Direzione Generale

CIRCOLARE

Al Personale dipendente dell'Agenzia regionale per lo sviluppo rurale – ERSA

e p.c.
Ai Direttori delegati al trattamento

Oggetto: Istruzioni operative in materia di trattamento dei dati personali ai sensi degli articoli 29 e 32, paragrafo 4 del Regolamento generale sulla protezione dei dati (UE) 2016/679, nonché dell'articolo 2 *quaterdecies*, comma 2 del Decreto legislativo 196/2003 e del decreto del Direttore generale di ERSA del 2 febbraio 2024, n. 41.

PREMESSA

Il modello organizzativo dell'Agenzia regionale per lo sviluppo rurale - ERSA in materia di protezione dei dati personali, approvato con decreto del Direttore generale del 2 febbraio 2024, n. 41, in attuazione del Regolamento generale sulla protezione dei dati (UE) 2016/679 (GDPR), prevede che il Titolare del trattamento dei dati personali sia l'ERSA nel suo complesso, rappresentata dal Direttore generale in qualità di legale rappresentante dell'Ente. Il Titolare esercita le proprie funzioni per il tramite di soggetti delegati, come individuati dal suddetto decreto, i quali assicurano il rispetto degli obblighi previsti dal GDPR e dalla normativa nazionale posta in capo al Titolare del trattamento, esclusivamente per i trattamenti di dati personali connessi all'espletamento delle funzioni di competenza, individuate dalle rispettive declaratorie di funzioni e, dove possibile, in coerenza con la responsabilità del procedimento amministrativo.
L'articolo 2 *quaterdecies*, comma 2 del Decreto legislativo 196/2003 (Codice in materia di protezione di dati personali) prevede che il Titolare del trattamento individui le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.
All'interno di ERSA, in conformità al decreto n. 41/2024, tutti i dipendenti dell'Agenzia sono autorizzati al trattamento dei dati personali esclusivamente nell'ambito delle competenze della struttura di appartenenza; tale autorizzazione si considera contestuale al momento dell'assegnazione del dipendente alla propria struttura.
Gli articoli 29 e 32, par. 4 del GDPR richiedono che qualsiasi persona autorizzata al trattamento dei dati personali sotto l'autorità del Titolare sia debitamente informata e istruita al fine di mettere in atto comportamenti che assicurino l'adeguato livello di sicurezza e riservatezza, commisurato al valore del dato trattato e ai conseguenti rischi per la riservatezza.
Al fine di rispondere alle suddette esigenze di informazione ed istruzione, il presente documento contiene istruzioni operative riferite agli aspetti generali di comportamento che devono essere adottate nello svolgimento dei compiti e delle funzioni di competenza di ciascun dipendente autorizzato al trattamento di dati personali.

Esulano dal presente documento le istruzioni specifiche, che devono essere di volta in volta impartite dal Direttore delegato al trattamento, con particolare riferimento a quei trattamenti per i quali il dipendente viene specificamente autorizzato, in quanto riguardanti dati personali che richiedono una peculiare tutela, come le categorie particolari di dati personali, i dati giudiziari o quelli relativi a particolari situazioni di disagio economico, sociale e familiare.

ISTRUZIONI

In ottemperanza alle disposizioni della normativa sulla protezione dei dati personali ed in relazione alle attività svolte nell'ambito della struttura di appartenenza, la persona autorizzata al trattamento dei dati personali deve effettuare i trattamenti di competenza attenendosi scrupolosamente alle istruzioni contenute nel presente documento e ad ogni ulteriore indicazione, fornita dal Titolare o da suo delegato. In generale, nell'assolvimento dei compiti attribuiti, l'Autorizzato deve ottemperare a quanto segue:

1. GARANTIRE I PRINCIPI DEL TRATTAMENTO DEI DATI PERSONALI (articolo 5 GDPR)

- conformarsi ai seguenti principi generali nelle operazioni di trattamento dei dati:
  - liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;
  - necessità e minimizzazione dei dati: i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento; il trattamento di dati personali deve essere ridotto strettamente al minimo indispensabile; ciascun autorizzato deve avere accesso soltanto ai dati personali necessari all'esercizio delle proprie funzioni e competenze;
  - esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
  - limitazione della conservazione: è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
  - integrità e riservatezza: garantire la sicurezza adeguata dei dati personali oggetto del trattamento;
  - principio di responsabilizzazione o accountability: trattare i dati personali rispettando le misure tecniche e organizzative messe in atto dal Titolare del trattamento ai sensi dell'articolo 5, par. 2 e dell'articolo 24, par. 1 del GDPR, per i quali "il Titolare 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";
- trattare i dati personali per finalità determinate, esplicite, legittime e compatibili all'esecuzione delle proprie funzioni o dei compiti affidati;
- trattare i dati personali in modo lecito, ai sensi dell'articolo 6 del GDPR. Si precisa che di norma l'Agenzia tratta dati personali per adempiere ad un obbligo legale o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (articolo 6, par. 1, lettere c) ed e) del GDPR);
- assicurarsi che il trattamento effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, si fondi su una idonea base giuridica, ai sensi dell'articolo 2 *ter* del Codice in materia di protezione di dati personali (norma di legge o di regolamento o atto amministrativo generale);

