

Privacy e protezione dei dati

Che cosa sono i dati personali e come trattarli bene ogni giorno

Gianluca Bonomo · www.gianlu.it · info@gianlu.it



Indice

Come usare questa dispensa 3

1. Che cos'è un dato personale 3

1.1 Il dato personale 4

2. Chi è chi e quali sono le regole 5

2.1 I principi in parole semplici 7

2.2 Perché la legge conta 9

3. Le buone prassi in ufficio 9

3.1 Raccogli e usa solo i dati necessari 9

3.2 Documenti in vista e stampanti 9

3.3 La copia nascosta (Ccn) 10

3.4 Prima di inviare, controlla 11

4. La violazione dei dati e la notifica al Garante 12

4.1 Le 72 ore 13

4.2 Che cosa tocca a te e che cosa tocca al titolare 14

Esercitazione pratica 16

Le domande che arrivano in aula 17

Glossario 17

Per approfondire 18

Come usare questa dispensa

Questa dispensa raccoglie, in forma scritta e ordinata, tutto quello che vediamo nella lezione. Non serve studiarla a memoria: serve a ritrovare le cose con calma, dopo, quando la lezione e' finita e resta una domanda in sospeso.

> **OBIETTIVO**
>
> Capire che cosa dicono il GDPR e il Codice privacy, riconoscere un dato personale, adottare le buone prassi quotidiane d'ufficio e sapere che cosa fare in caso di violazione dei dati, compresa la notifica al Garante entro 72 ore.

Che cosa saprai fare alla fine

- Riconoscere un dato personale e distinguerlo da un dato particolare.
- Spiegare i principi di base del GDPR con parole semplici.
- Applicare le buone prassi d'ufficio: dati necessari, documenti in vista, stampanti, copia nascosta.
- Riconoscere una violazione dei dati personali e avvisare subito chi deve decidere.
- Conoscere il termine di 72 ore per la notifica al Garante e chi ha il compito di farla.

1. Che cos'è un dato personale

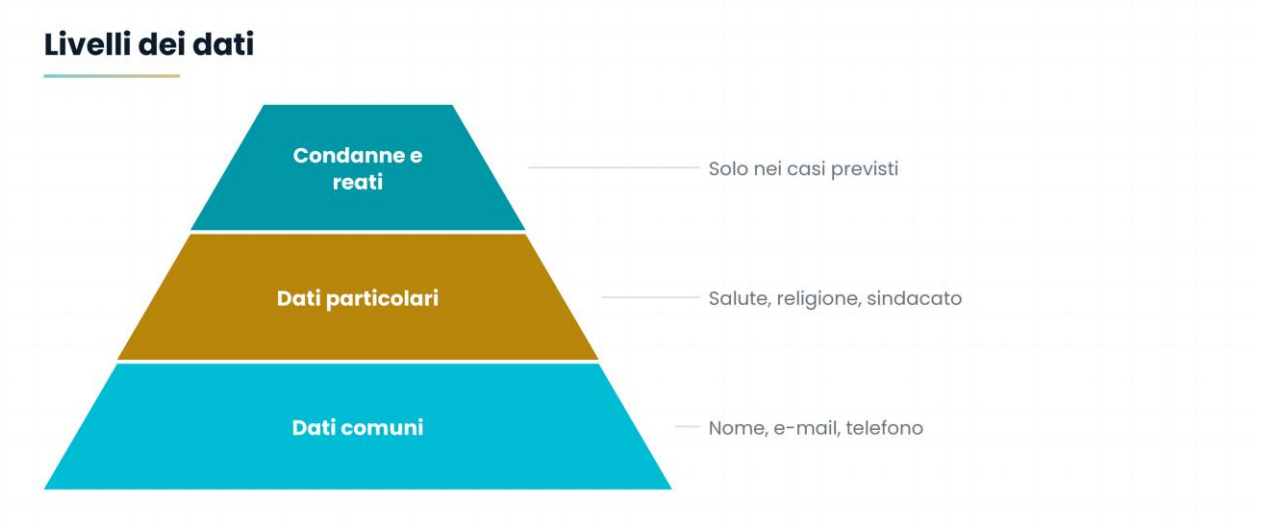
In una segreteria passano ogni giorno nomi, telefoni, indirizzi, voti, certificati. Ogni foglio racconta qualcosa di una persona vera.

Immagina Marta, che lavora nella segreteria dell'Istituto Esempio. Una famiglia le chiede di mandare per mail la scheda di un alunno. Marta ha fretta e sbaglia indirizzo. Un file con nome, classe e note sulla salute finisce a uno sconosciuto. Non c'è stato nessun attacco informatico, ma è comunque una violazione della privacy.

