oltrecode

Privacy · Cybersecurity · Trasformazione digitale per la PA

OTTOBRE IN WEBINAR 2026 · DISPENSA

Incontro 1
Il GDPR

Principi, obblighi e governance della compliance

Data	Martedì 27 ottobre 2026
Orario	9.00 – 11.00, in diretta
Relatore	Marco La Diega, fondatore di OltreCode

Questa dispensa riassume i contenuti del primo incontro: da dove nasce la privacy, che cosa dice il GDPR e chi risponde di che cosa. Non serve essere giuristi per applicarla: serve capire il perché delle regole.

> La maggior parte degli errori in materia di privacy non nasce da cattiva volontà, ma da gesti quotidiani fatti senza accorgersene. Tieni la dispensa a portata di mano: i suoi contenuti sono anche oggetto del **test finale di venerdì 30 ottobre**.

1 Dalla Kodak al GDPR

La privacy nasce da un fatto di vita quotidiana, non da un adempimento burocratico: ogni volta che arriva una nuova tecnologia, nasce il bisogno di proteggere la persona.

Anno	Tappa	Perché conta
1888	Kodak lancia la prima macchina fotografica portatile alla portata di tutti	Per la prima volta chiunque può fotografare chiunque, anche a sua insaputa
1890	Warren e Brandeis pubblicano *The Right to Privacy* sulla Harvard Law Review	Nasce il diritto di essere lasciati soli, come reazione a fotografi e stampa
1948–1950	Dichiarazione universale dei diritti dell'uomo; Convenzione europea dei diritti dell'uomo (art. 8)	La vita privata entra tra i diritti fondamentali
1981	Convenzione 108 del Consiglio d'Europa	Primo trattato vincolante sulla protezione dei dati trattati dai computer
1995	Direttiva 95/46/CE	Prima disciplina europea, ma ogni Stato la recepisce a modo suo
1996–2003	Legge 675/1996, poi Codice privacy (D.lgs. 196/2003)	La protezione dei dati arriva in Italia
2000	Carta dei diritti fondamentali UE (art. 8)	La protezione dei dati diventa un diritto autonomo
2016–2018	Regolamento (UE) 2016/679 (GDPR), applicabile dal 25 maggio 2018; Codice privacy aggiornato dal D.lgs. 101/2018	Regole uniformi in tutta Europa

> Cambia la tecnologia (foto, smartphone, social, telecamere, intelligenza artificiale), non il principio: **la persona viene prima del dato.**

2 Dato personale e trattamento

> **Anche solo guardare un dato sullo schermo è un trattamento.** Chi consulta un dato senza un motivo di lavoro sta già violando le regole.

- **Dato personale (art. 4 GDPR)** — qualsiasi informazione su una persona fisica identificata o *identificabile*. Non serve il nome: bastano codice fiscale, email, targa, indirizzo IP, foto, voce, posizione geografica.
- **Categorie particolari (art. 9)** — salute, origine razziale o etnica, opinioni politiche, convinzioni religiose, appartenenza sindacale, dati genetici e biometrici, vita sessuale. Regole più rigide: qui l'errore costa di più.
- **Dati su condanne penali e reati (art. 10)** — trattabili solo se una norma lo prevede.
- **Trattamento** — qualsiasi operazione sui dati, anche su carta: raccolta, registrazione, organizzazione, conservazione, consultazione, comunicazione, diffusione, cancellazione.

Esempi quotidiani nella PA e nelle aziende: anagrafe, protocollo, pratiche del personale, cartelle sanitarie, videosorveglianza, albo pretorio.

3 I principi del trattamento (art. 5 GDPR)

Sette principi reggono tutto il GDPR: ogni trattamento deve rispettarli tutti, sempre.

Principio	In una frase	Errore tipico
Liceità, correttezza e trasparenza	Serve una base giuridica (art. 6) e l'interessato deve sapere cosa succede ai suoi dati	Informativa assente o generica
Limitazione della finalità	I dati raccolti per uno scopo non si riusano per scopi incompatibili	Usare l'elenco dei contribuenti per fini promozionali
Minimizzazione	Solo i dati necessari	Chiedere documenti o campi inutili nei moduli
Esattezza	Dati corretti e aggiornati	Anagrafiche non allineate tra uffici
Limitazione della conservazione	Non oltre il tempo necessario	Archivi tenuti per sempre "per sicurezza"; atti lasciati sull'albo oltre i 15 giorni

Principio	In una frase	Errore tipico
Integrità e riservatezza	Misure di sicurezza tecniche e organizzative	Password condivise, documenti sulla scrivania, email al destinatario sbagliato
Responsabilizzazione (accountability)	Il Titolare deve poter dimostrare il rispetto di tutti gli altri principi	Regole rispettate ma non documentate

4 Accountability e governance

> **Se non è documentato, davanti al Garante non è successo.** Non basta rispettare le regole: bisogna poterlo dimostrare con documenti, procedure, formazione e controlli.

