Locasciulli Studio Legale
Via Tevere n. 20
00198 - Roma

GDPR

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

REGOLAMENTO (UE) 2016/679

Il regolamento UE 2016/679 è entrato in vigore il 25 maggio 2018

- Il Regolamento rappresenta una fonte normativa dell'UE che rende il contenuto precettivo delle norme immediatamente applicabile all'interno dei paesi membri
- Attualmente rappresenta la principale fonte normativa in materia di *data protection*
- Il Governo ha approvato uno schema preliminare di Decreto Legislativo volto ad allineare il quadro normativo nazionale alla nuova normativa UE – il testo è in attesa del vaglio delle Commissioni parlamentari

PERCHÉ IL GDPR?

➢ La proposta di un nuovo quadro giuridico per la protezione dei dati personali è stata dettata da:

- Eccessiva frammentazione nelle legislazioni nazionali
- Differenze nelle discipline applicabili
- Sanzioni non adeguate
- Difficoltà nel garantire il rispetto delle norme e la tutela degli interessati

Le Definizioni
e
I Principi Generali del Nuovo Regolamento

➔ Cos'è un Trattamento?

- Ha ad oggetto i dati personali
- rileva la FINALITA' ovvero lo scopo effettivo per cui i dati personali sono di volta in volta trattati
- le finalità devono essere esplicitate per ciascuna operazione di trattamento.

I PRINCIPI GENERALI

Sono introdotti e rafforzati alcuni principi in materia di protezione dei dati personali

→Principio di proporzionalità

I dati che vengono raccolti e trattati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (cosiddetta "minimizzazione dei dati")

I Principi generali

→Diritto All'oblio – Right to be forgotten

Il titolare del trattamento deve garantire all'interessato la cancellazione dei dati che lo riguardano senza ingiustificato ritardo

I principi generali

➔Portabilità dei Dati

l'interessato ha il diritto d vedersi garantita la trasmissione diretta dei dati personali da un titolare all'altro, se tecnicamente fattibile, senza impedimenti

IL DIRITTO ALLA PORTABILITA' DEI DATI

- Consente all'interessato di ricevere i propri dati in un formato strutturato, di uso comune e di trasmetterli ad altro titolare
- Facilita il passaggio da un fornitore di servizi all'altro
- Può essere accordata se i dati sono trattati sulla base del consenso o di un contratto

I principi generali

➔Privacy by design e privacy by default

Il GDPR obbliga di assicurare che le misure adottate attuino efficacemente i principi di:

- privacy by design (*id est*, protezione dei dati fin dalla progettazione)
- privacy by default (*id est*, impostazione predefinita che preveda il trattamento dei soli dati necessari al perseguimento delle finalità)

I Principi generali

➔Consenso

Il consenso deve essere esplicito e prestato liberamente: il GDPR richiede che l'interessato acconsenta al trattamento dei dati personali con atto positivo, libero, specifico e inequivocabile con il quale dimostri la decisione libera, specifica e informata di accettare il trattamento dei dati personali che lo riguardano

I PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI

- Liceità, correttezza e trasparenza
- Devono essere raccolti per finalità determinate, esplicite, legittime e trattati in modo non incompatibile con le finalità
- I dati devono essere esatti e quindi aggiornati
- La loro conservazione non può essere superiore al tempo necessario alle finalità del trattamento
- Integrità e riservatezza
- Accountability - responsabilizzazione

I DIRITTI RAFFORZATI NEL CASO DI PROFILAZIONE

COS'E' LA PROFILAZIONE?

Qualsiasi forma di trattamento **automatizzato** di **dati personali**, inclusi gli identificativi on-line, finalizzato a **valutare** determinati aspetti personali di una persona fisica (es. rendimento professionale, situazione economica, preferenze personali, interessi, affidabilità, comportamento ecc.)

Diritto dell'interessato nel caso di profilazione

- Diritto di essere informato sulle modalità di svolgimento del processo di profilazione
- Diritto di accesso
- Diritto di opporsi in qualsiasi momento al trattamento per finalità di marketing diretto

I SOGGETTI COINVOLTI NEL TRATTAMENTO

CAMPO DI APPLICAZIONE

A chi si applica la nuova normativa?

