Prof. Claudio Pantanali, PhD - cpantanali@units.it

Regolamento (UE) 2016/679

GDPR

Prof. Claudio Pantanali, PhD - cpantanali@units.it

Direttiva 95/46/CE

La **Direttiva 95/46/CE**, nota anche come **Direttiva sulla protezione dei dati personali**, è stata una normativa fondamentale dell'Unione Europea adottata il **24 ottobre 1995**. Il suo scopo principale era garantire un elevato livello di **tutela dei dati personali** dei cittadini dell'UE e armonizzare le legislazioni nazionali in materia di privacy.

Obiettivi principali della Direttiva 95/46/CE:

1. **Tutela dei dati personali**: garantire che i dati personali siano raccolti e trattati in modo lecito, corretto e trasparente.
2. **Libera circolazione dei dati**: consentire la libera circolazione dei dati personali tra gli Stati membri, senza ostacoli derivanti da differenze normative.
3. **Diritti degli interessati**: riconoscere ai cittadini diritti fondamentali, come:
    1. il diritto di accesso ai propri dati,
    2. il diritto di rettifica o cancellazione,
    3. il diritto di opporsi al trattamento in determinate circostanze.

Ambito di applicazione:

- Riguardava il **trattamento dei dati personali** (qualsiasi informazione riguardante una persona fisica identificata o identificabile) sia nel settore pubblico sia nel settore privato.
- Stabiliva **obblighi per i titolari del trattamento** (es. aziende, enti pubblici) e la necessità di notificare i trattamenti alle autorità di controllo nazionali.

Evoluzione:

La Direttiva 95/46/CE è rimasta in vigore per oltre 20 anni, ma è stata **sostituita** dal **Regolamento (UE) 2016/679**, meglio conosciuto come **GDPR (General Data Protection Regulation)**, che è entrato in vigore il **25 maggio 2018**. Il GDPR ha rafforzato e modernizzato le regole sulla protezione dei dati, rendendole **direttamente applicabili** in tutti gli Stati membri (a differenza della direttiva, che richiedeva l'attuazione tramite leggi nazionali).

Prof. Claudio Pantanali, PhD - cpantanali@units.it

GDPR - General Data Protection Regulation

L'esigenza di adottare un regolamento come il **GDPR** nasce da una combinazione di **trasformazioni tecnologiche, sociali e normative** che hanno reso **obsoleto il quadro giuridico precedente**, cioè la **Direttiva 95/46/CE** (risalente al 1995).

⚙ 1. Digitalizzazione e rivoluzione tecnologica

Negli anni '90, Internet era agli inizi. Con l'esplosione di:

- Social network
- Smartphone
- Big Data
- Cloud computing
- Intelligenza artificiale
- Internet of Things

è diventato evidente che i **dati personali** erano diventati una **risorsa strategica** e, al contempo, **molto vulnerabile**.

Servivano nuove regole per:

- proteggere meglio gli individui,
- regolamentare i nuovi modi in cui i dati venivano raccolti, usati, venduti.

Prof. Claudio Pantanali, PhD - cpantanali@units.it

🌍 2. Necessità di armonizzazione normativa tra i paesi dell'UE

La Direttiva 95/46/CE permetteva agli Stati membri **ampie libertà di interpretazione**, portando a:

- una **frammentazione normativa**,
- difficoltà per le imprese che operavano in più paesi UE.

Il GDPR, in quanto **regolamento**, è **direttamente applicabile** e **uguale in tutti gli Stati membri**, garantendo:

- coerenza,
- semplificazione per le aziende multinazionali,
- tutela uniforme per i cittadini europei.

👁 3. Scarsa consapevolezza e tutela degli utenti

Molti cittadini:

- non erano consapevoli dei loro **diritti**,
- **non avevano strumenti** per opporsi a trattamenti abusivi o pericolosi dei loro dati,
- non sapevano come ottenere **trasparenza** e **controllo** sulle proprie informazioni personali.

Il GDPR rafforza:

- i **diritti degli interessati**,
- la **trasparenza nei trattamenti**,
- l'obbligo di **informare in modo chiaro e accessibile**.

Prof. Claudio Pantanali, PhD - cpantanali@units.it

4. Aumento di abusi e violazioni della privacy

Con il tempo si sono moltiplicati:

- furti di identità,
- spam e marketing aggressivo,
- profili psicologici per fini pubblicitari o politici (es. caso **Cambridge Analytica**),
- **data breach** su larga scala.
- Serviva quindi un sistema di regole più **rigido**, **preventivo** e **sanzionatorio** per:
- responsabilizzare chi tratta dati,
- garantire un sistema efficace di controllo e intervento.

5. Favorire la fiducia e l'innovazione

L'UE ha anche voluto:

- promuovere l'**economia digitale**, ma in un contesto **etico e sicuro**,
- creare un **clima di fiducia** tra cittadini, istituzioni e imprese.

Il GDPR rappresenta un **compromesso tra protezione e progresso**: non è un freno all'innovazione, ma una **cornice legale di responsabilità**.

Conclusione

Il **GDPR** ha rappresentato un'evoluzione **profonda e strutturata** della Direttiva 95/46/CE, rafforzando:

- La **tutela dei diritti dei cittadini**,
- La **responsabilità dei titolari del trattamento**,
- La **capacità delle autorità di controllo**,
- L'**uniformità delle norme** in tutta l'UE.

Direttiva 95/46/CE VS GDPR

Confronto chiaro e dettagliato tra la Direttiva 95/46/CE e il Regolamento (UE) 2016/679 (GDPR):

1. Natura giuridica

Direttiva 95/46/CE	GDPR (Reg. UE 2016/679)
Direttiva: richiede l'attuazione attraverso leggi nazionali.	Regolamento: è direttamente applicabile in tutti gli Stati membri senza bisogno di recepimento.

2. Ambito territoriale

Direttiva	GDPR
Valida solo all'interno dell'UE.	Si applica anche a imprese extra-UE che trattano dati di cittadini UE (es. social network americani).

