oltrecode

Privacy · Cybersecurity · Trasformazione digitale per la PA

OTTOBRE IN WEBINAR 2026 · DISPENSA

Incontro 2
Ruoli e responsabilità

Gestione dei trattamenti e strumenti della compliance

Data	Mercoledì 28 ottobre 2026
Orario	9.00 – 11.00, in diretta
Relatore	Marco La Diega, fondatore di OltreCode

Ieri abbiamo visto da dove nasce la privacy e quali sono i principi del GDPR. Questa dispensa scende nella pratica: chi fa che cosa in un ente o in un'azienda, e con quali strumenti.

> La maggior parte dei partecipanti sono **autorizzati al trattamento**: la prima linea della privacy. Capire i ruoli serve a sapere a chi rivolgersi, di cosa si risponde e dove nascono le responsabilità.

1 Chi risponde di cosa

La privacy funziona se ognuno conosce il proprio ruolo. Ecco la mappa delle figure previste dal GDPR.

Ruolo	Chi è	Di cosa risponde
Titolare artt. 4 n. 7, 24	Chi decide finalità e mezzi del trattamento. Nella PA è l'ente (il Comune, l'ASL), non il sindaco o il dirigente come persona	Decisioni, scelte organizzative, conformità complessiva, che deve poter dimostrare
Contitolari art. 26	Due o più soggetti che decidono insieme finalità e mezzi, ad esempio enti che gestiscono un servizio associato	Ciò che stabilisce l'accordo tra loro; verso l'interessato rispondono tutti
Responsabile art. 28	Chi tratta dati *per conto* del Titolare: software house, cloud, paghe, mensa, manutenzione. Non decide, esegue	Rispetto del contratto e delle istruzioni, sicurezza nel proprio perimetro
Amministratore di sistema Garante, 27 nov. 2008	Chi gestisce sistemi, reti e database con accesso potenziale a molti dati: ha le chiavi di casa	Gestione sicura dei sistemi e tracciamento degli accessi
Autorizzato art. 29; art. 2-quaterdecies Codice	Dipendenti, collaboratori, tirocinanti che trattano dati sotto l'autorità del Titolare: anagrafe, tributi, protocollo, personale	Rispetto delle istruzioni ricevute nel lavoro quotidiano
DPO / RPD artt. 37-39	Figura indipendente, obbligatoria per tutti gli enti pubblici. Informa, consiglia, sorveglia, coopera con il Garante	Consulenza e sorveglianza. Non decide al posto dell'ente e non risponde della conformità

> **Siete voi la prima linea della privacy:** la maggior parte degli incidenti nasce da una disattenzione quotidiana, non da un attacco informatico.

2 Le figure da vicino

- **La nomina del Responsabile** — va fatta per iscritto e prima che il trattamento inizi. Deve indicare oggetto, durata, natura e finalità, tipo di dati, istruzioni, riservatezza, misure di sicurezza, sub-responsabili, assistenza per diritti e data breach, restituzione o cancellazione dei dati, audit.

- **La scelta del fornitore** — il Titolare deve scegliere fornitori che offrano garanzie sufficienti. Non basta fidarsi, bisogna verificare.
- **Gli amministratori di sistema** — designazione individuale con l'elenco delle funzioni, verifica annuale dell'operato, registrazione degli accessi (log) completa e inalterabile, conservata per almeno sei mesi. Il log è la prova di chi ha fatto cosa.
- **Gli autorizzati** — ricevono istruzioni scritte e formazione e trattano i dati solo secondo quelle istruzioni. Se un'istruzione manca, si chiede.
- **Il DPO** — competente, indipendente, senza conflitti di interessi, riferisce al vertice. I suoi contatti sono pubblicati e comunicati al Garante. Non è il Titolare e non compila i documenti al posto dell'ente.

Sono responsabile io personalmente se sbaglio?

Il Titolare è l'ente. L'autorizzato che viola le istruzioni può però avere responsabilità disciplinari, civili e, nei casi gravi, penali. Chi segue le istruzioni e nel dubbio chiede è tutelato.

