SODALIS
CSV SALERNO

2021

GDPR

GENERAL DATA PROTECTION

Sintesi dei contenuti

01
Presentazione del regolamento

02
Il GDPR: proviamo a sintetizzare per elementi chiave

03
Ambito di applicazione materiale e territoriale

04
Dati personali e particolari categorie di dati

05
Cosa impone il regolamento?

06
Principi e Diritti

07
Un modello di riferimento per l'implementazione

08
Il regime sanzionatorio

PRESENTAZIONE DEL REGOLAMENTO

Il Regolamento UE n. 679/2016 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 (di seguito denominato GDPR) è entrato in vigore il 24 maggio 2016 ed è applicabile dal 25 maggio 2018, abrogando ipso facto la Direttiva95/46/CE.
La Carta dei diritti fondamentali dell'Unione europea e il Trattato sul funzionamento dell'Unione Europea stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano, pertanto la privacy viene a configurarsi come tutela dei diritti e delle libertà fondamentali.
Il GDPR intende contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica correlata al progresso economico, al rafforzamento e alla convergenza delle economie di mercato interno e del benessere delle persone fisiche.
Con il GDPR si istituisce un quadro normativo incentrato sui doveri e sulla responsabilizzazione del Titolare del trattamento dei dati, che costituisce il punto centrale della normativa in materia di protezione dei dati personali. L'elemento di differenziazione dalla precedente normativa (Decreto Legislativo196/2003) va ricercato nell'approccio generale alla disciplina della privacy che richiede non solo il rispetto dei principi in esso contenuti, ma anche di comprovare l'applicazione e l'adozione di una serie di strumenti che lo stesso GDPR indica, a partire da un'attenta valutazione dei rischi e degli impatti.
Data la complessità dei temi trattati, le pagine di seguito forniscono una chiave di lettura sintetica in modo da consentire un primo approccio alla governace dei requisiti "facilitato".

IL GDPR: PROVIAMO A SINTETIZZARE PER ELEMENTI CHIAVE

Il GDPR sposa il principio di "accountability" o responsabilizzazione.

Il concetto di "responsabilizzazione" si traduce nel fatto che il Titolare è chiamato a dimostrare che i trattamenti sono coerenti con il disposto del GDPR, a pianificare e mettere in atto misure tecniche e organizzative per poterne comprovare l'adeguatezza, e ad attivare un modello di monitoraggio delle misure tecnico-organizzative implementate, conseguentemente due sono i presupposti chiave dell'impianto del GDPR:

- **privacy by design**: necessità di disegnare le misure di sicurezza e privacy già in fase di progettazione dei sistemi informativi e dei flussi di attività;
- **privacy by default**: vale a dire la capacità di disegnare le misure di sicurezza e privacy per default, come prerequisito di normale funzionamento dei sistemi organizzativi.

AMBITO DI APPLICAZIONE MATERIALE E TERRITORIALE

Il GDPR si applica a qualsiasi trattamento di dati personali (che riguardano una persona fisica) contenuti in un archivio o destinati a figurarvi, in modo indipendente dal fatto che si tratti di un trattamento interamente, parzialmente automatizzato, oppure non automatizzato.
Il legislatore europeo ha elencato all'art.2 par. 2, i trattamenti dei dati personali a cui il Regolamento non si applica.
L'art. 3 disciplina l'ambito di applicazione territoriale: il regolamento si applica ad ogni trattamento che ha ad oggetto dati personali, e a tutti i titolari (controller) e responsabili (processor) del trattamento stabiliti nel territorio dell'Unione, ma anche in generale a quelli che, offrendo beni e servizi a persone residenti nell'Unione, trattano dati di residenti nell'Unione europea (art. 3 del Regolamento). In tal modo la sua applicazione non è limitata alle sole organizzazioni che si trovano in Europa, ma tutela tutti gli interessati che risiedono nel territorio dell'Unione indipendentemente da dove si attua il trattamento dei loro dati.

DATI COMUNI E PARTICOLARI CATEGORIE DI DATI

Il GDPR pone al centro dell'impianto normativo il dato personale.

Come si identifica il dato comune?
Per dato comune si intende "qualsiasi informazione riguardante una persona fisica identificata o identificabile" (nominativo, data di nascita, numero di cellulare. gli studi compiuti...).

Come si identificano le particolari categorie di dati?
In relazione alla tipologia di informazioni da esse veicolate. Si tratta di tutti i dati atti a rivelare l'origine razziale o etnica, le opinioni politiche, l'appartenenza sindacale e le convinzioni religiose o filosofiche di un individuo, insieme alle informazioni genetiche, ai dati biometrici, alle notizie in merito alla salute, alla vita o all'orientamento sessuale della persona (articolo 9) e alle informazioni relative ai reati o alle condanne penali (articolo 10).