3. Principi e basi giuridiche del trattamento

Direttiva	GDPR
Principi di liceità, trasparenza, finalità, proporzionalità.	Gli stessi principi, ma con maggiore enfasi su trasparenza, accountability e minimizzazione.
6 basi giuridiche per il trattamento.	Le stesse 6 basi, ma definite in modo più rigoroso e chiaro (es. consenso esplicito).

4. Diritti dell'interessato

Direttiva	GDPR
Diritto di accesso, rettifica, cancellazione, opposizione.	Aggiunge: ➢ Diritto all'oblio (art. 17) ➢ Limitazione del trattamento ➢ Portabilità dei dati (art. 20)

Direttiva 95/46/CE VS GDPR

5. Responsabilità del titolare (accountability)

Direttiva	GDPR
Responsabilità poco strutturata.	Introduce il principio di accountability: il titolare deve dimostrare la conformità.
Nessun obbligo specifico di documentazione.	Obbligo di tenuta del registro dei trattamenti, valutazioni d'impatto (DPIA), ecc.

6. Autorità di controllo

Direttiva	GDPR
Ogni Stato membro aveva una propria autorità nazionale.	Mantiene le autorità nazionali, ma introduce il meccanismo di cooperazione (one-stop-shop) e il Comitato europeo per la protezione dei dati (EDPB).

7. Sanzioni

Direttiva	GDPR
Sanzioni decise a livello nazionale, spesso non efficaci.	Introduce sanzioni più severe e armonizzate: fino a 20 milioni di euro o il 4% del fatturato annuo mondiale.

8. DPO – Data Protection Officer

Direttiva	GDPR
Nessun obbligo di nomina.	Obbligo di nomina del Responsabile della protezione dei dati (DPO) in determinati casi (es. enti pubblici, trattamenti su larga scala).

Prof. Claudio Pantanali, PhD - cpantanali@units.it

CHE COS'E' IL GENERAL DATA PROTECTION REGULATION?

- Dopo **4 anni** di preparazione e dibattito è stato approvato il **GDPR** dal Parlamento Europeo il **27 aprile 2016**.
- Come prevede l'art. 99 il Regolamento l'applicazione è decorsa dal **25 maggio 2018**
- Il nuovo Regolamento Generale Europeo sulla Protezione dei Dati Personali n. 2016/679 (GDPR), con i suoi 99 articoli ha **riscritto la disciplina della Privacy a livello europeo.**
- La necessità di emanare un Regolamento Europeo in materia di privacy nasce dalla **continua evoluzione** degli stessi concetti di privacy e protezione dei dati personali e quindi della relativa tutela dovuta principalmente **alla diffusione del progresso tecnologico.**
- Quando si parla di privacy parliamo di dati relativi alle Persone Fisiche

Prof. Claudio Pantanali, PhD - cpantanali@units.it

COSA SI INTENDE PER DATO PERSONALE

📌 **Definizione di "dato personale" secondo il GDPR (art. 4, par. 1):

"Qualsiasi informazione riguardante una persona fisica identificata o identificabile ('interessato')".

🧠 Per ricordarlo con una frase semplice: "È dato personale **qualsiasi informazione** che può condurre, direttamente o indirettamente, a una **persona fisica identificabile**."

🔍 **In pratica, un dato personale è:**

- Un'informazione che **identifica direttamente** una persona (es. nome e cognome),
- Oppure che può **renderla identificabile indirettamente**, anche attraverso l'uso combinato di più dati.

✅ **Esempi di dati personali comuni:**

Diretti	Indiretti / tecnici
Nome e cognome	Indirizzo IP
Codice fiscale	Cookie identificativi
Indirizzo email personale	Dati di localizzazione (GPS)
Numero di telefono	Registrazioni vocali
Fotografia o video di una persona	Dati biometrici (es. impronta digitale)
Targa dell'auto	Identificativo utente su una piattaforma

🔒 **Categorie particolari di dati personali (art. 9 GDPR)** (aka "**dati sensibili**", più tutelati):

- Origine razziale o etnica
- Opinioni politiche
- Convinzioni religiose o filosofiche
- Appartenenza sindacale
- Dati genetici e biometrici
- Dati relativi alla salute
- Dati relativi alla vita sessuale o all'orientamento sessuale

👉 Il trattamento di questi dati è **vietato**, salvo specifiche eccezioni e tutele aggiuntive.

Prof. Claudio Pantanali, PhD - cpantanali@units.it

GDPR (Regolamento UE 2016/679) e il D.Lgs. 196/2003

La relazione tra il **GDPR (Regolamento UE 2016/679)** e il **D.Lgs. 196/2003** — conosciuto anche come **Codice in materia di protezione dei dati personali** o semplicemente **Codice Privacy** — è molto stretta, ed è fondamentale per comprendere come si applicano le norme sulla privacy in **Italia** e come viene disciplinato il trattamento dei dati personali sul territorio nazionale.

Obiettivi del Codice Privacy

- Tutelare i **diritti e le libertà fondamentali** delle persone, in particolare il diritto alla **riservatezza**.
- Regolare il trattamento dei dati da parte di **enti pubblici**, **privati**, **aziende** e **organizzazioni**.
- Stabilire i **principi** del trattamento: liceità, correttezza, pertinenza, trasparenza, necessità, sicurezza.

Struttura del Codice (principali sezioni)

1. **Principi generali**
2. **Diritti dell'interessato**
3. **Obblighi del titolare del trattamento**
4. **Comunicazioni e diffusione dei dati**
5. **Sanzioni e controlli**
6. **Autorità Garante per la protezione dei dati personali**

Evoluzione post-GDPR

Con l'entrata in vigore del **GDPR** nel 2018:

- Il D.Lgs. 196/2003 **non è stato abrogato**, ma **modificato** dal **D.Lgs. 101/2018**.
- Ora il Codice Privacy **integra il GDPR**, chiarendo le parti lasciate alla normativa nazionale (es. dati sanitari, lavoro, minori).