ART. 1 – oggetto e finalità

1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.

2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali

ART. 2 – ambito di applicazione materiale

Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi

ART. 3 – ambito di applicazione territoriale

Il regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione;

al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione ma offre servizi a tali interessati (anche senza pagamento) o monitora il loro comportamento

Locasciulli Studio Legale

Modalità di trattamento dei dati delle persone giuridiche

I dati delle persone giuridiche sono dati "personali"?

NO

Il GDPR concerne solo le persone fisiche.

i dati delle persone giuridiche non vengono considerati come dati personali

(Es: numero di P.IVA - denominazione sociale) Sono invece considerati dati personali tutti i dati relativi alle persone fisiche che prestano la loro opera all'interno dell'Azienda

I PROTAGONISTI

Il nuovo sistema vede la presenza di 2 protagonisti

- IL TITOLARE - colui che decide tempi e modi del trattamento
- L'INTERESSATO – è il proprietario dei dati personali

IL TITOLARE

- Ha l'obbligo di proteggere i dati by default e by design; quindi deve trattare meno dati personali possibili e proteggerli fin dall'inizio in modo adeguato, tenendo conto di tutte le tecnologie disponibili , ma soprattutto effettuando una valutazione dei RISCHI per i diritti degli interessati
- Su di lui incombe l'obbligo di progettare in maniera efficace il sistema di data protection del quale diventa *accountable* *(id est responsabile)*.

Vengono definiti dei NUOVI RUOLI

- Titolare del trattamento
- Responsabile del trattamento
- Autorizzato al trattamento
- Data protection officer – D.P.O.

Il titolare, diventa accountable e, pertanto, deve rispondere dei risultati ed è chiamato a progettare il sistema di data protection in conformità al GDPR

- **FOCUS SULL' ACCOUNTABILITY**

- Maggiore assunzione di responsabilità da parte del titolare e maggiore coinvolgimento dei soggetti che intervengono nel trattamento dei dati

- Obbligo di dimostrare la conformità e l'efficacia delle misure adottate

- Obbligo di prevenire i rischi mediante la predisposizione di misure adeguate

LA NUOVA FIGURA DEL D.P.O.

La sua nomina è obbligatoria nei seguenti casi:

- il titolare è una autorità pubblica
- il trattamento è effettuato da un'organizzazione avente più di 500 interessati nell'arco di di 12 mesi
- le attività principali del Titolare consistono in operazioni di trattamento che richiedono un monitoraggio regolare e sistematico su larga scala
- le attività di monitoraggio del titolare consistono in attività di trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati

FOCUS

quando un trattamento può dirsi operante su larga scala, quali sono gli elementi da temerei considerazione?:

➢Il numero dei soggetti interessati dal trattamento espresso in termini assoluti, ovvero espressi in percentuale della popolazione di riferimento

➢Il volume dei dati, le diverse tipologie dei dati oggetto del trattamento

➢ la durata del trattamento

➢ la portata geografica dell'attività di trattamento

Locasciulli Studio Legale

RICAPITOLANDO LE PRINCIPALI CARATTERISTICHE DELLA NUOVA FIGURA PROFESSIONALE DEL D.P.O.

- Ha approfondite conoscenze della legge sulla protezione dei dati e in materia di sicurezza delle informazioni.
- familiarità con le tecnologie informatiche.
- Deve vigilare e verificare sull'efficacia e l'efficienza delle misure poste in essere dal titolare del trattamento

Garanzie di indipendenza

- Il titolare non può interferire nello svolgimento dei compiti del DPO
- Il DPO non può essere sanzionato o licenziato per lo svolgimento dei compiti a lui attribuiti
- Insussistenza di una responsabilità individuale
- Vengono identificate delle ipotesi di incompatibilità qualora sussista un conflitto di interessi

I NUOVI STRUMENTI DELLA CONFORMITA'

Applicazione del principio della Privacy by design e privacy by default – ART. 25

Privacy by design: il titolare mette in atto misure tecniche e organizzative volte ad attuare efficacemente i principi di protezione dei dati, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento

Privacy by default: il titolare mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati per impostazione predefinita solo i dati personali necessari per ogni specifica finalità del trattamento

LA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI (DPIA)

Art. 35 GDPR

- 1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

- 2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.

