Il regolamento GDPR per la «privacy

Recepito in Italia dal D.Lgs. 101/2018 che ha modificato il D.Lgs. 196/2003

A CURA DI DOTT. DAVIDE TREPICCIONE

CONTESTO

In Italia, la normativa privacy è regolamentata dal Codice in materia di protezione dei dati personali (Codice Privacy) che recepisce le direttive europee in materia di protezione dei dati personali. Il Codice Privacy stabilisce le regole per il trattamento dei dati personali da parte di aziende, organizzazioni e pubbliche amministrazioni, al fine di tutelare i diritti e la privacy dei cittadini.

Secondo la normativa privacy italiana, i dati personali sono definiti come qualsiasi informazione riguardante una persona fisica identificata o identificabile. Questi dati possono essere raccolti, conservati e trattati solo con il consenso dell'interessato, oppure in base ad una legittima base giuridica come, ad esempio, per adempiere ad un obbligo di legge o per l'esecuzione di un contratto.

CONTESTO

La normativa prevede che i dati personali siano trattati in modo lecito, corretto e trasparente, e che vengano adottate tutte le misure necessarie per garantire la sicurezza e la riservatezza dei dati stessi. Inoltre, il titolare del trattamento dei dati deve fornire all'interessato informazioni chiare e complete su come i suoi dati verranno utilizzati e sui suoi diritti, tra cui il diritto di accesso, di rettifica, di cancellazione e di portabilità dei dati.

Il trattamento dei dati personali è soggetto a numerose limitazioni e vincoli, in particolare per quanto riguarda la raccolta, la conservazione e l'utilizzo di tali informazioni. I dati personali possono essere raccolti, conservati e trattati solo con il consenso dell'interessato, oppure in base ad una legittima base giuridica come, ad esempio, per adempiere ad un obbligo di legge o per l'esecuzione di un contratto.

LA LEGISLAZIONE PRIVACY IN ITALIA

Anno	Normativa di riferimento
1996	Legge n. 675 del 31 dicembre 1996 «Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali»
2003	Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali»
2016	REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 «relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)»
2018	DECRETO LEGISLATIVO 10 agosto 2018 , n. 101 . «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)»

LA LEGISLAZIONE PRIVACY IN ITALIA

La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il regolamento UE 679/2016 è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche.

LA LEGISLAZIONE PRIVACY IN ITALIA

Il trattamento dei dati personali deve essere al servizio dell'uomo.

Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica.

Il Regolamento UE 679/2016 – Alcune definizioni

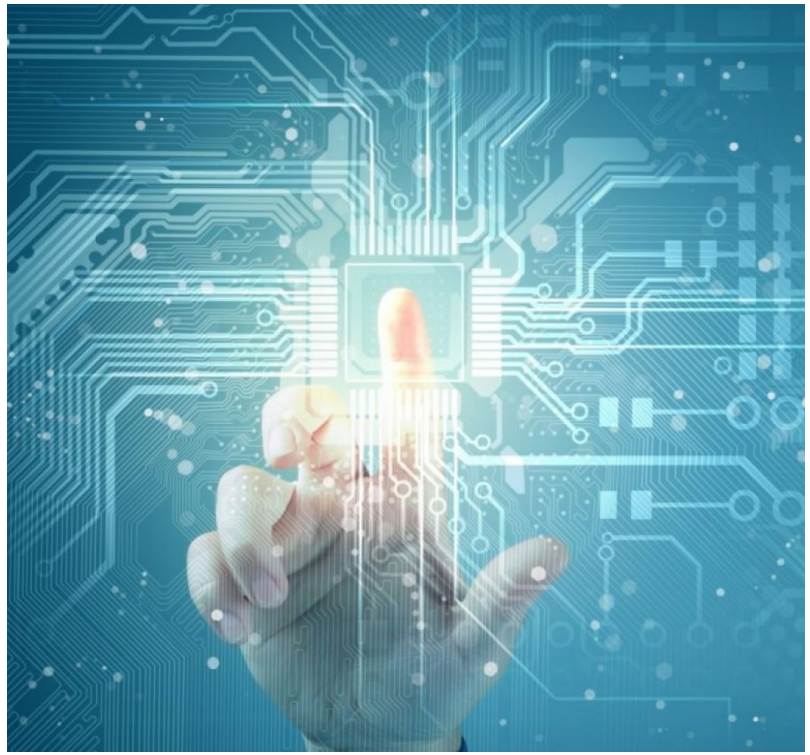
Art. 4 - DATO PERSONALE

Ai fini del presente regolamento s'intende per:

