Quali dati sono protetti dalla privacy

Cosa si intende per “dato personale” e “dato sensibile” (categorie particolari) ai sensi del GDPR? Scopri quali informazioni sulla tua persona sono protette dalla normativa sulla privacy, con quali regole e con esempi pratici.

(Fonte: https://www.laleggepertutti.it/ 8 luglio 2025)

Nell’era digitale in cui viviamo, i nostri dati personali sono diventati una sorta di moneta corrente: li condividiamo per accedere a servizi, per fare acquisti online, per interagire sui social media. Ma siamo sempre consapevoli di quali informazioni stiamo fornendo e di come vengono protette? La crescente attenzione verso la tutela della sfera privata ha portato a normative sempre più stringenti, con il Regolamento Generale sulla Protezione dei Dati (GDPR) dell’Unione Europea a fare da faro. Di fronte a questo scenario, una domanda sorge spontanea e quanto mai attuale: **quali dati sono protetti dalla privacy?** Comprendere cosa rientra in questa tutela è il primo passo per essere cittadini digitali più consapevoli e per far valere i propri diritti. Questa guida, basata sul GDPR e sulla normativa italiana (il Codice Privacy, come aggiornato per armonizzarsi al regolamento europeo), ti aiuterà a fare chiarezza, illustrando le regole generali e fornendo esempi concreti.

Indice

Cosa si intende per "dato personale" secondo il GDPR?

Il punto di partenza di tutta la normativa sulla privacy è la definizione di "dato personale". L'articolo 4, paragrafo 1, punto 1 del GDPR ([Regolamento Generale sulla Protezione dei Dati / Articolo 4]) lo definisce come:

"**qualsiasi informazione riguardante una persona fisica identificata o identificabile** (denominata 'interessato')".

Una persona fisica è considerata "identificabile" quando può essere individuata, direttamente o indirettamente, attraverso un riferimento a un **identificativo**. Questi identificativi possono essere di vario tipo:

- il **nome e cognome**;
- un **numero di identificazione** (come il codice fiscale, il numero della carta d'identità, il numero di passaporto, la matricola universitaria o aziendale);
- **dati relativi all'ubicazione** (come l'indirizzo di residenza o i dati di geolocalizzazione di un dispositivo);
- un **identificativo online** (come un indirizzo IP, l'indirizzo email, un nome utente, i cookie di navigazione, i tag di identificazione a radiofrequenza – RFID);
- uno o più **elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale**.

Come si può vedere, la definizione è volutamente molto ampia e include una vasta gamma di informazioni che, da sole o in combinazione con altre, possono portare all'identificazione di una persona specifica e fornire dettagli sulle sue caratteristiche, **abitudini**, **stile di vita**, **relazioni personali**, stato di **salute**, **situazione economica** e molto altro. Diverse pronunce della Corte di Giustizia Europea e provvedimenti del Garante Privacy italiano confermano questa interpretazione estensiva.

La normativa **non si applica alle informazioni completamente anonime**, cioè a quei dati che non si riferiscono a una persona fisica identificata o identificabile, o a dati personali che sono stati resi anonimi in modo tale da impedire o non consentire più l'identificazione dell'interessato.

Quali operazioni sui dati personali sono considerate "trattamento" dalla legge?

La protezione offerta dalla normativa sulla privacy si estende a qualsiasi **"trattamento"** di dati personali. Anche qui, la definizione fornita dall'articolo 4, paragrafo 1, punto 2 del GDPR è estremamente ampia. Per "trattamento" si intende:
"qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali".
Questa definizione include, a titolo esemplificativo e non esaustivo, operazioni come:

- la raccolta dei dati;
- la registrazione e l'organizzazione;
- la strutturazione e la conservazione;
- l'adattamento o la modifica;
- l'estrazione e la consultazione;
- l'uso;
- la comunicazione mediante trasmissione, la diffusione o qualsiasi altra forma di messa a disposizione;
- il raffronto o l'interconnessione;
- la limitazione, la cancellazione o la distruzione.

In pratica, quasi ogni azione che coinvolge un dato personale è considerata un "trattamento".