Ruolo del Garante

Il **Garante per la protezione dei dati personali** (istituito proprio con il Codice Privacy) è l'autorità indipendente che:

- Vigila sull'applicazione delle norme,
- Riceve reclami e segnalazioni,
- Emana provvedimenti,
- Sanziona i comportamenti illeciti.

Prof. Claudio Pantanali, PhD - cpantanali@units.it

⚖️ 1. Origine diversa, obiettivo comune

Norma	Natura	Ambito	Stato attuale
GDPR	Regolamento europeo	Valido in tutta l'UE	In vigore dal 25 maggio 2018
D.Lgs. 196/2003	Legge nazionale italiana	Solo Italia	Modificato dal D.Lgs. 101/2018 per adattarsi al GDPR

Aspetti disciplinati	GDPR	Codice Privacy (aggiornato)
Principi generali	✅	🔁 (solo in parte)
Diritti degli interessati	✅	🔁 (es. minori, decesso)
Basi giuridiche del trattamento	✅	❌
Obblighi del titolare e responsabile	✅	🔁
Sanzioni amministrative	✅	🔁
Aspetti specifici nazionali (es. lavoro, sanità, giustizia)	❌	✅
DPO, Garante Privacy, procedimenti	✅	✅ (solo aspetti operativi italiani)

🔄 2. Cosa è successo nel 2018: modifica del D.Lgs. 196/2003

Per **adeguare la normativa italiana al GDPR**, è stato emanato il:

➡️ **D.Lgs. 101/2018**, entrato in vigore il 19 settembre 2018.

Questo decreto ha:

- **abrogato alcune parti** del vecchio Codice Privacy,
- **modificato e aggiornato** altri articoli,
- **coordinato** la normativa italiana con le disposizioni europee.

Quindi oggi parliamo di un **"Codice della Privacy riformato"** che **integra il GDPR**.

📌 3. Divisione delle competenze: cosa disciplina il GDPR e cosa il Codice italiano

Prof. Claudio Pantanali, PhD - cpantanali@units.it

Tabella di raffronto: GDPR vs D.Lgs. 196/2003 (aggiornato dal D.Lgs. 101/2018)

Argomento	GDPR (Reg. UE 2016/679)	D.Lgs. 196/2003 aggiornato
Natura giuridica	Regolamento UE, direttamente applicabile	Decreto legislativo italiano
Entrata in vigore	25 maggio 2018	1 gennaio 2004 (modificato nel 2018)
Campo di applicazione	Tutti i paesi UE	Solo Italia
Finalità	Protezione uniforme dei dati personali in UE	Adattamento italiano al GDPR, regolazione di casi specifici
Principi generali	Art. 5 GDPR	Art. 2-septies e successivi (in parte)
Diritti degli interessati	Articoli 12–22	Artt. 2-ter e ss. (integrazione: minori, deceduti, ecc.)
Età del consenso digitale	Lasciata agli Stati membri	Fissata a 14 anni (art. 2-quinquies)
Trattamenti particolari (sanità, lavoro, giustizia)	Regole generali, lascia spazio agli Stati membri	Regolamenta in dettaglio questi casi
Ruolo del Garante	Stabilito nel GDPR (art. 51-59)	Dettagli operativi, poteri e procedura (Titolo II del Codice)
Sanzioni	Ammende amministrative fino a 20 milioni € o 4% fatturato	Disposizioni procedurali italiane; pene penali in alcuni casi
Profilazione e decisioni automatizzate	Art. 22	Nessuna modifica sostanziale
DPO (Responsabile protezione dati)	Obbligatorio in certi casi (art. 37-39)	Coordinamento con obblighi italiani

Prof. Claudio Pantanali, PhD - cpantanali@units.it

Garante per la protezione dei dati personali

Il **Garante per la protezione dei dati personali**, comunemente noto come **Garante della Privacy**, è l'autorità indipendente italiana incaricata di vigilare sul rispetto della normativa in materia di protezione dei dati personali, in particolare del **Regolamento (UE) 2016/679 (GDPR)** e del **Codice della Privacy italiano (D.Lgs. 196/2003, modificato dal D.Lgs. 101/2018)**.

🦴 1. Compiti principali

Il Garante:

- **Vigila** sull'applicazione delle norme in materia di privacy.
- **Esamina i reclami** presentati da cittadini o imprese.
- **Svolge indagini e ispezioni** (anche d'ufficio).
- **Autorizza determinati trattamenti** di dati sensibili o particolari.
- **Fornisce pareri** su atti normativi e regolamenti che impattano la privacy.
- **Promuove la consapevolezza** tra cittadini, enti pubblici e imprese.
- **Collabora con altre autorità europee** nell'ambito dell'EDPB (European Data Protection Board).

⚖️ 2. Poteri ispettivi e sanzionatori

Il Garante ha poteri molto ampi:

- **Può effettuare ispezioni** presso enti pubblici e privati.
- **Può imporre misure correttive**, ad esempio: avvertimenti, ammonimenti, limitazioni o divieti al trattamento dei dati.
- **Può infliggere sanzioni amministrative pecuniarie**, che nel GDPR arrivano fino a **20 milioni di euro** o **il 4% del fatturato annuo mondiale** (per imprese).
- **Può denunciare all'autorità giudiziaria** eventuali reati connessi al trattamento illecito dei dati.

Prof. Claudio Pantanali, PhD - cpantanali@units.it

Garante per la protezione dei dati personali

3. Struttura e nomina

- Il Garante è un **collegio composto da 4 membri**, eletti **dal Parlamento**: 2 dalla Camera e 2 dal Senato.
- I membri restano in carica **7 anni** e non sono rieleggibili.
- Eleggono al loro interno un **Presidente**, che rappresenta l'Autorità.