3 Gli strumenti della compliance quotidiana

Strumento	Cosa serve sapere
Informativa estesa artt. 12-14	Il documento completo: Titolare, DPO, finalità, base giuridica, destinatari, tempi di conservazione, diritti, reclamo al Garante
Informativa breve	Sintetica e immediata, rinvia a quella estesa. Esempio: il cartello della videosorveglianza con QR o rimando al sito
Nomine e designazioni artt. 28-29	Nomina dei Responsabili, designazione degli autorizzati con istruzioni e profili di accesso, designazione individuale degli amministratori di sistema
Diritti degli interessati artt. 15-22	Accesso, rettifica, cancellazione, limitazione, portabilità, opposizione, no a decisioni solo automatizzate. Risposta **entro un mese**, prorogabile di due mesi nei casi complessi con comunicazione motivata
Procedure interne	Scritte e brevi: richieste degli interessati, data breach, accessi, conservazione, uso degli strumenti informatici e dei dispositivi personali
Controlli periodici	Verifiche a campione, audit interni, aggiornamento del registro e delle nomine, test sulle misure di sicurezza, formazione ricorrente
Fascicolo privacy	Registro dei trattamenti, informative, nomine, DPIA, registro dei data breach, registro delle richieste, verbali di controllo. Strumenti come GovDPO aiutano a tenerlo in ordine con scadenze e promemoria

Errori tipici: informative copiate e mai aggiornate; contratti con i fornitori senza clausola privacy; nomine mai riviste. Tornando in ufficio, verifica se i contratti che gestisci contengono la clausola privacy.

Una richiesta di un interessato può arrivare a chiunque, anche a chi non se ne occupa: bisogna sapere subito a chi girarla, perché il termine di un mese decorre dal momento in cui arriva all'ente.

4 Caso pratico: l'accesso a un atto con dati di terzi

Un cittadino chiede l'accesso a un atto del Comune, ma nel documento ci sono anche dati di altre persone. Come ci si muove?

1. **Non rispondere subito.**
   Capire chi è il richiedente, verificarne l'identità e chiarire che cosa chiede davvero.

2. **Scegliere la strada giusta.**
   Accesso agli atti (L. 241/1990), accesso civico (D.lgs. 33/2013) o accesso ai propri dati (art. 15 GDPR): tre strade con regole diverse.

3. **Bilanciare trasparenza e riservatezza.**
   Oscurare i dati di terzi non pertinenti e chiedere il parere del DPO.

4. **Nel dubbio, fermarsi.**
   Prima di rispondere, consultare il referente privacy o il DPO.

5 Quando l'errore diventa sanzione

L'articolo del magazine OltreCode *L'albo non dimentica* (18 ottobre 2026) raccoglie nove provvedimenti del Garante tra il 2023 e il 2026 su albo pretorio e Amministrazione Trasparente: Comuni piccoli e medi, sanzioni da 1.800 a 12.000 euro. Cinque casi esemplari:

Ente e sanzione	Cosa è successo	La lezione
Mirabella Imbaccari (CT) 1.800 €, maggio 2026	Delibere con il nome di un cittadino online oltre i 15 giorni dell'albo; nomina del nuovo RPD non comunicata al Garante	Anche gli adempimenti verso il Garante vanno rispettati
Roccaraso (AQ) 2.000 €, marzo 2025	Il gestionale pubblicava in automatico atti su un dipendente; nessuna risposta alla richiesta di cancellazione entro un mese	Risponde il Titolare, non il fornitore del software
San Severo (FG) 10.000 €, settembre 2023	Tre determine con circa 140 dipendenti, la loro categoria e il premio di ciascuno	Un errore di configurazione resta una responsabilità del Titolare
Comune non nominato 12.000 €, luglio 2025	Registri degli accessi agli atti con 1.455 richieste, nomi e descrizioni, rimasti online	Trasparenza e riservatezza vanno bilanciate

Ente e sanzione	Cosa è successo	La lezione
Ponte nelle Alpi (BL) 4.000 €, aprile 2025	Delibere con i nomi sanzionate all'albo; le stesse con numeri progressivi in Amministrazione Trasparente non contestate	Lo stesso contenuto è lecito o illecito a seconda di come lo si pubblica

Cosa fare: durata di pubblicazione fissata per tipologia di atto con scadenza automatica; albo e archivio distinti; atti scritti sapendo che saranno pubblicati; ricognizione periodica di Amministrazione Trasparente; RPD comunicato al Garante; risposta agli interessati entro un mese; formazione di chi pubblica.

6 Da ricordare

In tre frasi: ogni ruolo ha obblighi precisi; gli strumenti documentali dimostrano la conformità; le sanzioni colpiscono enti piccoli e grandi. E soprattutto: **se non è documentato, per il Garante non è stato fatto.**

Prossimo incontro

Giovedì 29 ottobre, 9.00–11.00
Videosorveglianza, lavoratori e geolocalizzazione

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