1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Il Regolamento UE 679/2016 – Alcune definizioni

Art. 4 - TRATTAMENTO



Ai fini del presente regolamento s'intende per:

2) «trattamento»: 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, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

Il Regolamento UE 679/2016 – Alcune definizioni

Art. 4 - TRATTAMENTO

Ai fini del presente regolamento s'intende per:

3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

6) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

Il Regolamento UE 679/2016 – Alcune definizioni

Art. 4 – TITOLARE E RESPONSABILE

Ai fini del presente regolamento s'intende per:

7) «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

Il Regolamento UE 679/2016 – Alcune definizioni

Art. 4 – INTERESSATO

Ai fini del presente regolamento s'intende per:

9) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

10) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

Art. 4 – CONSENSO

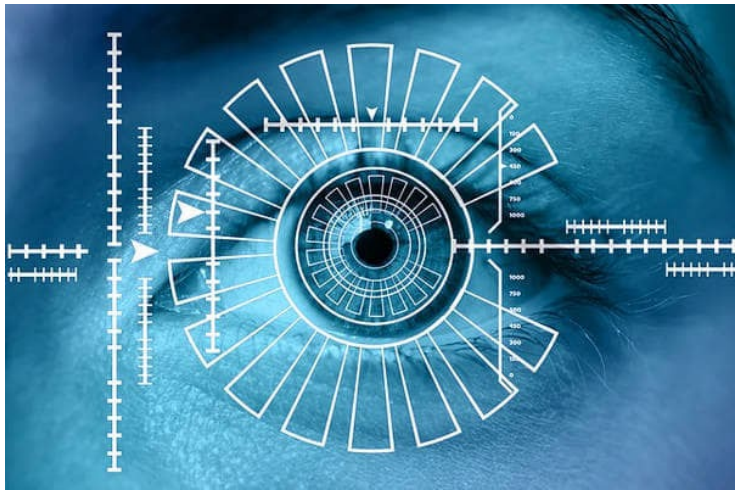
Ai fini del presente regolamento s'intende per:

11) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

12) «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

Il Regolamento UE 679/2016 – Alcune definizioni

Art. 4 – TIPOLOGI DI DATI



Ai fini del presente regolamento s'intende per:

13) «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

14) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

Il Regolamento UE 679/2016 – Alcune definizioni

Art. 4 – TIPOLOGI DI DATI

Ai fini del presente regolamento s'intende per:

15) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

I dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

I dati relativi alla salute della persona, rientrano nei dati ***" particolari "***

Il Regolamento UE 679/2016 – Alcune definizioni

Art. 9 – DATI PARTICOLARI

È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Quello che oggi viene chiamato dato particolare, nella precedente normativa era chiamato dato sensibile, ci si riferisce generalmente alla stessa tipologia di dati.

I dati relativi alla salute di una persona, quindi dati particolari, possono far riferimento a diverse informazioni, come lo stato di salute, ma anche relative alle prestazioni sanitarie **anche esser presente all'interno di una struttura sanitaria**, diventa dato relativo alla salute

Art. 9 – DATI PARTICOLARI

2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:

a) l'interessato ha prestato il proprio consenso esplicito	f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria
b) il trattamento è necessario per assolvere gli obblighi in materia di diritto del lavoro	g) il trattamento è necessario per motivi di interesse pubblico
c) il trattamento è necessario per tutelare un interesse vitale dell'interessato qualora l'interessato si trovi nell'incapacità fisica o giuridica	h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro
d) il trattamento è effettuato, da una fondazione o associazione che persegua finalità politiche, filosofiche, religiose o sindacali	i) il trattamento è necessario per motivi di interesse pubblico
e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;	j) il trattamento è necessario a fini di archiviazione nel pubblico interesse

Il Regolamento UE 679/2016 – Principi

Art. 5 – PRINCIPI

I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

Il Regolamento UE 679/2016 – Principi

Art. 5 – PRINCIPI

I dati personali sono:

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

e) 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; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

Il Regolamento UE 679/2016 – Principi

Art. 5 – PRINCIPI

I dati personali sono:

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Il Regolamento UE 679/2016 – Alcuni comportamenti

Comportamenti da tenere

Secondo la normativa privacy italiana, i dati personali sono definiti come qualsiasi informazione riguardante una persona fisica identificata o identificabile. Questi dati possono essere raccolti, conservati e trattati solo con il consenso dell'interessato, oppure in base ad una legittima base giuridica come, ad esempio, per adempiere ad un obbligo di legge o per l'esecuzione di un contratto.