2. ASSICURARE LA TRASPARENZA DEL TRATTAMENTO: INFORMATIVA (articoli 12, 13 e 14 GDPR)

- fornire l'informativa ai sensi degli articoli 13 e 14 del GDPR.

L'informativa deve essere messa a disposizione degli interessati (ad esempio tramite la pubblicazione nella pagina dedicata al singolo trattamento, presente sul sito istituzionale dell'Agenzia), il cui contenuto

minimo corrisponde ai modelli di informativa privacy disponibili nella sezione "Trattamento dati personali" del sito istituzionale (https://www.ersa.fvg.it/cms/hp/trattamento_dati_personali/index.html);

3. GARANTIRE L'ESERCIZIO DEI DIRITTI DEGLI INTERESSATI (articoli 12 e 15-21 GDPR)
• garantire l'esercizio dei diritti degli interessati, quali il diritto di accesso ai propri dati, il diritto di rettifica, il diritto di cancellazione (diritto all'oblio), il diritto di limitazione del trattamento, il diritto alla portabilità dei dati e il diritto di opposizione, laddove esercitabili, dandone informazione al Responsabile per la protezione dei dati dell'Agenzia per il tramite del Referente privacy dell'Agenzia;

4. PROPORRE LA NOMINA DEL RESPONSABILE ESTERNO DEL TRATTAMENTO (articolo 28 GDPR)
• nel caso in cui il trattamento dei dati personali venga attuato da un soggetto esterno a cui è stata delegata un'attività dell'Agenzia (ad esempio, tramite apposita Convenzione) o con il quale è stato stipulato un contratto, proporre al Direttore delegato al trattamento, nella sua qualità di soggetto delegato con specifici compiti di assistenza al Titolare, di nominare tale soggetto responsabile esterno del trattamento. Il modello di nomina a responsabile esterno è disponibile nella sezione "Trattamento dati personali" del sito istituzionale sopra indicata;

5. ADEMPIMENTI CONNESSI AL REGISTRO DEI TRATTAMENTI (articolo 30 GDPR)
• con riferimento ai trattamenti di competenza, adempiere alle richieste di aggiornamento periodico del Registro dei trattamenti di titolarità dell'ERSA trasmesse dal Referente privacy dell'Agenzia, oppure, al di là di dette richieste, trasmettere autonomamente al Referente medesimo i dati aggiornati da inserire nel Registro (articolo 30, par. 1 del GDPR);
• nel caso in cui il proprio Direttore sia stato nominato responsabile del trattamento relativamente a un contratto o ad una convenzione stipulati dal medesimo Direttore, occorre:
  – compilare il registro del responsabile dei trattamenti relativo al contratto o alla convenzione stipulati. In tal caso, il registro del responsabile del trattamento viene redatto secondo il modello disponibile nella sezione "Trattamento dati personali" del sito istituzionale;
  – comunicare al Referente privacy dell'Agenzia la nomina a Responsabile del trattamento del proprio Direttore, al fine di consentire al Referente medesimo di procedere con gli adempimenti di competenza;

6. RISPETTARE LE MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE (articolo 32 GDPR)
• rispettare le misure di sicurezza attuate dal Titolare del trattamento o dal Direttore delegato al trattamento per garantire l'integrità, la riservatezza e la disponibilità dei dati, idonee ad assicurare un livello di sicurezza adeguato al rischio del trattamento, con l'obiettivo di evitare distruzione accidentale o illecita, perdita, modifica, rivelazione, accesso non autorizzato;
• rispettare le seguenti prescrizioni per il trattamento di dati personali con strumenti cartacei:
  – non conservare fascicoli o documenti contenenti dati personali in locali accessibili a personale non autorizzato alla visione di tali dati, senza l'uso di armadi o cassettiere chiusi con opportuna serratura;
  – i documenti contenenti dati personali sono portati fuori dai locali individuati per la loro conservazione solo per specifiche esigenze d'ufficio e, nel caso ciò avvenga, l'esportazione è ridotta al tempo minimo necessario per effettuare le operazioni di trattamento;