Quali sono i principi fondamentali che devono guidare il trattamento dei dati personali?
Il GDPR, all'articolo 5 stabilisce una serie di principi fondamentali che devono essere sempre rispettati quando si trattano dati personali. Questi principi, richiamati costantemente dalla giurisprudenza e dal Garante Privacy (es. Provvedimento del 14 ottobre 2021 [9714644]), sono:

- **liceità, correttezza e trasparenza:** il trattamento deve avere una base legale valida, deve essere corretto nei confronti dell'interessato e le informazioni sul trattamento devono essere facilmente accessibili e comprensibili;
- **limitazione della finalità:** i dati possono essere raccolti solo per scopi determinati, espliciti e legittimi, e non possono essere trattati successivamente in modo incompatibile con tali scopi;
- **minimizzazione dei dati:** devono essere trattati solo i dati adeguati, pertinenti e strettamente necessari rispetto alle finalità per cui sono raccolti e trattati;
- **esattezza:** i dati devono essere esatti e, se necessario, aggiornati. Bisogna adottare misure per cancellare o rettificare tempestivamente i dati inesatti;
- **limitazione della conservazione:** i dati devono essere conservati in una forma che consenta l'identificazione degli interessati solo per il tempo necessario a raggiungere le finalità per cui sono trattati. Periodi di conservazione più lunghi sono ammessi solo per specifici scopi (archiviazione, ricerca, statistica) e con adeguate garanzie;

- **integrità e riservatezza:** i dati devono essere trattati in modo da garantirne un'adeguata sicurezza, proteggendoli da trattamenti non autorizzati o illeciti, dalla perdita, dalla distruzione o da danni accidentali, attraverso misure tecniche e organizzative appropriate;
- **responsabilizzazione (accountability):** il titolare del trattamento (chi decide le finalità e i mezzi del trattamento) è responsabile del rispetto di questi principi e deve essere in grado di dimostrarlo.

Esistono dati personali che richiedono una protezione ancora maggiore? Le "categorie particolari di dati personali" o ex dati sensibili

La normativa riserva una tutela speciale a determinate categorie di dati personali, considerate particolarmente delicate a causa della loro natura e dei rischi significativi che un loro trattamento improprio potrebbe comportare per i diritti e le libertà fondamentali delle persone. L'articolo 9, paragrafo 1, del GDPR elenca queste **"categorie particolari di dati personali"** (che in passato venivano comunemente definiti "dati sensibili"):

- dati personali che rivelino l'**origine razziale o etnica**;
- le **opinioni politiche**;
- le **convinzioni religiose o filosofiche**;
- l'**appartenenza sindacale**;
- i **dati genetici**;
- i **dati biometrici** trattati con lo scopo di identificare in modo univoco una persona fisica;
- i **dati relativi alla salute**;
- i dati relativi alla **vita sessuale o all'orientamento sessuale** della persona.

Il trattamento di queste categorie particolari di dati è, in linea di principio, **vietato**. Tuttavia, l'articolo 9, paragrafo 2, del GDPR prevede delle eccezioni a questo divieto, consentendo il trattamento solo in presenza di specifiche condizioni. Tra queste, le più rilevanti sono:

- il **consenso esplicito** dell'interessato per una o più finalità specifiche;
- la necessità del trattamento per assolvere obblighi ed esercitare diritti specifici del titolare del trattamento o dell'interessato in materia di **diritto del lavoro e della sicurezza sociale e protezione sociale**;
- la necessità di tutelare un **interesse vitale** dell'interessato o di un'altra persona fisica, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- il trattamento effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una **fondazione, associazione o altro organismo senza scopo di lucro** che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con l'organismo;
- il trattamento di dati personali **resi manifestamente pubblici dall'interessato**;

- la necessità del trattamento per **accertare, esercitare o difendere un diritto in sede giudiziaria**;
- la necessità del trattamento per motivi di **interesse pubblico rilevante** sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
- la necessità per finalità di **medicina preventiva o medicina del lavoro**, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale, o gestione dei sistemi e servizi sanitari o sociali;
- la necessità per motivi di **interesse pubblico nel settore della sanità pubblica**, come la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici;
- la necessità a fini di **archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici**, a determinate condizioni.