La normativa prevede che i dati personali siano trattati in modo **LECITO, CORRETTO E TRASPARENTE**, e che vengano adottate tutte le misure necessarie per garantire la sicurezza e la riservatezza dei dati stessi. Inoltre, il titolare del trattamento dei dati deve fornire all'interessato informazioni chiare e complete su come i suoi dati verranno utilizzati e sui suoi diritti, tra cui il diritto di accesso, di rettifica, di cancellazione e di portabilità dei dati.

Il Regolamento UE 679/2016 – Alcuni comportamenti

Comportamenti da tenere

Chi lavora in una struttura sanitaria è obbligata tutti i giorno a trattare dati personali, il trattamento è necessario al fine di erogare la prestazione per la quale il cliente ha fatto accesso nella struttura.

ALLORA COME CI SI DEVE COMPORTARE?

È importante rispettare gli stessi obblighi in capo al titolare del trattamento:

- Gestire i dati in modo lecito
- Gestire il dato in modo corretto e trasparente
- Gestire il dato in maniera di garantire sicurezza e riservatezza

Gestire in dati in modo lecito

Per gestire i dati in modo lecito, basta semplicemente attenersi ai regolamenti interni e non usare in alcun caso i dati che abbiamo conosciuto in occasione dell'attività lavorativa.

Assolutamente vietato utilizzare i dati per fini personali o divulgare ad altri i dati.

I dati sono trattati in modo lecito se:

- Sono raccolti e trattati con il consenso dell'interessato
- Se sono trattati nel suo interesse, come salva vita o salvaguardia di interessi legali

Il Regolamento UE 679/2016 – Alcuni comportamenti

Gestire il dato in modo corretto e trasparente

Gestire i dati in modo corretto e trasparente, è necessario sempre attenersi ai regolamenti interni e comportarsi in modo corretto con l'utente. Ricordare che un comportamento sbrigativo e superficiale, può suscitare nei confronti dell'utente un sospetto di correttezza nella gestione del dato. In particolare è sempre consigliabile:

- Rendere disponibili l'informativa privacy
- Illustrare correttamente la finalità della raccolta
- Evitare una raccolta frettolosa del consenso
- Precompilare il consenso prima della firma
- Permettere all'utente di leggere l'informativa

Gestire il dato in maniera di garantire sicurezza e riservatezza

Gestire il dato in maniera di garantire sicurezza e riservatezza, è uno degli aspetti più importanti all'interno di una struttura sanitaria. Gli utenti saranno molto attenti alla discrezione del personale e saranno più attenti a comportamenti che possano ledere la lore riservatezza. Anche qui osservare i regolamenti interni, per evitare ogni tipo di violazione. In particolare:

- Non chiamare i pazienti per nome
- Far rispettare gli spazi di riservatezza
- Non lasciare documenti con dati in modo tale di essere visti
- Non lasciare schermi attivi, quando ci si allontana
- Conservare in modo ordinato ogni documento che contenga dati dell'utente

Il Regolamento UE 679/2016 – Consenso

Art. 7 – IL CONSENSO

Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

- Raccolta della firma è per avere prova del consenso
- Il consenso deve essere inequivocabile
- Il consenso è revocabile
- Il consenso del minore è valido se prestato da un maggiore di 16 anni, per i minori di anni 16 è prestato dal genitore o dal tutore legale del minore

I RUOLI DELLA PRIVACY

La normativa in materia di trattamento dei dati personali, prevede specifici ruolo e specifici compiti e responsabilità per ogni ruolo:

- Titolare del trattamento
- Responsabile del trattamento
- Responsabile della protezione dati (DPO)

Il Regolamento UE 679/2016 – Ruoli

IL TITOLARE

È la persona o l'organizzazione responsabile del modo in cui i dati personali vengono raccolti, utilizzati, conservati e protetti. Tra le sue responsabilità ci sono:

- Definire le finalità e i mezzi utilizzati per il trattamento
- Informare le persone
- Garantire che i dati siano trattati in modo sicuro e confidenziale
- Assicurarsi che i dati personali siano accurati e aggiornati
- Garantire che i diritti siano rispettati
- Garantire la conformità alle normative sulla privacy applicabili.