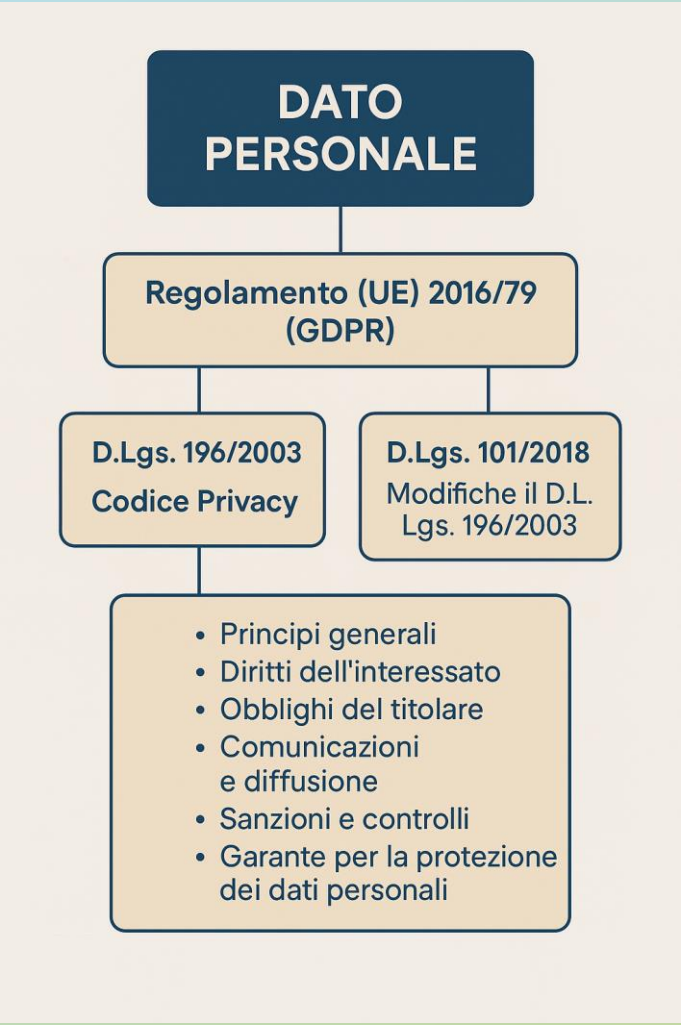
4. Attività pratica

Il Garante opera concretamente in vari ambiti, ad esempio:

- **Tutela dei dati sanitari** (es. cartelle cliniche, referti online).
- **Protezione dei dati sul lavoro** (es. controllo a distanza, email aziendali).
- **Internet e social media** (es. cyberbullismo, rimozione dati dai motori di ricerca).
- **Trasparenza nella pubblica amministrazione** (accesso civico e privacy).
- **Marketing e profilazione** (consenso, informativa, cookie).

5. Contatti e interazioni con il pubblico

- Chiunque può **presentare un reclamo o una segnalazione** al Garante (anche online).
- Il sito ufficiale è: **www.garanteprivacy.it**
- Pubblica **newsletter, provvedimenti, pareri, linee guida** e notizie sull'evoluzione della normativa.



Garante per la protezione dei dati personali

il Garante italiano può agire in autonomia nel rispetto del **quadro normativo europeo**, ma ci sono **casi in cui è tenuto a coordinarsi** con le altre autorità europee, soprattutto attraverso l'**EDPB** (European Data Protection Board, ovvero il Comitato europeo per la protezione dei dati).

✅ Quando il Garante può agire autonomamente

Il Garante può prendere decisioni indipendenti in tutti i casi che:

- **Riguardano trattamenti effettuati solo in Italia**, senza impatti transfrontalieri (cioè senza coinvolgere interessati in altri Stati membri).
- Sono legati a **autorità pubbliche italiane**, enti locali, scuole, aziende italiane che trattano dati solo di residenti italiani.
- Comportano interventi **urgenti a tutela dei diritti degli interessati**, anche senza il coinvolgimento del Comitato europeo.

Esempi:

- Sanzionare un'azienda italiana che fa spam o usa telecamere in modo illecito.
- Imporre limiti al trattamento dei dati sanitari in un ospedale.
- Intervenire su casi di violazione della privacy in ambito scolastico o lavorativo.

🏛️ Quando deve coordinarsi con l'Europa

Il Garante **non può decidere da solo** quando:

- Il trattamento dei dati ha **effetti in più Paesi UE** (es. social network, servizi cloud, e-commerce internazionali).
- L'azienda o l'organizzazione coinvolta ha **stabilimenti o utenti in più Stati UE**.
- È necessaria una **decisione congiunta** secondo il **meccanismo di coerenza** previsto dal GDPR (artt. 60-65).
- In questi casi:
- Si attiva il **meccanismo di cooperazione** tra le autorità garanti degli altri Paesi interessati.
- L'EDPB può intervenire per **emettere un parere vincolante** o risolvere controversie tra autorità nazionali.
- La decisione finale può essere adottata in modo **congiunto**.

Prof. Claudio Pantanali, PhD - cpantanali@units.it

Garante europeo della protezione dei dati (GEPD)

Le istituzioni e gli organi dell'UE talvolta, nello svolgimento delle loro funzioni, trattano i **dati personali dei cittadini**, in formato elettronico, per iscritto o visivamente.
Il trattamento comprende la raccolta, la registrazione, la conservazione, il recupero, la trasmissione, il blocco o la cancellazione di dati. È compito del Garante europeo della protezione dei dati (GEPD) tutelare le **rigorose norme sulla privacy** che disciplinano tali attività.

Cosa fa il GEPD?

- **Controlla** il trattamento dei dati personali da parte dell'amministrazione dell'UE allo scopo di assicurare il rispetto delle norme sulla privacy
- **fa da consulente** per le istituzioni e gli organi dell'UE su tutti gli aspetti del trattamento dei dati personali e delle relative politiche e legislazione
- gestisce le **denunce** e conduce indagini
- collabora con le **amministrazioni nazionali** dei paesi dell'UE per assicurare la coerenza nell'ambito della protezione dei dati
- controlla le **nuove tecnologie** che possono influire sulla protezione dei dati.

Come funziona il GEPD?