- **Il Titolare del trattamento (art. 24)** — è l'ente o l'azienda, non il singolo dipendente: il Comune, l'Azienda sanitaria, la società. Decide finalità e mezzi e risponde della conformità. L'ente però ha bisogno di ogni dipendente per essere in regola.
- **Governance della privacy** — non un documento nel cassetto, ma un sistema che funziona, con ruoli chiari, procedure, responsabilità e verifiche periodiche.
- **Misure organizzative e documentali** — informative, nomine e designazioni, registro dei trattamenti, procedure interne, formazione, controlli.
- **Registro dei trattamenti (art. 30)** — la mappa dei trattamenti dell'ente: finalità, categorie di dati e di interessati, destinatari, tempi di conservazione, misure di sicurezza. Non si può proteggere ciò che non si sa di avere.
- **Privacy by design e by default (art. 25)** — la protezione dei dati si progetta prima, non dopo; per impostazione predefinita si trattano solo i dati necessari. Un nuovo software si sceglie guardando anche la privacy, non solo il prezzo.
- **Sanzioni (art. 83)** — fino a 20 milioni di euro o al 4% del fatturato mondiale annuo. Per la PA pesa anche il danno reputazionale: la prima cosa in gioco è la fiducia dei cittadini.
- **DPO / RPD (artt. 37-39)** — figura di supporto e sorveglianza, non sostituisce il Titolare. Ne parliamo nell'Incontro 2.

5 Il decalogo dell'autorizzato

Dieci regole per chi lavora ogni giorno con i dati personali.

1. **Tratta solo i dati che ti servono per il tuo lavoro.**
   Se non serve, non si guarda.
2. **Non lasciare documenti o schermi accessibili.**
   Blocca lo schermo quando ti alzi, chiudi i cassetti, non dimenticare fogli in stampante.
3. **Password personali, mai condivise.**
   Chi condivide la password non può più dimostrare chi ha fatto cosa.
4. **Controlla il destinatario prima di inviare un'email o un allegato.**
   È la causa più frequente di violazioni.
5. **Non portare dati fuori dall'ufficio senza autorizzazione.**
   Niente chiavette, stampe a casa o copie su dispositivi personali.
6. **Non usare canali non autorizzati per dati di lavoro.**
   WhatsApp ed email personali sono fuori dal controllo dell'organizzazione.
7. **Rispetta i tempi di conservazione.**
   Ciò che scade va cancellato o archiviato secondo le regole dell'ente.
8. **Al telefono e allo sportello verifica sempre l'identità.**
   Chi chiama non è sempre chi dice di essere.
9. **Nel dubbio, chiedi al referente privacy o al DPO.**
   Chiedere è il comportamento giusto.
10. **Se perdi un documento o sbagli un invio, segnalalo subito.**
    La tempestività è decisiva e non c'è colpa nel segnalare: ne parliamo nell'Incontro 5.

6 Da ricordare

> **In tre frasi:** la privacy nasce dalla tutela della persona; il GDPR si regge su principi chiari; la responsabilità è del Titolare, ma l'attuazione passa dalle persone.

Glossario essenziale

Termine	Significato
Interessato	La persona a cui si riferiscono i dati
Titolare	L'ente o l'azienda che decide perché e come trattare i dati
Autorizzato	Il dipendente o collaboratore che tratta i dati seguendo le istruzioni del Titolare
DPO / RPD	Responsabile della protezione dei dati: supporta e sorveglia, non sostituisce il Titolare
Garante	Autorità di controllo italiana per la protezione dei dati personali
Data breach	Violazione dei dati: perdita, accesso o diffusione non autorizzati

Riferimenti normativi: Regolamento (UE) 2016/679 (GDPR), in particolare artt. 4, 5, 6, 9, 10, 24, 25, 30, 37-39, 83; D.lgs. 196/2003 (Codice privacy), come modificato dal D.lgs. 101/2018.

Prossimo incontro

Mercoledì 28 ottobre, 9.00–11.00
Ruoli, responsabilità e gestione dei trattamenti

Test finale

Venerdì 30 ottobre, 12.30–13.00, in diretta
15 domande a risposta multipla, si supera con 10 corrette. Superato il test, ricevi l'attestato di partecipazione all'intero ciclo.

oltrecode
Marco La Diega S.r.l. · Via John Kennedy 154, 90031 Belmonte Mezzagno (PA) · Unità locale a Palermo
Sito: www.oltrecode.it · Magazine: oltrecode.it/magazine · Piattaforma GovDPO: www.govdpo.it