento regionale dell'Agricoltura devono osservare almeno le seguenti misure di sicurezza:

- l'accesso da postazione remota alle immagini riprese dalle telecamere di videosorveglianza 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;
- 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 o informatiche per uso personale di documenti, manuali, fascicoli, lettere, database 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 devono essere riposti in cartelle ed armadi chiusi in

modo da evitare che, in assenza degli autorizzati, ne possano prendere visione i soggetti non autorizzati;

- 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, saranno 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 tra gli uffici dipartimentali, dovranno essere adottate idonee misure organizzative per salvaguardare la riservatezza dei dati personali (es. trasmissione dei documenti in cartelle, carpette o buste chiuse, ecc.);
- non devono essere riutilizzate copie fotostatiche di documenti contenenti dati personali, seppur non perfettamente riuscite, come carta da riciclo o da appunti;
- se si rende necessario trattare dati personali per telefono, si raccomanda di non parlare ad alta voce, soprattutto se si utilizzano telefoni cellulari, in presenza di terzi non autorizzati;
- in caso di eliminazione di documenti contenenti dati particolari (ex dati sensibili) o giudiziari, questi ultimi 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 all'utente;
- il nome utente e la password sono personali e non devono essere condivisi con altri soggetti (almeno 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;
- la password deve essere cambiata periodicamente;
- nel caso di cessazione del rapporto di lavoro, il dirigente responsabile dell'Ufficio deve chiedere la disattivazione dell'account presso qualunque sistema informativo utilizzato o server di rete e della mail aziendale gestita dall'ex dipendente;
- è vietato accedere ad un computer, alla rete o ad un sistema informativo utilizzando credenziali di altre persone;

- 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 non autorizzate per iscritto dal Titolare o dal Responsabile, di utilizzare gli strumenti informatici, personal computer o video terminali installati negli uffici;
- in caso di allontanamento dalla propria postazione di lavoro anche per la pausa caffè o pranzo, devono essere adottate 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;
- nei computer nei quali vengono utilizzati dati personali, ciascun dipendente deve 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 deve 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 deve tentare di acquisire privilegi di amministratore di sistema informatico;
- non si devono detenere chiavi di armadi o archivi ai quali non sia stato consentito l'accesso;
- non si può collegare modem o altro dispositivo che consenta un accesso non controllato alla rete informatica regionale senza apposita autorizzazione;
- il dipendente utilizza con consapevolezza gli strumenti informatici che sono di proprietà della Regione Siciliana. Essi devono essere utilizzati esclusivamente per rendere la prestazione lavorativa. Ogni dipendente è 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;
- è opportuno effettuare copie di sicurezza (backup) 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 potranno 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;
- 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, 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 l'altro, debba effettuarsi la trasmissione di categorie particolari di dati personali via mail, gli autorizzati dovranno 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 un'intestazione standardizzata in cui si avverta della eventuale riservatezza del messaggio;
- la navigazione su internet è 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.

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, i sub-Responsabili e il Referente privacy (dirigente responsabile dell'UO A1.06), 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 dellaviolazione dei dati personali (data breach)

Per "*data breach*" si intende 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.

Rientrano nella fattispecie gli eventi e i comportamenti atti a danneggiare i dati, a comprometterne la disponibilità o l'integrità indipendentemente da finalità o interventi fraudolenti, nonché gli incidenti avvenuti per fatti accidentali che compromettono l'integrità dei dati.

Fatti simili si verificano nella gestione e conservazione di dati con supporti informatici e tecnologici, ma assumono rilevanza quando la violazione dei dati personali presenta un rischio per i diritti e le libertà delle persone fisiche.

La corretta gestione del "*data breach*" ed in particolare la valutazione degli aspetti di rilevanza giuridica, organizzativa, tecnica e tecnologica, nonché quelli inerenti gli interventi posti in essere, hanno una notevole importanza per limitare le conseguenze sui diritti e le libertà personali degli interessati e per prevenire o evitare eventuali conseguenze di carattere economico-finanziario dovute a pretese risarcitorie e danni per l'Amministrazione regionale.

Sulla violazione di dati personaliil Regolamento UE 2016/679 stabilisce che il Titolare effettua la comunicazione al Garante della privacy e, qualora si presenti il rischio per i diritti e le libertà dell'interessato, informa quest'ultimo.

Nel caso di notifica all'Autorità, il modello da utilizzare è quello messo a disposizione dal Garante, disponibile anche nel sito della Regione Siciliana nella sezione del RPD: http://pti.regione.sicilia.it/portal/page/portal/PIR_PORTALE/PIR_LaStrutturaRegionale/PIR_PresidenzadellaRegione/responsabile-protezione-dati.

Il modello va compilato dal Titolare, assistito dal Responsabile del trattamento e con l'ausilio del Referente Privacy, sulla base delle informazioni fornite dal sub-Responsabile e dal sub-Responsabile tecnico che cura la eventuale gestione informatizzata dei dati e notificato dal all'Autorità di controllo entro 72 ore dal momento in cui la violazione è conosciuta.

Per ulteriori informazioni sull'argomento si rimanda alla sezione web dedicata: (link)

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO DEL DIPARTIMENTO

In adempimento al GDPR 2016/679 il Dipartimento dell'Agricoltura ha predisposto un registro delle attività di trattamento svolte dal Dipartimento sia per conto del Titolare – Assessore per l'Agricoltura, lo Sviluppo rurale e la Pesca mediterranea che, per quanto riguarda alcune attività inerenti il pagamento di contributi, per conto del Titolare - AGEA.

Tale 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.

Il registro è un documento in costante evoluzione e, pertanto, i dirigenti responsabili delle strutture intermedie hanno il compito di segnalare con tempestività, per la parte di specifica competenza, eventuali errori, modifiche e/o aggiornamenti da apportare.

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 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 quest'ultimo, entro il termine di 72 ore.

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 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.

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

Per gli approfondimenti si rimanda alla homepage del sito dipartimentale, sezione *AREE TEMATICHE → Altri contenuti →Privacy e sicurezza*e al sito istituzionale: http://pti.regione.sicilia.it/portal/page/portal/PIR_PORTALE/PIR_LaStrutturaRegionale/PIR_AssessoratoRegionaleAutonomieLocaliFunzionePubblica/PIR_PersonaleAffariGenerali/PIR_Areetematiche/PIR_Altricontenuti/PIR_PrivacyeSicurezza.

Palermo, 9 Giugno 2020

Il Dirigente Generale
f.to *Dario Cartabellotta*

VISTO
Si approva

L'Assessore
f.to Edgardo Bandiera