Il **Garante** e il **Garante aggiunto** sono nominati per mandati rinnovabili di cinque anni. Per svolgere le funzioni correnti il GEPD conta su **due sezioni principali**:

- controllo e rispetto delle norme - **esamina il rispetto della protezione dei dati** da parte delle istituzioni e degli organi dell'UE
- politica e consultazione - **fornisce consulenza ai legislatori dell'UE su aspetti concernenti la protezione dei dati** attinenti alle politiche di diversi settori e a nuove proposte legislative.

Il GEPD e i cittadini

Gli organi e le istituzioni dell'UE non devono trattare i dati personali riguardanti:

- **l'origine etnica** o **razziale**
- **le opinioni politiche**
- le **concezioni filosofiche** o **religiose**
- **l'affiliazione sindacale**.

Né possono trattare dati concernenti la **salute** o l'**orientamento sessuale** se non per scopi sanitari. Anche in questo caso, il trattamento deve essere eseguito da un professionista del settore sanitario o da altre persone tenute al segreto professionale.

Ove si ritenga che il proprio **diritto alla privacy sia stato violato** da un'istituzione o da un organo dell'UE, ci si dovrebbe **rivolgere** in prima istanza **al personale dell'UE responsabile del trattamento dei propri dati nel servizio in cui si ritiene sia stata commessa la violazione**. Se i risultati non sono soddisfacenti, contattare il responsabile della protezione dati dell'istituzione o dell'organo dell'UE che si ritiene abbia commesso la violazione.

Se ciò non ha effetto, si può **presentare un reclamo** al GEPD utilizzando un modulo apposito. Il Garante europeo della protezione dei dati **indagherà** e comunicherà agli interessati se concorda con il reclamo presentato e, in caso affermativo, come si sta procedendo a correggere la situazione.
Se **si è in disaccordo** con la decisione del GEPD, è possibile deferire la questione alla Corte di giustizia dell'UE.

Prof. Claudio Pantanali, PhD - cpantanali@units.it

Trattamento dei dati personali

Il trattamento dei dati personali, secondo il **Regolamento Generale sulla Protezione dei Dati (GDPR)**, comprende una serie di operazioni svolte su dati personali, sia con strumenti automatizzati che manuali. Queste operazioni includono la raccolta, la registrazione, l'organizzazione, la conservazione, la modifica, la consultazione, l'uso, la comunicazione, la diffusione e la cancellazione dei dati.

Fasi del trattamento dei dati personali

1. **Raccolta**: Acquisizione dei dati personali direttamente dall'interessato o da terze parti.
2. **Registrazione**: Memorizzazione dei dati su supporti elettronici o cartacei.
3. **Organizzazione e strutturazione**: Classificazione e disposizione dei dati secondo criteri specifici per facilitarne l'accesso e l'uso.
4. **Conservazione**: Mantenimento dei dati per un periodo limitato, proporzionato alle finalità del trattamento.
5. **Consultazione e uso**: Accesso e utilizzo dei dati da parte di personale autorizzato per le finalità dichiarate.
6. **Modifica e aggiornamento**: Correzione o aggiornamento dei dati per garantirne l'accuratezza.
7. **Comunicazione e diffusione**: Trasmissione dei dati a terzi, se necessario e legittimo.
8. **Cancellazione o distruzione**: Eliminazione definitiva dei dati quando non più necessari o su richiesta dell'interessato.

Principi fondamentali del trattamento

- **Liceità, correttezza e trasparenza**: I dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.
- **Limitazione della finalità**: I dati devono essere raccolti per scopi specifici, espliciti e legittimi.
- **Minimizzazione dei dati**: Devono essere trattati solo i dati adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento.
- **Esattezza**: I dati devono essere esatti e, se necessario, aggiornati.
- **Limitazione della conservazione**: I dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.
- **Integrità e riservatezza**: I dati devono essere trattati in modo da garantire adeguata sicurezza, compresa la protezione contro il trattamento non autorizzato o illecito e contro la perdita, la distruzione o il danno accidentale.

Obblighi del titolare del trattamento

Il titolare del trattamento deve:

- Informare gli interessati sulle modalità e finalità del trattamento.
- Ottenere il consenso, quando richiesto.
- Garantire i diritti degli interessati, come l'accesso, la rettifica e la cancellazione dei dati.
- Adottare misure tecniche e organizzative adeguate per garantire la sicurezza dei dati.Tenere un registro delle attività di trattamento.Notificare eventuali violazioni dei dati personali alle autorità competenti e, se necessario, agli interessati.

Prof. Claudio Pantanali, PhD - cpantanali@units.it

Conservazione dei dati personali

La **conservazione dei dati personali** è regolata dal **GDPR** (Regolamento Generale sulla Protezione dei Dati), che stabilisce criteri precisi per garantire che i dati siano mantenuti solo per il tempo necessario e in modo sicuro.

🕒 Durata della conservazione

Secondo l'articolo 5, paragrafo 1, lettera e) del GDPR, i dati personali devono essere:

"conservati in una forma che consenta l'identificazione degli interessati per un periodo non superiore al conseguimento delle finalità per le quali sono trattati"

🧰 Criteri per determinare i tempi di conservazione

Il GDPR non specifica tempi precisi per la conservazione dei dati, lasciando ai titolari del trattamento la responsabilità di stabilirli in base a:

- **Finalità del trattamento**: ad esempio, i dati raccolti per un contratto devono essere conservati per la durata del contratto e per eventuali obblighi legali successivi.
- **Obblighi legali**: alcune normative richiedono la conservazione dei dati per periodi specifici (es. 10 anni per documenti fiscali).
- **Consenso dell'interessato**: se il trattamento si basa sul consenso, i dati devono essere eliminati una volta revocato il consenso.

È fondamentale documentare questi criteri nel **registro delle attività di trattamento** e comunicarli nell'**informativa privacy**.