IL TITOLARE

Ogni titolare del trattamento sono tenuti a tenere un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene:

- I nome e i contatti del titolare,
- le finalità del trattamento
- Un descrizione della categoria di dati trattati e i sistemi di sicurezza

In caso di violazione, il titolare del trattamento notifica la violazione all'autorità di controllo competente entro 72 ore dal momento in cui ne è venuto a conoscenza. Poi quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

IL RESPONSABILE DEL TRATTAMENTO

l responsabile del trattamento è incaricato dal titolare dei dati personali è un'organizzazione o un individuo che viene designato dal titolare per eseguire specifiche attività di trattamento per suo conto. Il responsabile del trattamento incaricato deve trattare i dati personali solo secondo le istruzioni del titolare dei dati e in conformità con le leggi sulla protezione dei dati applicabili.

- Assicurarsi che i dati personali trattati siano protetti da accessi non autorizzati, perdita, distruzione o danneggiamento
- Tenere un registro delle attività di trattamento dei dati personali
- Notificare tempestivamente il titolare ogni caso di violazione
- Cura la tenuta del registro del responsabile

RESPONSABILE DELLA PROTEZIONE DATI (DPO)

Il Responsabile della protezione dati o DPO (Data Protection Officer) è una figura professionale responsabile della protezione dei dati personali all'interno di un'organizzazione. Ha il compito di monitorare l'adeguatezza del trattamento dei dati personali all'interno dell'organizzazione, fornendo supporto e consulenza ai responsabili del trattamento dei dati e ai titolari dei dati.

Il DPO può essere un dipendente dell'organizzazione o un consulente esterno, a patto che sia dotato di competenze specialistiche in materia di protezione dei dati personali e che operi in modo indipendente e imparziale.

Il Regolamento UE 679/2016 – Diritti dell'interessato

DIRITTI

A tutela degli interessi delle persone, sono poi sanciti una serie di diritti al quale il titolare non può opporsi e che vanno sempre garantiti, in particolare:

1.Diritto di accesso: l'interessato ha il diritto di accedere ai propri dati personali e di ricevere informazioni su come vengono trattati.

2.Diritto di rettifica: l'interessato ha il diritto di richiedere la correzione dei propri dati personali inesatti o incompleti.

3.Diritto di cancellazione (o "diritto all'oblio"): l'interessato ha il diritto di richiedere la cancellazione dei propri dati personali, ad esempio se non sono più necessari per gli scopi per cui sono stati raccolti.

Il Regolamento UE 679/2016 – Diritti dell'interessato

DIRITTI

Segue…..

4.Diritto di limitazione del trattamento: l'interessato ha il diritto di chiedere che il trattamento dei propri dati personali sia limitato, ad esempio se ritiene che i dati siano inesatti o che il trattamento sia illecito.

5.Diritto alla portabilità: l'interessato ha il diritto di ricevere i propri dati personali in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e di trasferire tali dati a un altro titolare del trattamento.

6.Diritto di opposizione: l'interessato ha il diritto di opporsi al trattamento dei propri dati personali per motivi legittimi, ad esempio se ritiene che il trattamento violi i propri diritti fondamentali.

Il Regolamento UE 679/2016 – Sanzioni

TUTELE E SANZIONI

Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

Il titolare che si verifichi responsabile di violazione della norma in tema di protezione dei dati, può subire una sanzione che va **dal 2% al 4% del fatturato totale annuo** dell'esercizio precedente.

Per particolari condotte lesive dell'interessato è prevista anche una pena detentiva che, a seconda dei casi, va da sei mesi a tre anni.

DOCUMENTI PRIVACY AZIENDALI

CONSEGNA REFERTO

ISTRUZIONE CORRETTA INFORMAZIONE ALL'UTENZA

ISTRUZIONE GESTIONE COMUNICAZIONE

INFORMATIVA PER IL TRATTAMENTO DEI DATI

GRAZIE

IZIANO

SERVIZI E FORMAZIONE