Su quale base legale generale possono essere trattati i miei dati personali?
Oltre al rispetto dei principi generali e, per le categorie particolari di dati, delle condizioni specifiche appena viste, ogni trattamento di dati personali deve fondarsi su una **base giuridica legittima**, come stabilito dall'articolo 6 del GDPR ([Tribunale di Ancona, Sentenza n.739 del 10 aprile 2024]; [Tribunale di Cassino, Sentenza n.399 del 26 aprile 2024]). Le principali basi giuridiche che rendono lecito un trattamento sono:

- quando l'interessato ha **espresso il consenso** al trattamento dei propri dati personali per una o più specifiche finalità. Il consenso deve essere libero, specifico, informato e inequivocabile;
- quando il trattamento è necessario all'**esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso (ad esempio, i dati forniti per acquistare un bene online o per sottoscrivere un abbonamento);
- quando il trattamento è necessario per **adempiere un obbligo legale** al quale è soggetto il titolare del trattamento (ad esempio, gli obblighi fiscali o contabili di un'azienda);
- quando il trattamento è necessario per la **salvaguardia degli interessi vitali dell'interessato** o di un'altra persona fisica (ad esempio, in situazioni di emergenza medica);
- quando il trattamento è **necessario per l'esecuzione di un compito** svolto nel pubblico interesse o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento (ad esempio, da parte di enti pubblici);
- quando il trattamento è necessario per il perseguimento del **legittimo interesse del titolare del trattamento o di terzi**, a condizione che non prevalgano gli interessi o i diritti e le

libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. Questa base giuridica richiede un attento bilanciamento degli interessi in gioco.

Esempi pratici di dati personali comuni che sono protetti dalla privacy

Certo, ecco alcuni esempi concreti di dati personali che incontriamo quotidianamente e che sono protetti dalla normativa sulla privacy:

- **Dati anagrafici e identificativi diretti:**
  - *Esempio:* il tuo nome, cognome, data e luogo di nascita, indirizzo di residenza, codice fiscale, numero di telefono, indirizzo email. Quando compili un modulo online per un acquisto, quando ti iscrivi a una newsletter, o quando ti registri a un servizio, questi dati sono protetti.
- **Dati economici e finanziari:**
  - *Esempio:* il tuo numero di conto corrente o di carta di credito, le informazioni sul tuo reddito o sul tuo patrimonio che fornisci per una richiesta di finanziamento, la cronologia dei tuoi acquisti su un sito di e-commerce, il tuo **codice IBAN**;
- **Dati di navigazione online e identificativi digitali:**
  - *Esempio:* il tuo indirizzo IP (che identifica la tua connessione a Internet), i cookie di tracciamento depositati sul tuo browser mentre navighi, gli identificativi univoci del tuo smartphone o tablet, i dati di geolocalizzazione del tuo telefono. Queste informazioni, anche se tecniche, possono essere usate, da sole o in combinazione, per identificarti o per creare un profilo delle tue abitudini.
- **Dati relativi al lavoro:**
  - *Esempio:* il tuo curriculum vitae, le informazioni contenute nella tua busta paga, le valutazioni delle tue performance lavorative, le comunicazioni email aziendali.
- **Dati relativi all'istruzione:**
  - *Esempio:* i tuoi voti scolastici o universitari, i titoli di studio conseguiti, la frequenza a determinati corsi.
- **Fotografie e video:**
  - *Esempio:* una tua fotografia in cui sei riconoscibile, una registrazione video in cui appari. Se queste immagini permettono di identificarti, sono considerate dati personali.

Come sono tutelati i miei dati sanitari dalla privacy?