🔐 Misure di sicurezza durante la conservazione

Durante il periodo di conservazione, i dati devono essere protetti mediante:

- **Crittografia**: per proteggere i dati da accessi non autorizzati.
- **Pseudonimizzazione**: per ridurre il rischio in caso di violazione dei dati.
- **Controlli di accesso**: per garantire che solo il personale autorizzato possa accedere ai dati.
- **Backup e piani di recupero**: per prevenire la perdita di dati.

Queste misure devono essere proporzionate al rischio associato al trattamento dei dati.

🗑️ Cancellazione dei dati

Una volta scaduto il periodo di conservazione, i dati devono essere:

- **Cancellati**: eliminati in modo sicuro per impedire il recupero.
- **Anonimizzati**: modificati in modo da non poter più identificare l'interessato.

È importante implementare procedure per garantire la cancellazione tempestiva dei dati non più necessari.

SISTEMI DI GESTIONE DELL'IGIENE E SICUREZZA NEGLI AMBIENTI DI LAVORO
Prof. Claudio Pantanali, PhD - cpantanali@units.it

7 principi fondamentali del GDPR

I **7 principi fondamentali del GDPR** (art. 5 del Regolamento UE 2016/679) rappresentano la **base giuridica** su cui si fonda tutta la disciplina della protezione dei dati personali.

✅ **1. Liceità, correttezza e trasparenza**

- Il trattamento deve essere **lecito** (cioè fondato su una delle basi giuridiche previste: consenso, obbligo legale, contratto, ecc.),
- **Corretto** (senza inganni, scorrettezze o trattamenti abusivi),
- E **trasparente** (l'interessato deve sapere chiaramente cosa viene fatto con i suoi dati).

🎯 **2. Limitazione della finalità**

- I dati devono essere raccolti per **finalità determinate, esplicite e legittime**,
- E **non devono essere trattati ulteriormente** in modo incompatibile con tali finalità.

📉 **3. Minimizzazione dei dati**

- Si devono trattare **solo i dati strettamente necessari** al raggiungimento della finalità: "Meno dati raccogli, meno rischi corri.«

🎯 **4. Esattezza**

- I dati personali devono essere **esatti e aggiornati**.
- Devono essere adottate misure per **cancellare o rettificare** quelli inesatti o incompleti.

⏳ **5. Limitazione della conservazione**

- I dati vanno conservati **solo per il tempo necessario** al raggiungimento delle finalità per cui sono stati raccolti.
- Dopo tale periodo, vanno **cancellati o anonimizzati**, salvo obblighi legali di conservazione.

🔐 **6. Integrità e riservatezza (sicurezza)**

- I dati devono essere trattati in modo da garantirne **sicurezza, integrità e riservatezza**,
- Proteggendoli da **accessi non autorizzati**, **perdite**, **danneggiamenti**, **diffusioni illecite**, ecc.

📜 **7. Responsabilizzazione (accountability)**

- Il titolare del trattamento è **responsabile** del rispetto di tutti i principi sopra elencati,
- E deve poter **dimostrare** in ogni momento la conformità al GDPR (es. documentazione, valutazioni d'impatto, misure di sicurezza, ecc.).

SISTEMI DI GESTIONE DELL'IGIENE E SICUREZZA NEGLI AMBIENTI DI LAVORO
Prof. Claudio Pantanali, PhD - cpantanali@units.it

7 principi fondamentali del GDPR

PRINCIPIO DI CORRETTEZZA

La correttezza del trattamento è essenzialmente legata all'idea che gli interessati devono essere **consapevoli** del fatto che i loro dati personali saranno trattati, compreso il modo in cui i dati saranno raccolti, conservati e utilizzati, per consentire loro di **prendere una decisione informata**

PRINCIPIO DI TRASPARENZA

Il **principio della trasparenza** impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro.

PRINCIPIO DI ESATTEZZA

- I dati raccolti dovranno essere esatti e, se necessario, aggiornati.
- Di conseguenza le Aziende dovranno adottare tutte le misure ragionevoli per cancellare o rettificare tempestivamente eventuali dati inesatti rispetto alle finalità per le quali sono trattati.

PRINCIPIO DI MINIMIZZAZIONE DEI DATI

- Il principio della "minimizzazione dei dati" indica che un Titolare del trattamento dei dati dovrebbe limitare la raccolta di informazioni personali a ciò che è direttamente rilevante e necessario per raggiungere uno scopo specifico.
- Dovrebbero inoltre conservare i dati solo per il tempo necessario a raggiungere lo scopo.

PRINCIPIO DI LIMITAZIONE DELLA CONSERVAZIONE

- Il GDPR non stabilisce alcun periodo minimo o massimo per la conservazione dei dati personali ma non devono essere conservati per un periodo superiore a quello necessario per tale scopo o per tali finalità.

PRINCIPIO DI LIMITAZIONE DELLE FINALITA'

- I Titolari devono innanzitutto identificare le particolari finalità per le quali i dati personali saranno trattati (by design)
- Tali scopi diverranno i limiti entro i quali i dati personali devono essere raccolti e utilizzati dai responsabili del trattamento dei dati.
- Il trattamento secondario può essere effettuato legalmente solo quando tale trattamento è considerato compatibile con lo scopo originale per il quale i dati personali sono stati raccolti.

PRINCIPIO DI INTEGRITA' E RISERVATEZZA

- i dati dovranno essere sempre trattati in maniera da garantire una sicurezza adeguata, il che prevede l'adozione di misure di sicurezza tecniche ed organizzative adeguate per proteggere i dati stessi da trattamenti non autorizzati o illeciti, dalla loro perdita o distruzione o dal danno accidentale.