La **privacy** (parola inglese che indica il diritto alla riservatezza) in Europa è tutelata da due testi. Il primo è il **Regolamento UE 2016/679**, chiamato **GDPR** (dall'inglese General Data Protection Regulation), valido in tutti gli Stati dell'Unione e applicato dal 25 maggio 2018. Il secondo è il **Codice in materia di protezione dei dati personali**, cioè il decreto legislativo 196 del 2003, aggiornato nel 2018 per adeguarlo al GDPR. In Italia si applicano insieme.

1.1 Il dato personale

Un **dato personale** è qualsiasi informazione che riguarda una persona fisica identificata o identificabile. Non serve il nome: basta che da quell'informazione si possa risalire a chi è.



Tre livelli di delicatezza dei dati

Tipo di dato	Esempi	Come trattarlo
Dati comuni	Nome, indirizzo, e-mail, telefono, codice fiscale, foto, targa	Solo quelli necessari, con cura
Dati particolari	Salute, origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, vita sessuale o orientamento sessuale, dati genetici e dati biometrici usati per identificare una persona	Regole più severe: attenzione massima
Dati su condanne e reati	Informazioni su condanne penali e reati	Si trattano solo nei casi previsti dalla legge

Più il dato è delicato, più sono severe le regole.



Un'informazione identificabile riguarda una persona.

L'IDEA IN UNA RIGA

Se un'informazione ti permette di capire di chi si parla, è un dato personale, e va trattata con cura.

2. Chi è chi e quali sono le regole

La legge dà un nome a ogni ruolo. Sapere chi è chi serve a capire a chi rivolgersi quando qualcosa va storto.



I ruoli previsti dalla legge

- **Interessato**: la persona a cui i dati si riferiscono (l'alunno, il cliente, il paziente);
- **Titolare del trattamento**: chi decide perché e come si usano i dati, cioè la scuola, lo studio, l'azienda. È il titolare a rispondere davanti alla legge;
- **Responsabile del trattamento**: chi tratta i dati per conto del titolare, per esempio il fornitore del gestionale o del cloud;
- **Persona autorizzata**: tu, quando lavori in segreteria e tratti dati seguendo le istruzioni ricevute;
- **Garante per la protezione dei dati personali**: l'autorità italiana indipendente che controlla il rispetto delle regole (in inglese, the Italian Data Protection Authority).



Ruoli diversi, responsabilità diverse.

2.1 I principi in parole semplici

Il GDPR (articolo 5) fissa alcuni principi che puoi tradurre in abitudini quotidiane.

Principio	Che cosa significa nella pratica
Liceità, correttezza, trasparenza	Si usano i dati in modo corretto e la persona sa che cosa ne fai (informativa)
Limitazione della finalità	Raccogli i dati per uno scopo preciso e non li usi per altro
Minimizzazione	Chiedi e tieni solo i dati davvero necessari
Esattezza	I dati sono corretti e aggiornati
Limitazione della conservazione	Non li tieni più del necessario
Integrità e riservatezza	Li proteggi da accessi, perdite e usi non autorizzati

I principi di base del GDPR.



Scopo preciso, minimo necessario, esattezza, durata e sicurezza.

CASO PRATICO: IL MODULO TROPPO CURIOSO

Un'associazione sportiva fa compilare un modulo di iscrizione che chiede anche la professione dei genitori e il loro reddito, senza motivo. Per iscrivere un ragazzo a un corso quei dati non servono: per il principio di minimizzazione non vanno chiesti. Togliere due righe dal modulo riduce il rischio e il lavoro.



Chiedi soltanto informazioni pertinenti allo scopo.

2.2 Perché la legge conta

Chi non rispetta le regole rischia sanzioni amministrative. Per le violazioni più gravi il GDPR (articolo 83) prevede importi che possono arrivare a 20 milioni di euro o, per le imprese, al 4 per cento del fatturato mondiale annuo, se è più alto. Per altre violazioni, come quelle sugli obblighi di sicurezza e di notifica, il massimo è 10 milioni di euro o il 2 per cento. Ma c'è un motivo più concreto: dietro ogni dato c'è una persona che può subire un danno.

3. Le buone prassi in ufficio

La maggior parte delle violazioni della privacy non nasce da un attacco: nasce da una distrazione.

3.1 Raccogli e usa solo i dati necessari

Prima di chiedere un dato, domandati a che cosa serve. Se non sai rispondere, probabilmente non serve. Meno dati hai, meno dati puoi perdere.

3.2 Documenti in vista e stampanti

Una pratica sulla scrivania, vista da chi passa, è già una piccola violazione. Lo stesso vale per i fogli dimenticati nella stampante, che chiunque può prendere e leggere.