I dati relativi alla salute (diagnosi mediche, risultati di esami, informazioni su terapie, cartelle cliniche, dettagli su malattie o condizioni fisiche e mentali) rientrano a pieno titolo nelle

“categorie particolari di dati personali” (ex dati sensibili) e, come tali, godono di una protezione rafforzata.
La loro diffusione è generalmente vietata e il loro **trattamento è ammesso** solo in presenza di rigorose condizioni, come il tuo **consenso esplicito** o la **necessità per finalità di cura, diagnosi, o per motivi di interesse pubblico** nel settore della sanità. Ad esempio, la pubblicazione online da parte di un ente pubblico delle generalità complete di una persona unitamente alla motivazione del suo collocamento a riposo per inabilità permanente è stata considerata una chiara violazione della privacy, proprio perché associava dati anagrafici a dati sensibili sullo stato di salute.
Per proteggere questi dati, è spesso richiesta l’adozione di misure di sicurezza particolari, come la cifratura o l’uso di codici identificativi per renderli inintelligibili o identificabili solo in caso di effettiva necessità.

Le mie impronte digitali o il riconoscimento facciale sono considerati dati protetti? I dati biometrici

I dati biometrici, come le immagini facciali o i dati dattiloscopici (impronte digitali), sono protetti. Rientrano nelle “categorie particolari di dati personali” quando vengono trattati attraverso un processo tecnico specifico con lo scopo di identificare in modo univoco una persona fisica (come precisato dal Tribunale Ordinario Milano, sez. 1, sentenza n. 8174/2022 e dal Provvedimento del Garante del 31 agosto 2023).
È importante notare che la semplice ripresa video di un individuo, di per sé, non costituisce automaticamente un trattamento di dati biometrici ai sensi dell’articolo 9 del GDPR, a meno che l’immagine non sia poi sottoposta a un trattamento tecnico specifico volto a estrarre parametri univoci per l’identificazione. Essendo categorie particolari, il loro trattamento è soggetto a restrizioni e richiede una base giuridica solida.

Le informazioni sulla mia navigazione online (indirizzo IP, cookie) sono considerati dati personali?

Come accennato, anche gli **identificativi online** come gli indirizzi IP, gli ID dei cookie e altri identificatori di dispositivi sono considerati dati personali ai sensi del GDPR, perché possono essere utilizzati, specialmente se combinati con altre informazioni, per creare profili degli utenti e identificarli. La Corte di Giustizia Europea si è espressa più volte su questo tema, confermando la loro natura di dato personale (ad esempio, nella Sentenza (Quarta Sezione) del 7 marzo 2024, Causa C-604/22). Il loro trattamento, ad esempio per finalità di profilazione pubblicitaria o per l’analisi del traffico web, deve rispettare pienamente i principi del GDPR, inclusa la necessità di un consenso valido o di un’altra base giuridica appropriata.

Le immagini della videosorveglianza sono considerate dati personali e quindi protette?

Le riprese video che consentono di identificare le persone fisiche sono considerate dati personali e il loro trattamento (che include la raccolta, la registrazione, la conservazione, la visualizzazione, ecc.) ricade nell'ambito di applicazione della normativa sulla privacy.
L'installazione di sistemi di videosorveglianza, sia da parte di soggetti pubblici che privati (inclusi i condomini o i singoli cittadini per la propria abitazione), costituisce un trattamento di dati personali.
Se l'angolo visuale delle telecamere è strettamente limitato agli spazi di esclusiva pertinenza del titolare (ad esempio, l'interno della propria abitazione o il proprio giardino recintato, senza riprendere aree pubbliche o altrui), il trattamento può rientrare nell'ambito delle attività a carattere esclusivamente personale o domestico, per le quali il GDPR prevede delle deroghe.
Se, invece, le telecamere riprendono aree comuni (come cortili condominiali, pianerottoli, ingressi), aree aperte al pubblico, o proprietà altrui, oppure se la videosorveglianza è effettuata per fini diversi da quelli strettamente personali (ad esempio, per sicurezza contro i furti, per controllo accessi), allora è necessario rispettare tutti i principi del GDPR. Questo include l'obbligo di fornire un'adeguata informativa (i classici cartelli "Area Videosorvegliata"), la necessità di una base giuridica legittima (che può essere il consenso degli interessati, ma più frequentemente il legittimo interesse del titolare, attentamente bilanciato con i diritti e le libertà degli interessati), e il rispetto dei principi di minimizzazione e limitazione della conservazione delle immagini.