



PROVINCIA DI FERMO

GDPR

<https://www.provincia.fermo.it/gdpr>

## Newsletter

# Trattamento dati personali

n. 1/2024

Aggiornamenti giuridici e pratici attinenti al trattamento dei dati personali in conformità al Regolamento UE 679/2016 e al D. Lgs 196/2003, come aggiornato dal D. Lgs. 101/2018.

### Approfondimento 🔍

Nel Regolamento UE 2016/69, uno dei principi più importanti è quello della “**privacy by design**” e della “**privacy by default**”.

Cosa si intende con i due termini?

Con riferimento agli Enti Locali, e in genere agli Enti Pubblici, il principio di **privacy by design** (o meglio di protezione dei dati fin dalla progettazione) comporta che le Amministrazioni, quando intendono affidare in appalto un servizio (ad es. un servizio sociale) o anche procedere all'appalto di una fornitura, devono richiedere e verificare che quel servizio e/o quel prodotto sia stato progettato e venga eseguito nel rispetto dei dati personali che saranno trattati.

Il principio di **privacy by design** comporta dunque che l'Ente non si limiti a verificare le misure di sicurezza adottate dall'operatore economico che sarà deputato a svolgere un determinato servizio per conto dell'Ente, ma che lo stesso Ente, nel progettare il servizio pubblico, tenga conto delle esigenze di tutela dei dati personali.

Pertanto, a titolo strettamente dimostrativo, nel progettare un servizio deve essere definita, ad esempio:

- la minimizzazione dei dati: il servizio deve essere gestito raccogliendo solo i dati strettamente necessari al servizio offerto e non dati eccedenti, a meno che in tal caso si richieda il consenso espresso al destinatario del servizio.
- la limitazione dello scopo: utilizzare i dati raccolti solo per gli scopi dichiarati e non per altri fini. Se i dati (per esempio elenco di nominativi o anche indirizzi mail) sono raccolti da



un servizio (ad es. servizio di tipo sociale) non possono poi essere utilizzati da altri uffici per scopi diversi (ad es. dall'Ufficio Tributi).

Per **privacy by default** si intendono le misure tecniche con le quali il Titolare del trattamento, **per impostazione predefinita, tratta esclusivamente i dati personali necessari per la specifica finalità del trattamento e per il periodo strettamente necessario, garantendo la non eccessività di tutti i dati raccolti.**

Il principio di **privacy by default**, quindi, prevede un'impostazione predefinita del trattamento dei dati: vale a dire l'adozione di automatismi e procedure che appunto, di default, riducono le possibilità di data breach\* e conseguenti rischi per l'interessato. In tal senso diventa importante l'adozione di un Regolamento sul trattamento dei dati e, soprattutto, la formazione specifica di tutto il personale che tratti i dati.

*\*Data Breach: Una 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.*

---

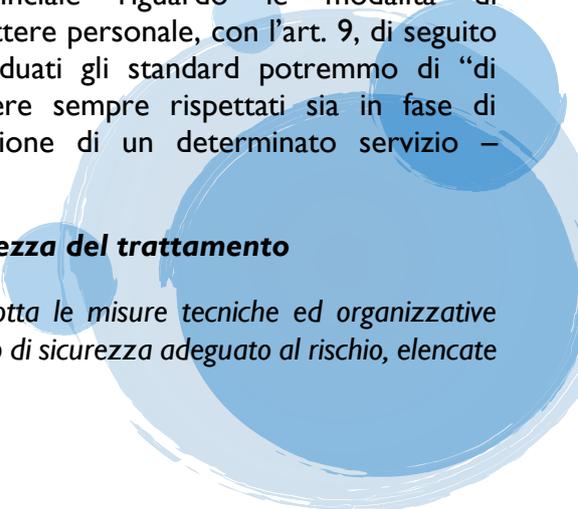
## FOCUS

Proprio in riferimento a quanto sopra, e in particolare al concetto di **privacy by default**, si ricorda che l'Ente, con decreto presidenziale n. 23 del 28/11/2019, ha adottato il "**Regolamento per la protezione dei dati personali**", consultabile sulla home page del sito istituzionale dell'Ente ed in ogni caso al link <https://www.provincia.fermo.it/public/2019/12/13/regolamento-per-il-trattamento-dei-dati-personali.pdf>

Nell'ambito di tale Regolamento, con il quale sono disciplinate le misure organizzative, procedurali e tecnologiche prescelte dall'Amministrazione Provinciale riguardo le modalità di trattamento dei dati di carattere personale, con l'art. 9, di seguito riportato, sono stati individuati gli standard potremmo di "di default" che debbono essere sempre rispettati sia in fase di progettazione che di gestione di un determinato servizio – fornitura.

