



Linee guida

ai sensi del

Regolamento UE 2016/679

*ad uso del personale
del Comando del Corpo forestale*

Il **Regolamento** concerne la “tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati” e disciplina i trattamenti di dati personali, sia nel settore privato, sia nel settore pubblico.

SI APPLICA al trattamento automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

NON SI APPLICA, tra l'altro, al trattamento di dati personali effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

«dato personale»

permette l'identificazione fisica di una persona direttamente (dati anagrafici, nome e cognome, sesso, immagine) o indirettamente (numero di identificazione, codice fiscale, indirizzo IP, numero di targa, dati relativi a ubicazione, IBAN, identificativo online), c.d. “**comuni**”;

può rientrare in particolari categorie, c.d. “sensibili” (origine razziale od etnica, convinzioni religiose, filosofiche, opinioni politiche, appartenenza sindacale, dati relativi alla salute o alla vita sessuale, dati genetici e biometrici);

relativo a condanne penali e reati, c.d. “giudiziari”, che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti a iscrizione nel casellario giudiziale o la qualità di imputato o di indagato, ivi compresi i dati relativi a condanne penali e reati o connessi a misure di

«trattamento»

qualsiasi operazione compiuta con o senza ausilio di processi automatizzati e applicata a dati personali: **raccolta, registrazione, organizzazione, strutturazione, conservazione, modifica, estrazione, consultazione, uso, comunicazione**, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, **cancellazione** o distruzione.

«interessato»

è la persona fisica alla quale si riferiscono i dati personali.

**Diritto di accesso ai propri dati
Diritto all'oblio
Diritto di limitazione**

NON si applicano alle società le norme sulla protezione dei dati personali. Tuttavia, le informazioni relative a imprese individuali possono costituire dati personali se consentono l'identificazione di una persona fisica.

Trattamento dei DATI PERSONALI

Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano, come riconosciuto dall'articolo 8 della **Carta** dei diritti fondamentali dell'Unione europea e dall'articolo 16 del **Trattato** sul funzionamento dell'Unione europea.

Principi applicabili al trattamento dei dati personali (articolo 5 del regolamento)

«**liceità, correttezza e trasparenza**»: devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;

«**limitazione della finalità**»: devono essere raccolti per finalità determinate, esplicite e legittime;

«**minimizzazione dei dati**»: devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

«**esattezza**»: devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

«**limitazione della conservazione**»: devono essere 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;

«**integrità e riservatezza**»: devono essere trattati in maniera da garantire un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Fondamenti di liceità del trattamento

(articolo 6 del regolamento)

Ogni trattamento di dati personali deve trovare fondamento in un'adeguata base giuridica.

Esso è lecito quando si verifica almeno una delle seguenti condizioni.

Consenso dell'interessato

Deve essere, in tutti i casi, **libero, specifico, informato e inequivocabile**. Non è ammesso il consenso tacito o presunto.

Deve essere manifestato attraverso “dichiarazione o azione positiva inequivocabile”; a tal fine la “forma scritta” è una modalità idonea.

La richiesta di consenso deve essere **chiaramente distinguibile** da altre richieste o dichiarazioni e la formula utilizzata comprensibile, semplice, chiara.

L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento.

La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca.

Nel caso di “**dati sensibili**” il consenso deve essere “esplicito”, come anche per i trattamenti automatizzati, compresa la profilazione.

Per approfondimenti: Linee guida 5/2020 del Comitato europeo per la protezione dei dati (EDPB) sul consenso.

Adempimento di obblighi contrattuali

Obblighi di legge cui è soggetto il titolare

Interesse pubblico o esercizio di pubblici poteri da parte del titolare

Salvaguardia degli interessi vitali della persona interessata o di terzi

L'interesse vitale di un terzo si può invocare quale base giuridica solo nel caso in cui nessuna delle altre condizioni di liceità trovi applicazione.

«TITOLARE del trattamento» del Comando del Corpo forestale:

Assessore del Territorio e dell'Ambiente - Determina le finalità e i mezzi del trattamento.

«RESPONSABILE del trattamento» del Comando del Corpo forestale:

Dirigente Generale - Tratta i dati personali per conto del titolare, mediante sub-responsabili e autorizzati.

La sicurezza dei dati personali

(articoli 32-34 del regolamento)



Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

misure di protezione dati

Si distinguono misure **tecniche** e **organizzative** adeguate per garantire un livello di sicurezza adeguato al rischio.