• rispettare le prescrizioni contenute nel decreto del Direttore generale di ERSA del 13 marzo 2020, n. 17 "Adozione delle Regole per l'utilizzo di strumentazioni informatiche"; in particolare, è compito del dipendente assegnatario di dispositivi informatici:
  - utilizzare in modo appropriato e responsabile i dispositivi hardware e software assegnati;
  - assicurare periodicamente il salvataggio dei dati nelle specifiche aree di archiviazione della rete regionale messe a disposizione del dipendente e della struttura di appartenenza;
  - non installare in autonomia software non compresi nell'elenco di quelli autorizzati per non pregiudicare la funzionalità del dispositivo o compromettere la riservatezza dei dati in esso contenuti;
  - rispettare le procedure di autenticazione e di gestione delle password;
  - in caso di allontanamento temporaneo dal proprio posto di lavoro è fatto obbligo al dipendente di utilizzare la procedura standard del sistema operativo di "blocca computer";
  - impostare e utilizzare il blocco automatico dello schermo del dispositivo dopo un predefinito periodo di inattività;
  - adottare adeguate misure di sicurezza nel caso di utilizzo dei beni al di fuori delle sedi dell'ERSA;
  - proteggere l'accesso al proprio account sul dispositivo con password;
• porre all'attenzione del Titolare, per il tramite del Direttore delegato al trattamento, i trattamenti di dati personali riguardanti dati che richiedono una peculiare tutela, come le categorie particolari di dati personali (articolo 9 del GDPR), i dati giudiziari (articolo 10 del GDPR) o quelli relativi a particolari situazioni di disagio economico, sociale e familiare, per i quali sono necessari un distinto atto autorizzatorio e istruzioni specifiche;
• custodire e controllare i dati oggetto del trattamento, rispettare la massima riservatezza e discrezione nella gestione dei dati, realizzando ogni attività necessaria ad evitare i rischi, anche accidentali, di distruzione o perdita, di divulgazione o accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
• non condividere, comunicare o trasmettere i dati personali trattati a persone non autorizzate al trattamento;
• alla cessazione dell'attività lavorativa non utilizzare le autorizzazioni ancora in essere e comunicare ai propri diretti responsabili le eventuali de-registrazioni da effettuare;

7. INFORMARE IL DIRETTORE DELEGATO AL TRATTAMENTO DI UNA VIOLAZIONE DEI DATI PERSONALI (articolo 33 GDPR)
• in caso di violazioni di dati personali o di incidente di sicurezza che coinvolga dati personali – costituiti a titolo esemplificativo da distruzione di dati digitali o documenti cartacei; perdita di dati conseguente a smarrimento/furto di supporti o di documentazione; rilevamento di modifica non autorizzata di dati; divulgazione di dati e documenti a soggetti terzi non legittimati; accesso non autorizzato a sistemi IT – informare tempestivamente il proprio Direttore ai sensi delle prescrizioni contenute nel decreto del Direttore generale sostituto del 29 marzo 2021, n. 25 (Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, articolo 33. Notifica di una violazione dei dati personali all'Autorità di controllo. Approvazione delle "Linee guida per la notifica della violazione dei dati personali "Data Breach" per gli uffici dell'Agenzia regionale per lo sviluppo rurale – ERSA".);

8. PROPORRE LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (articolo 35 GDPR)

• laddove necessario, proporre al Titolare, per il tramite del Direttore delegato al trattamento, di effettuare la valutazione di impatto ai sensi dell'articolo 35 del GDPR, in particolare nel caso in cui il trattamento possa comportare un rischio elevato per i diritti e le libertà delle persone interessate, nei casi individuati dall'articolo 35, par. 3 e dai Considerando 89, 90, 91 del GDPR nonché sulla base di quanto indicato dal Garante privacy nel Provvedimento n. 467 del 2018. Per l'elaborazione della valutazione di impatto si rinvia al software consigliato dall'Autorità Garante della privacy scaricabile dal seguente link: https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil;

9. REDIGERE GLI ATTI NEL RISPETTO DELLA PROTEZIONE DEI DATI

• adottare, fin dalla redazione degli atti, tutte le cautele necessarie per evitare un trattamento di dati personali non lecito, specialmente laddove l'atto debba essere poi diffuso o comunicato ad altri soggetti. Pertanto, occorre minimizzare l'esposizione di dati personali (trattasi di dati personali relativi ai titolari di aziende individuali oppure liberi professionisti selezionati per l'affidamento di servizi o di qualunque altra persona fisica i cui dati sono oggetto di trattamento per quanto di competenza) omettendo nel testo degli atti dati personali non pertinenti o necessari rispetto alle finalità del trattamento;