### **Art. 9 Sicurezza del trattamento**

*1. La Provincia di Fermo adotta le misure tecniche ed organizzative necessarie a garantire un livello di sicurezza adeguato al rischio, elencate*





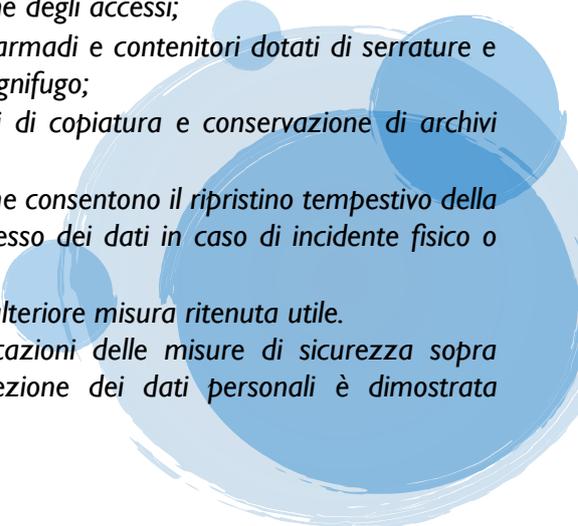
*in modo non tassativo al comma 2 del presente articolo, tenendo conto dello stato dell'arte, dei costi di attuazione, nonché della natura, del 12 Regolamento protezione dati personali campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.*

*2. Le misure tecniche ed organizzative di sicurezza adottate dalla Provincia di Fermo per ridurre i rischi del trattamento ricomprendono, in via generale: – la pseudominimizzazione: conservazione e pubblicazione dei dati in una forma che impedisca l'identificazione del soggetto interessato senza l'utilizzo di informazioni aggiuntive, conservate separatamente e soggette a misure tecniche e organizzative che garantiscano la non attribuibilità ad una persona fisica identificata o identificabile; – la minimizzazione: utilizzo dei soli dati personali assolutamente indispensabili rispetto al trattamento da effettuare; – la cifratura: se il trattamento prevede la gestione di dati ultrasensibili, il Segretario Generale o il competente Dirigente valuta l'opportunità di innalzare il livello di sicurezza attraverso l'adozione della tecnica di crittografia, vale a dire il processo volto a impedire la leggibilità in chiaro di un testo a chi non abbia il sistema di cifratura e la chiave per decifrare il testo stesso, anch'esso conservato separatamente; – la capacità di assicurare la continua riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali; – la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; – possibilità di verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative adottate al fine di garantire la sicurezza del trattamento.*

*3. Costituiscono ulteriori misure tecniche ed organizzative che possono essere adottate dall'Ente:*

- l'utilizzo di sistemi di autenticazione;*
- l'utilizzo di sistemi di autorizzazione;*
- l'utilizzo e l'aggiornamento di sistemi di protezione delle banche dati telematiche (antivirus, firewall, antintrusione, altro);*
- la predisposizione di idonee misure antincendio;*
- l'utilizzo di sistemi di rilevazione di intrusione, di sorveglianza e l'eventuale registrazione degli accessi;*
- la presenza di porte, armadi e contenitori dotati di serrature e costruite in materiale ignifugo;*
- la presenza di sistemi di copiatura e conservazione di archivi elettronici;*
- l'adozione di misure che consentono il ripristino tempestivo della disponibilità e dell'accesso dei dati in caso di incidente fisico o tecnico;*
- l'applicazione di ogni ulteriore misura ritenuta utile.*

*4. La conformità delle applicazioni delle misure di sicurezza sopra elencate in materia di protezione dei dati personali è dimostrata*



attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato. 13 Regolamento protezione dati personali

5. Il Titolare, il Segretario Generale ed i Dirigenti autorizzati al trattamento nonché l'Amministratore del sistema informatico e il RPD provvedono, per quanto di rispettiva competenza, a impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.



## FORMAZIONE OBBLIGATORIA:

Si ricorda che il rispetto della disciplina concernente il trattamento dei dati personali rende ineludibile una adeguata formazione. L'art. 29 del Regolamento UE 2016/679 prevede infatti che chi abbia accesso a dati personali "non può trattare tali dati se non è istruito in tal senso".

In considerazione di quanto sopra si riportando di seguito le credenziali con le quali accedere alla piattaforma telematica "All Privacy – Entionline" e fruire gratuitamente dei corsi di formazioni presenti:

**INDIRIZZO:** <https://www.entionline.it/>

**USER NAME:** prfermo-fpy-2

**PASSWORD:** FORMAZIONEFERMO

Per attivare il video corso seguire il seguente percorso:

- > selezionare il bottone di colore arancione in alto a sinistra "I tuoi servizi";
- > selezionare il bottone di colore azzurro posizionato sulla destra dello schermo "Formazione privacy 2022";
- > scegliere la proposta formativa che si desidera visionare. Si consiglia di partire dai seguenti corsi:
  - ❖ Formazione privacy 2022 – Corso generale per i nuovi dipendenti parte I e II
  - ❖ Formazione privacy 2022 – Corso generale per i nuovi dipendenti parte III e IV.

Al termine di ogni corso sarà possibile, previo superamento di un test di verifica, scaricare l'attestato di frequenza che si invita a trasmettere al Servizio Risorse Umane ai fini dell'acquisizione al fascicolo personale.