- 3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:
- a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
- c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

LA PROCEDURA DI VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI

- Finalizzata alla descrizione ed analisi dei trattamenti al fine di valutarne i rischi e individuare le misure idonee alla prevenzione e/o gestione
- E' uno strumento di accountability
- è obbligatoria solo in alcuni casi

Misure di sicurezza del trattamento dei dati

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonchè della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, **il titolare del trattamento** e **il responsabile del trattamento** mettono in atto misure tecniche e organizzative adeguate per **garantire un livello di sicurezza adeguato al rischio**, che comprendono, tra le altre, se del caso:

a) La pseudonomizzazione e la cifratura dei dati personali;

b) La capacità di assicurare su base permanente la riservatezza, l'integrità la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) Una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

DATA BREACH E SISTEMA SANZIONATORIO

COS'E' IL DATA BREACH?

ART. 4

una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, perdita, modifica, divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati

Nel caso di una violazione di dati personali, il titolare del trattamento notifica la violazione ***all'autorità di controllo*** *competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo*

CARATTERISTICHE DELLA NOTIFICA

La notifica di cui al paragrafo 1 deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali; d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo

FOCUS: il processo di notifica

- Il **RESPONSABILE** del trattamento comunica la violazione al titolare del trattamento
- Il **TITOLARE** del trattamento provvede a notificare la violazione all'autorità garante e/o agli interessati
- Il **TITOLARE** deve provvedere alla compilazione e tenuta di un registro interno dei rischi
- La mancata ottemperanza comporta l'applicazione di **sanzioni amministrative**

Locasciulli Studio Legale

IL SISTEMA SANZIONATORIO

Il sistema sanzionatorio si inasprisce

- **Responsabilità civile per il c.d.** danno da trattamento. Art. 82: «*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*».

- **Responsabilità amministrativa:** sanzioni fino a 20 Milioni di Euro o al 4% del fatturato mondiale

- **Responsabilità penale:** solo se prevista dai singoli paesi.

APPLICAZIONI CONCRETE NEL MONDO SANITARIO

Locasciulli Studio Legale

Il trattamento dei dati sanitari secondo la nuova disciplina dettata dal GDPR

Non è prevista una disciplina specifica per il trattamento dei dati personali effettuato in ambito sanitario, tuttavia la materia è stata oggetto di attenzione da parte del legislatore comunitario

Considerando n. 35

Nei dati personali relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio (1); un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro.

Cosa si intende per dati relativi alla salute?

ART. 4 N. 15

dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelino informazioni relative allo stato di salute

I Dati Sanitari sono qualificati come DATI SENSIBILI/ PARTICOLARI e, pertanto, sottoposti alla specifica tutela di cui all'art. 9

ART. 9

È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonchè 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.

DEROGHE AL DIVIETO

IL TRATTAMENTO DEI DATI SANITARI è CONSENTITO QUANDO SIA NECESSARIO ALL'EROGAZIONE DELLA PRESTAZIONE SANITARIA COMPLESSIVAMENTE INTESA

Es: valutazione capacità lavorativa del dipendente

LA C.D. SANITA' ELETTRONICA

L'obiettivo è quello di costruire un moderno sistema sanitario in rete tra tutti i soggetti interessati e i cittadini.

STRUMENTI

- Cartella sanitaria elettronica
- Dossier sanitario
- ricetta elettronica
- Certificati di malattia telematici

Principi specificamente applicabili al settore

- Accountability
- Privacy by design e privacy by default
- Principio di trasparenza

Adempimenti

- Data protection impact assessment
- Registro del trattamento dei dati
- Data breach

CONCLUSIONI

Nella vigenza della precedente normativa contenuta nel D.Lgs 196/2003, al fine di essere esenti da responsabilità era sufficiente adeguarsi alle regole di volta in volta emanate

Il Nuovo sistema delineato dal GDPR, invece, definisce un modello di gestione dei dati che determina una **responsabilizzazione** del titolare e di tutti i soggetti coinvolti nel trattamento, i quali hanno l'onere di applicare i sistemi che ritengono più opportuni per una corretta e sicura gestione dei dati