Prof. Claudio Pantanali, PhD - cpantanali@units.it

6 elementi di liceità del trattamento

Consenso: l'interessato ha dato il consenso al trattamento dei propri dati personali per uno o più scopi specifici;

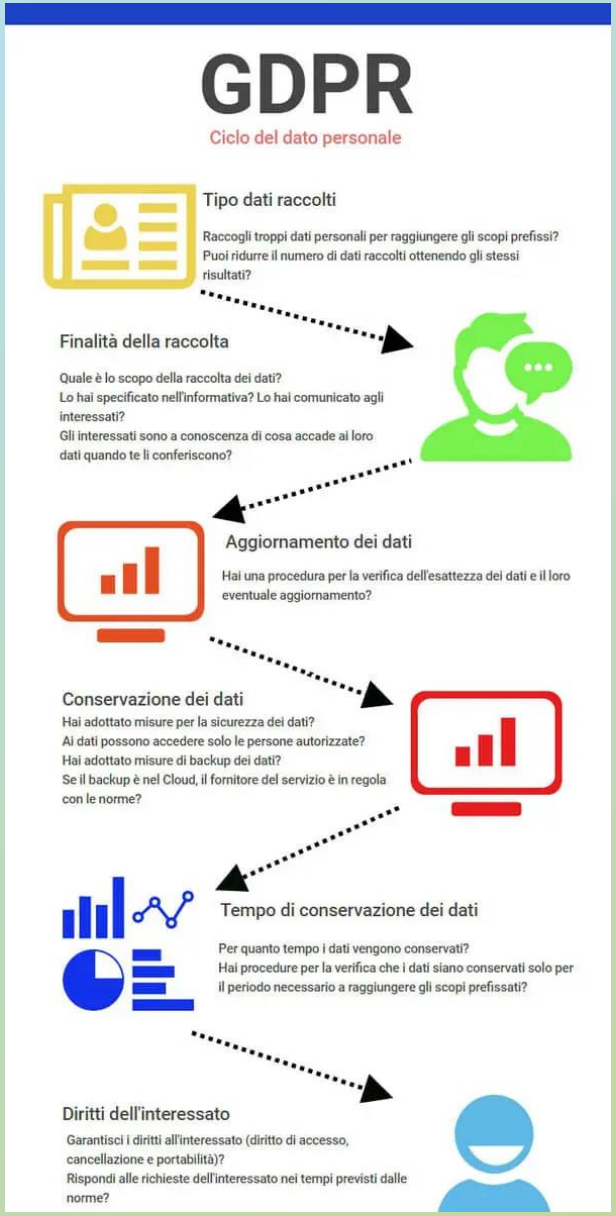
Esecuzione contrattuale: l'elaborazione è necessaria per l'esecuzione di un contratto a cui l'interessato è parte o per prendere provvedimenti su richiesta dell'interessato prima di stipulare un contratto;

Obbligo legale: l'elaborazione è necessaria per adempiere a un obbligo legale a cui è soggetto il responsabile del trattamento;

Interesse vitale delle persone: il trattamento è necessario per proteggere gli interessi vitali dell'interessato o di un'altra persona fisica;

Interesse pubblico: il trattamento è necessario per l'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio di pubblici poteri conferiti al responsabile del trattamento;

Interesse legittimo: il trattamento è necessario ai fini degli interessi legittimi perseguiti dal responsabile del trattamento o da una terza parte



Prof. Claudio Pantanali, PhD - cpantanali@units.it

Data Breach

🔒 Cosa si intende per Data Breach?

Un **data breach** (violazione dei dati personali) è un evento **accidentale o illecito** che comporta:

1. **La distruzione**
2. **La perdita**
3. **La modifica non autorizzata**
4. **La divulgazione non autorizzata**
5. **L'accesso non autorizzato** ai dati personali trasmessi, conservati o comunque trattati.

📌 Anche un errore umano può causare un data breach (es. invio di dati a destinatario sbagliato).

🧱 Tipologie principali di data breach

Tipo	Descrizione	Esempi
Riservatezza violata	Accesso non autorizzato ai dati	Hackeraggio, email inviata a persona sbagliata
Integrità compromessa	Modifica non autorizzata dei dati	Alterazione dolosa o errore tecnico
Disponibilità persa	I dati non sono più accessibili quando necessario	Attacco ransomware, guasto server senza backup

Prof. Claudio Pantanali, PhD - cpantanali@units.it

📢 Obblighi in caso di data breach (Art. 33 GDPR)

1. Notifica al Garante Privacy

- **Entro 72 ore** dalla scoperta della violazione.
- Obbligatoria **se la violazione comporta un rischio per i diritti e le libertà delle persone**.
- La notifica deve contenere:
  - Natura della violazione.
  - Numero e tipo di soggetti coinvolti.
  - Dati compromessi.
  - Misure adottate per mitigare gli effetti.

2. Comunicazione all'interessato (Art. 34 GDPR)

- Solo **se la violazione è ad alto rischio per i diritti e le libertà** delle persone.
- Obiettivo: permettere all'interessato di adottare misure di protezione.
- Deve essere **chiara e comprensibile**.

🛡️ Misure preventive raccomandate

- Sistemi di **autenticazione forte**.
- **Crittografia** dei dati sensibili.
- **Backup regolari**.
- Procedure per la **gestione delle emergenze**.
- **Formazione del personale** sulla sicurezza dei dati.

⚖️ Conseguenze e sanzioni

Mancata notifica può comportare sanzioni fino a:

- **10 milioni di euro** o
- **2% del fatturato mondiale annuo** (in base all'entità della violazione).

📌 Esempio reale

Cambridge Analytica – Facebook (2018): uso improprio di dati di milioni di utenti a fini politici. È uno dei casi di data breach più famosi, che ha sollevato l'attenzione globale su privacy e protezione dei dati.

Si stabilisce l'obbligo per tutti i Titolari del trattamento di effettuare la notifica della violazione all'autorità di controllo entro 72 ore ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati

Prof. Claudio Pantanali, PhD - cpantanali@units.it

DIRITTI INDIVIDUALI

I diritti dell'interessato

I diritti dell'interessato al trattamento enumerati nel capo III del GDPR sono:

- il diritto ad essere informato (artt. 12-13-14);
- il diritto di accesso ai dati (art. 15);
- il diritto di rettifica (art. 16);
- il diritto alla cancellazione dei dati, o «diritto all'oblio» (art. 17);
- il diritto alla limitazione del trattamento (art. 18);
- il diritto alla portabilità dei dati (art. 20);
- il diritto ad opporsi a determinate forme di trattamento (art. 21)
- Il diritto a non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato dei dati che lo riguardano (art. 22).