- a fine giornata riponi le pratiche in armadi o cassetti **chiusi a chiave**;

- quando ti alzi, **blocca lo schermo** con i tasti Windows e L (ne abbiamo parlato nella lezione sui dispositivi);
- dopo aver stampato, **ritira subito i fogli**; se la stampante ha la stampa protetta con codice, usala;
- per i documenti da buttare usa il **distruggidocumenti**, non il cestino;
- non lasciare password su post-it e non lasciare fogli con dati sul tavolo durante le visite.



Armadi chiusi, schermi bloccati, stampe ritirate e scarti protetti.

3.3 La copia nascosta (Ccn)

Quando mandi una mail a molte persone che non si conoscono tra loro, gli indirizzi sono dati personali. Se li metti nel campo "A" o "Cc" (copia conoscenza), tutti vedono gli indirizzi di tutti. Usa il campo **Ccn** (copia conoscenza nascosta, in inglese Bcc), che nasconde i destinatari agli altri.

> **PRIMA E DOPO**
>
> **Prima:** una mail di avviso inviata a quaranta genitori, con tutti gli indirizzi nel campo "A". Ognuno vede l'indirizzo degli altri.
>
> **Dopo:** gli stessi indirizzi nel campo Ccn. Ognuno riceve il messaggio, nessuno vede gli altri.



Ccn evita di esporre gli indirizzi degli altri destinatari.

3.4 Prima di inviare, controlla

Molte violazioni nascono da un invio sbagliato: un destinatario simile, un allegato sbagliato. Prima di premere invio rileggi destinatario e allegato. Per i documenti molto delicati, come quelli sulla salute, valuta di proteggere il file con una password, comunicata a parte con un altro mezzo.



Rileggi destinatario e allegato; per dati delicati proteggi il file e separa la password.

> **ATTENZIONE**
>
> Fare una foto con il telefono personale a un documento di lavoro con dati altrui è un trattamento di dati: non farlo, a meno che il titolare non l'abbia espressamente consentito.

4. La violazione dei dati e la notifica al Garante

Può capitare a chiunque, anche a chi è molto attento. Quello che conta è come si reagisce.

Il GDPR chiama **violazione dei dati personali** (in inglese data breach) ogni violazione di sicurezza che provoca, in modo accidentale o illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali. Non serve un hacker.

- una **chiavetta persa** con elenchi di persone;
- una mail con **allegati inviati alla persona sbagliata**;
- un **computer rubato** o un portatile lasciato in auto;
- un **ransomware** che cifra l'archivio dei clienti;
- un **account della posta** violato dopo un phishing;
- un faldone di pratiche **buttato intero nel cestino**.



Una violazione può nascere anche da un errore o da una perdita.

4.1 Le 72 ore

L'articolo 33 del GDPR dice che il **titolare del trattamento** deve notificare la violazione al Garante **senza ingiustificato ritardo e, ove possibile, entro 72 ore** da quando ne è venuto a conoscenza. L'obbligo c'è a meno che sia improbabile che la violazione comporti un rischio per i diritti e le libertà delle persone. Se la notifica arriva più tardi, va spiegato il motivo del ritardo.



Che cosa succede dopo una violazione

Il termine parte dal momento in cui il titolare ha la ragionevole certezza che sia avvenuta una violazione. Per questo il tuo compito è uno solo: **avvisare subito** il titolare o la persona che lui ha incaricato. Ogni ritardo tuo toglie tempo a chi deve decidere.

4.2 Che cosa tocca a te e che cosa tocca al titolare

Chi	Che cosa fa
Tu, quando scopri il problema	Fermi ciò che stai facendo, avvisi subito il responsabile, racconti i fatti con precisione, non cancelli nulla
Il titolare	Valuta il rischio per le persone, decide se notificare e notifica al Garante tramite la procedura online prevista sul sito del Garante
Il responsabile del trattamento (fornitore)	Se la violazione avviene presso di lui, avvisa il titolare senza ingiustificato ritardo
Le persone coinvolte	Se il rischio per loro è elevato, il titolare le informa senza ingiustificato ritardo (articolo 34)

I compiti in caso di violazione.

Anche quando non notifica al Garante, il titolare deve **documentare** ogni violazione in un registro interno, con i fatti, le conseguenze e le misure adottate. Dunque, anche un piccolo incidente va segnalato: è il titolare a decidere che cosa farne.



Il titolare valuta il rischio e gli obblighi; tutti i casi vanno documentati.

CASO PRATICO: LA MAIL SBAGLIATA

Marta si accorge di aver inviato la scheda di un alunno a un indirizzo sbagliato. Non aspetta e non spera che nessuno se ne accorga: avvisa subito la dirigente e le racconta i fatti, indirizzo compreso. La dirigente, titolare per la scuola, valuta il rischio e decide i passi successivi, compresa una richiesta al destinatario di cancellare il messaggio e, se serve, la notifica al Garante.



Avvisa subito chi è incaricato e riferisci fatti precisi.