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

Essendo un'operazione di de-identificazione reversibile, il dato potrà essere ricostruito, a differenza del dato anonimo. Non è una misura di sicurezza a sé stante, ma va inserita nel complesso delle misure adottate per garantire la sicurezza dei dati.

requisiti di sicurezza

- a) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- b) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- c) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

La violazione dei dati personali (articolo 4 del regolamento)

Data breach è 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. Può essere un evento doloso (un attacco informatico), o accidentale (un accesso abusivo, un incidente, la perdita di una chiavetta USB, un malfunzionamento hardware o software). In caso di violazione dei dati personali, dovrà essere effettuata una valutazione del rischio, cioè dei possibili effetti, in considerazione della natura, sensibilità e volume dei dati personali violati, del numero degli interessati, del 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. Qualora si ravvisi un rischio alle libertà personali della persona a cui si riferiscono i dati, sarà necessario informare prontamente il Responsabile del trattamento, per il tramite dei Sub-Responsabili del Comando del Corpo forestale.

È VIETATO A TUTTI I DIPENDENTI

- accedere ad un computer, alla rete o ad un sistema informativo, utilizzando credenziali di altri, nonché la consultazione di documenti assegnati su IRIDE ad altri dipendenti.

- installare ed eseguire 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.

Ciascun dipendente deve adottare tutte le accortezze e precauzioni, in caso di allontanamento dalla propria postazione di lavoro, al fine di impedire l'accesso fisico a chi non è legittimato, esterno all'amministrazione o interno non specificamente autorizzato. Deve, inoltre, spegnere fisicamente il computer alla fine della sessione di lavoro e porre particolare attenzione ai programmi e ai servizi online utilizzati sul proprio pc, al fine di escludere la diffusione, anche involontaria, di dati personali ai quali ha avuto accesso in ragione delle autorizzazioni ricevute.



Privacy e Trasparenza

Prima della pubblicazione di un documento che contiene dati personali **verificare** l'esistenza di una specifica **norma di legge** o regolamento che prevede la **pubblicazione**.

SE ESISTE si deve distinguere la natura di dati personali oggetti di diffusione.

DATI COMUNI

Selezionare i dati personali da pubblicare, rispettando i **principi di necessità, di pertinenza e di non eccedenza**:

è consentita la diffusione dei soli dati personali realmente necessari e proporzionata alla finalità di **Trasparenza**.

I dati personali oggetto di pubblicazione devono essere esatti, aggiornati e contestualizzati.

Controllare l'attualità delle informazioni/dati pubblicati nel sito, modificarle opportunamente, a seguito di controllo o nel caso in cui l'interessato ne richieda l'aggiornamento o la rettifica.

In caso di presenza nel documento di **dati o informazioni personali ulteriori** la pubblicazione è legittima solo procedendo all'**anonimizzazione**, oscurando del tutto il nominativo e le altre informazioni riferite all'interessato che possono consentire l'identificazione anche a posteriori. **NO** anonimizzazione con iniziali, di nome e cognome.

DATI SENSIBILI E GIUDIZIARI

Si applica il **principio della indispensabilità del trattamento**: dati sensibili e giudiziari possono essere diffusi solo se indispensabili per raggiungere la finalità della pubblicazione.

SE NON ESISTE è necessario anonimizzare i dati personali per rendere legittima la pubblicazione.

EVITARE IL TRATTAMENTO QUANDO LE FINALITÀ PERSEGUITE POSSONO ESSERE REALIZZATE MEDIANTE DATI ANONIMI.

Vita sessuale

Divieto di diffusione per finalità di trasparenza.

Stato di salute

Divieto assoluto di diffusione.

RIDURRE AL MINIMO L'UTILIZZAZIONE DI DATI PERSONALI E IDENTIFICATIVI.

La **denominazione** di un documento soggetto a pubblicazione non deve contenere dati personali.

*I documenti, le informazioni e i dati oggetto di **pubblicazione obbligatoria** ai sensi della normativa vigente, sono pubblicati in **formato di tipo aperto** (".txt" - ".pdf" - ".xml"), che favorisce la circolazione dei dati; questi sono riutilizzabili senza ulteriori restrizioni diverse dall'obbligo di citare la fonte e di rispettarne l'integrità.*

DATI A SCADENZA

"In ogni informativa sulla privacy dovrà essere specificato il tempo entro il quale il dato sensibile andrà trattato, scaduto il quale il trattamento diventerà illegittimo".

Obblighi di pubblicazione dei curricula professionali

NO alla diffusione di tutti i contenuti previsti dal modello europeo, ma solo di quelli pertinenti rispetto alle finalità di trasparenza perseguite, ovvero le informazioni riguardanti i titoli di studio e professionali, le esperienze lavorative e ulteriori informazioni di carattere professionale (conoscenze linguistiche, competenze nell'uso delle tecnologie, partecipazione a convegni, redazione di pubblicazioni).