• con specifico riferimento alla redazione di provvedimenti di concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici laddove possibile indicare soltanto il beneficiario, il capitolo e l'importo, mentre non devono essere indicati i dati eccedenti (quali, a titolo esemplificativo, il codice fiscale del beneficiario persona fisica, l'IBAN, i recapiti personali, la residenza). Tali informazioni, se necessarie, sono contenute nell'allegato contabile, che è parte integrante del decreto medesimo e non è oggetto di pubblicazione;

10. ADOTTARE PARTICOLARI CAUTELE IN CASO DI DIFFUSIONE E COMUNICAZIONE DEI DATI PERSONALI

• laddove sia prevista la diffusione (ad es. pubblicazione per finalità di trasparenza o pubblicità legale) o la comunicazione dei dati personali ad altri soggetti, accertare l'esistenza di un'idonea base giuridica, ai sensi dell'articolo 2 *ter* del Codice in materia di protezione di dati personali (norma di legge o di regolamento o atto amministrativo generale), nonché assicurare anche in tal caso il rispetto del principio di minimizzazione, omettendo i dati personali non pertinenti o necessari rispetto alle finalità del trattamento;

• in caso di diffusione o comunicazione di atti per i quali sia necessario procedere all'oscuramento di parti del testo, contenenti dati personali non pertinenti o necessari, è indispensabile intervenire sul documento in word e sostituire i dati da omettere con una serie di XXXXXX. Laddove il documento fosse in formato PDF, si ricorda che il mero oscuramento di parti di testo effettuato sul documento non è definitivo, infatti la parte oscurata, se copiata e incollata in word, restituisce in chiaro quanto oscurato. In questo caso è possibile richiedere l'installazione di apposito applicativo tramite CRM per effettuare un oscuramento definitivo;

• con specifico riferimento alla pubblicazione di atti effettuato per finalità di pubblicità e trasparenza sul sito web istituzionale, rispettare le indicazioni fornite nelle "Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati", adottate dal Garante per la protezione dei dati personali con Provvedimento n. 243/2014, disponibile nella sezione privacy del sito istituzionale;

11. ADOTTARE PARTICOLARI CAUTELE NELLA TRASMISSIONE DI MAIL

• ogni qualvolta si trasmette una comunicazione via e-mail a più destinatari con un'unica azione, è necessario porre attenzione alla presenza di dati personali nel contenuto della comunicazione e nei suoi allegati. Speciale attenzione va posta nel caso in cui si tratti di categorie particolari di dati personali o dati giudiziari (articoli 9 e 10 del GDPR). Laddove la comunicazione o i documenti allegati contengano dati personali non è possibile procedere con l'invio unico a più destinatari, ma è necessario inviare l'e-mail a ciascun destinatario separatamente;

• ogniqualvolta si voglia trasmettere una mail a più destinatari con un'unica azione, anche se il suo contenuto è privo di dati personali, deve essere utilizzato lo strumento della copia conoscenza nascosta (CCN), al fine di mantenere gli indirizzi dei destinatari riservati, in quanto l'indirizzo e-mail è già di per sé un dato personale. Quest'ultima avvertenza non si applica per le comunicazioni di lavoro che avvengono all'interno dell'Agenzia, in quanto gli indirizzi mail istituzionali dei dipendenti sono dati personali già conosciuti all'interno dell'ente;

12. "SCRIVANIA PULITA"

• adottare una politica di pulizia per le postazioni di lavoro di computer e stampanti, in modo tale da garantire che tutte le informazioni sensibili e riservate, siano esse cartacee, su un dispositivo di archiviazione o su un dispositivo hardware, siano adeguatamente chiuse a chiave o smaltite quando la postazione di lavoro non è in uso. In particolare, è compito di ciascun dipendente:

- rimuovere dalla scrivania, a fine giornata, tutti i documenti sensibili e conservarli in un cassetto, armadio o altre forme di protezione chiuse a chiave;
- smaltire i documenti cartacei contenenti informazioni sensibili con gli appositi strumenti di smaltimento;
- utilizzare, ove possibile, stampanti con l'inserimento delle credenziali di accesso per la protezione dei documenti; in caso contrario, rimuovere quanto prima i documenti contenenti informazioni sensibili dalla stampante;

13. PARTECIPARE ALLA FORMAZIONE DEDICATA

• partecipare costantemente all'attività di formazione proposta in materia di privacy e protezione dei dati personali.

Per gli autorizzati al trattamento operanti presso la UOS OPR FVG, resta fermo, infine, anche quanto altro disposto dal Direttore dell'OPR FVG in materia di Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

Tutti gli autorizzati sono chiamati ad applicare ed attenersi scrupolosamente alle presenti istruzioni, impartite ai sensi delle normative vigenti in materia di trattamento dei dati personali.

Il Direttore Generale sostituto
dott. Francesco Miniussi
sottoscritto digitalmente
ai sensi del D.Lgs. 82/2005 e s.m.i.