ATTENZIONE

Nascondere una violazione è l'errore più grave: peggiora il danno e può aggravare le sanzioni. Segnalare in fretta e con onestà protegge te, le persone e l'ente.

IL LEGAME CON LA PROSSIMA LEZIONE

Quando succede, serve un metodo. Nella lezione finale vedi i passi da seguire in qualsiasi incidente, compresa la segnalazione alla Polizia Postale e delle Comunicazioni.

Esercitazione pratica

Una breve esercitazione sulla tua scrivania e sulla tua posta, con quello che hai già.

1. Guarda la tua scrivania e il tuo schermo come li vedrebbe un visitatore: che dati personali si vedono?
2. Scegli un modulo che usi (iscrizione, richiesta, scheda) e segna i dati che non servono davvero allo scopo.
3. Apri la tua posta e cerca l'ultima mail inviata a più persone: gli indirizzi erano in A, Cc o Ccn?
4. Scrivi in tre righe che cosa faresti se ti accorgessi di aver inviato un allegato alla persona sbagliata.
5. Chiedi a chi di dovere chi è il titolare nel tuo ufficio e a chi segnalare una violazione, e scrivi il nome in un posto che ritrovi.

CONTROLLO FINALE

Sai chi avvisare in caso di violazione?

Usi Ccn quando gli indirizzi non devono essere visibili?

Le pratiche sono chiuse a chiave a fine giornata?

Chiedi solo i dati necessari?

Le domande che arrivano in aula

Anche un nome e un numero di telefono sono dati personali?

Sì. Nome, telefono, e-mail, indirizzo, foto e perfino una targa sono dati personali, perché permettono di risalire a una persona.

Devo avvisare il Garante se mi accorgo di una violazione?

No, tocca al titolare del trattamento, cioè all'ente per cui lavori. Il tuo compito è avvisarlo subito: è lui a valutare il rischio e a decidere se notificare al Garante entro 72 ore.

Le 72 ore contano dal momento in cui è successo?

Contano da quando il titolare ne è venuto a conoscenza. Per questo avvisare subito è così importante.

Il GDPR vale anche per un piccolo studio o per un'associazione?

Sì. Vale per chiunque tratti dati di persone, a prescindere dalle dimensioni. Cambia, in alcuni casi, la quantità di adempimenti, non la responsabilità.

Posso inviare via WhatsApp i documenti di un cliente?

Dipende dalle regole del tuo ente e dalla delicatezza dei dati. Per documenti con dati particolari, come quelli sulla salute, chiedi al titolare quale canale è autorizzato: non decidere da solo.

Che differenza c'è tra GDPR e Codice privacy?

Il GDPR è il regolamento europeo, uguale in tutta l'Unione. Il Codice è la legge italiana che lo completa, aggiornata nel 2018 per adeguarla al regolamento. Si applicano insieme.

Glossario

Termine	Che cosa significa
Ccn	Copia conoscenza nascosta: campo della mail che nasconde i destinatari agli altri.
Dato particolare	Dato più delicato (salute, origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, vita sessuale o orientamento sessuale, dati genetici e dati biometrici usati per identificare una persona) con regole più severe.
Dato personale	Qualsiasi informazione su una persona fisica identificata o identificabile: nome, e-mail, telefono, codice fiscale, foto, targa.

Termine	Che cosa significa
Garante	Autorità italiana indipendente per la protezione dei dati personali.
GDPR	Regolamento UE 2016/679 sulla protezione dei dati personali, applicato dal 25 maggio 2018.
Interessato	La persona a cui i dati si riferiscono.
Minimizzazione	Principio per cui si raccolgono e si tengono solo i dati necessari allo scopo.
Responsabile del trattamento	Chi tratta i dati per conto del titolare, per esempio il fornitore di un servizio cloud.
Titolare del trattamento	Chi decide perché e come si usano i dati: la scuola, lo studio, l'azienda.
Violazione dei dati	Evento che provoca perdita, distruzione, modifica, divulgazione o accesso non autorizzati a dati personali.

Per approfondire

Regolamento (UE) 2016/679 (GDPR) - testo ufficiale su EUR-Lex; in particolare articoli 4, 5, 33, 34 e 83

Codice in materia di protezione dei dati personali, D.Lgs. 196/2003 - come modificato dal D.Lgs. 101/2018

Garante per la protezione dei dati personali - www.garanteprivacy.it: schede informative e procedura di notifica delle violazioni

Comitato europeo per la protezione dei dati (EDPB) - linee guida sulla notifica delle violazioni di dati personali

> **ATTENZIONE**
>
> Informazioni aggiornate a ottobre 2026. Questa lezione è formazione generale e non sostituisce una consulenza legale: le norme sono in evoluzione, controlla sempre il sito del Garante; per i casi specifici rivolgiti al titolare o al responsabile della protezione dei dati del tuo ente.