Il diritto all'informazione - Informativa

Sinteticamente, l'interessato ha diritto a essere informato in merito:

- all'esistenza di trattamenti di dati personali che lo riguardano;
- alle finalità di tali trattamenti;
- all'identità dei soggetti che svolgono il trattamento (titolari) e dei loro principali collaboratori (rappresentanti e responsabili della protezione dei dati);
- all'identità dei soggetti terzi a cui i dati potrebbero essere comunicati (destinatari), e alla possibilità che i dati siano trasmessi in un Paese extra-europeo;
- al periodo di conservazione dei dati;
- all'eventuale obbligo di comunicare i propri dati e alle conseguenze della mancata comunicazione;
- all'eventuale automatizzazione dei processi di trattamento, alle logiche utilizzate in tali processi e alle possibili conseguenze;
- all'origine dei dati personali (quando non sono stati comunicati dall'interessato stesso);
- ai diritti che l'interessato può esercitare in relazione al trattamento.

Diritto alla cancellazione (diritto all'oblio)

inteso come il diritto dell'interessato di ottenere dal titolare la cancellazione dei dati personali che lo riguardano in presenza di particolari condizioni

Diritto di limitazione di trattamento,

con cui l'interessato può chiedere una restrizione del trattamento

(ad es. la sola conservazione dei dati con esclusione di qualsiasi altro utilizzo)

Prof. Claudio Pantanali, PhD - cpantanali@units.it

Il diritto alla cancellazione: eccezioni e limiti

L'interessato non ha diritto a ottenere la cancellazione di dati quando il trattamento è necessario:

- per l'esercizio del diritto alla libertà di espressione e di informazione;
- per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- per l'adempimento di un obbligo di legge previsto dal diritto nazionale o comunitario;
- per l'esecuzione di un compito svolto nel pubblico interesse o nell'esercizio dei pubblici poteri, da un soggetto investito di tali poteri;
- per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità; se si tratta di «dati particolari», il diritto alla cancellazione non sussiste solo se il trattamento è effettuato da o sotto la responsabilità di un professionista soggetto al segreto professionale;
- per motivi di interesse pubblico nel settore della sanità pubblica, quali 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;
- per fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici se la cancellazione rischia di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento, e purché il trattamento sia soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, e avvenga nel rispetto del principio della minimizzazione dei dati, utilizzando, ove praticabile, la pseudonimizzazione o l'anonimizzazione dei dati.

Prof. Claudio Pantanali, PhD - cpantanali@units.it

DATA PORTABILITY

GDPR introduce la **data portability.**

Il Diritto alla portabilità dei dati, definito "il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e di trasmettere tali dati a un altro titolare senza impedimenti"

CONSENSO

SPECIFICO E INFORMATO

Un consenso per ogni finalità

Preceduto dall'informativa

DIMOSTRABILE

Il Titolare del trattamento

deve essere in grado di dimostrare che l'interessato ha espresso il proprio consenso al trattamento dei propri dati personali (onere della prova)

FACILITÀ DI REVOCA

ESPLICITO

Solo per il trattamento dei dati particolari e per la profilazione

All'interno di un contratto scritto la richiesta di consenso deve essere presentata in modo chiaramente distinguibile e con un linguaggio semplice e chiaro.

Prof. Claudio Pantanali, PhD - cpantanali@units.it

ACCOUNTABILITY

SISTEMI DI GESTIONE DELL'IGIENE E SICUREZZA NEGLI AMBIENTI DI LAVORO
Prof. Claudio Pantanali, PhD - cpantanali@units.it

Le figure previste dal GDPR "Accountability e Responsability "

📜 ACCOUNTABILITY – Responsabilizzazione

📖 Definizione (art. 5, par. 2 GDPR):

Titolare del trattamento

- Responsabile dell'applicazione del GDRP
- Sanzioni fino a 20 mln o 4% del fatturato

Responsabile del trattamento

- Incarico con contratto vincolante
- Istruzione documentata
- Assiste il titolare

Persone autorizzate al trattamento

- Esecutori materiali delle attività di trattamento

RPD o DPO

- Responsabile Protezione dati personali (non è il responsabile del trattamento)

📌 Cosa significa in pratica?

Il principio di **accountability** impone al titolare del trattamento non solo di **rispettare** le regole del GDPR, ma anche di **poter dimostrare concretamente** di averle rispettate.

⚙️ Come si attua l'accountability?

Ecco gli strumenti principali per dare concreta attuazione a questo principio:

1. ✅ **Registro dei trattamenti (art. 30)**
Documento obbligatorio che descrive in dettaglio i trattamenti effettuati.
2. 🔍 **Valutazione d'impatto (DPIA – art. 35)**
Analisi preventiva dei rischi nei trattamenti ad alto impatto (es. videosorveglianza, profilazione, dati sanitari su larga scala).
3. 📄 **Adozione di policy, procedure e regolamenti interni**
Tutto documentato e aggiornato: gestione del consenso, gestione delle violazioni, conservazione, nomine degli incaricati.
4. 🧠 **Formazione del personale**
Obbligatoria per chiunque tratti dati. È parte integrante della responsabilizzazione.
5. 🔒 **Adozione di misure tecniche e organizzative adeguate (art. 24)**
Es. cifratura, pseudonimizzazione, backup, gestione degli accessi.
6. 👨‍💼 **Designazione del DPO (se necessario)**
Figura di riferimento che assiste il titolare e funge da collegamento col Garante.
7. 🛠️ **Documentazione delle scelte e delle valutazioni fatte**
Anche quando si decide di **non fare** qualcosa (es. "non serve DPIA"), è bene **motivarla per iscritto**.

Prof. Claudio Pantanali, PhD - cpantanali@units.it