La normativa identifica le seguenti categorie di dati:

- *Dati genetici: sono i dati relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, che forniscono informazioni univoche sulla sua fisiologia o sulla sua salute, e sono desumibili in particolare dall'analisi di un suo campione biologico.*
- *Dati biometrici: sono i dati ottenuti da un trattamento tecnico specifico che forniscono informazioni relative alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, consentendone o confermandone l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.*
- *Dati relativi alla salute: sono i dati 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.*
- *Dati relativi a condanne penali o reati: sono i dati relativi alle condanne penali, ai reati o a connesse misure di sicurezza.*

Perché il focus sui dati particolari?
Alla violazione dei dati "particolari" è associato un rischio maggiore per i dirittie le libertà fondamentali degli individui a cui le informazioni si riferiscono conseguentemente il trattamento dei dati personali appartenenti a queste "categorie particolari" necessita perciò di maggiori cautele e garanzie.

COSA IMPONE IL REGOLAMENTO?

Il trattamento delle categorie particolari di dati personali di cui al citato articolo 9 è sempre vietato a meno che:

- l'individuo abbia prestato il proprio consenso esplicito al trattamento di tali dati per finalità specifiche;
- il trattamento sia necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare del trattamento o dell'individuo in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
- il trattamento sia necessario per tutelare un interesse vitale di un individuo o di un'altra persona fisica qualora l'individuo si i trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- il trattamento sia effettuato 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 dette entità, avvenga in relazione a fini che sono loro propri e che i dati personali non siano comunicati all'esterno senza il consenso dell'individuo;
- il trattamento riguardi dati personali resi manifestamente pubblici dall'individuo;
- il trattamento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria; il trattamento sia necessario per motivi di interesse pubblico;
- il trattamento sia necessario 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, fatti salvi i casi in cui i dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza;
- il trattamento sia necessario 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;
- il trattamento sia necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, sia proporzionato alla finalità perseguita, rispetti l'essenza del diritto alla protezione dei dati e preveda misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'individuo.

Il trattamento di dati personali relativi a condanne penali e reati o a connesse misure di sicurezza di cui al citato articolo 10 è sempre vietato a meno che esso avvenga sotto il controllo dell'autorità pubblica, oppure per autorizzazione del diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

ACQUISIZIONE DEL CONSENSO DA PARTE DELL'INTERESSATO

Ciascun titolare deve distinguere i casi in cui per eseguire un trattamento è richiesto il (previo) consenso dell'interessato, da quelli in cui non è necessario acquisirlo. La richiesta del consenso deve essere presentata in modo distinto da altre richieste, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Quando per un trattamento è necessario il consenso, il titolare deve essere in grado di dimostrare che il consenso è stato effettivamente prestato.

TRATTAMENTO DI PARTICOLARI CATEGORIE DI DATI

È formalizzato il divieto generale del trattamento dei dati corrispondenti a quelli attualmente definiti 'sensibili', oltre che dei dati genetici e biometrici. Dopodiché sono disposte specifiche eccezioni al divieto, come quelle relative alle ipotesi in cui: l'interessato ha prestato il consenso; i dati sono trattati per eseguire un contratto di lavoro e per le connesse esigenze di sicurezza/protezione sociale; i dati sono trattati a fini di tutela di un interesse vitale dell'interessato; i dati personali sono stati resi pubblici dall'interessato, ecc.

PRINCIPI E DIRITTI

QUALI SONO I PRINCIPI CARDINE?

I principi cardine rispetto al trattamento dei dati con cui familiarizzare, sono:

- (art.5) liceità del trattamento che può essere possibile solo se l'interessato ha espresso un esplicito consenso(che il Titolare deve dimostrare di aver raccolto),
- (art.7), adeguatezza, pertinenza e non eccedenza dei dati rispetto alle finalità per cui vengono trattati.

In sintesi, nella matrice principi cardine e linee di azione

- **Liceità e correttezza= nelle modalità di raccolta e scopo di utilizzo.**
- **Finalità= i dati raccolti per una finalità specifica non possono essere utilizzate per altri scopi.**
- **Minimizzazione= raccogliere solo le informazioni essenziali per il raggiungimento dello scopo.**
- **Esattezza e aggiornamento= i dati devono corrispondere ad informazioni esatte ed aggiornate.**
- **Pertinenza e completezza= i dati devono essere pertininenti allo scopo dichiarato e non devono essere incompleti o parziali.**

QUALI SONO I DIRITTI DELL'INTERESSATO?

- **Informativa** sul trattamento (art.12) laddove si evidenzia che deve essere fatta in forma concisa, trasparente, intellegibile e facilmente comprensibile e laddove si pone attenzione alla necessità di fornire precise indicazioni (art.13)sulla finalità del trattamento, gli eventuali destinatari/utilizzatori dei dati, il periodo di conservazione dei dati, le modalità per richiedere rettifica o cancellazione degli stessi;
- **Accesso** ai dati da parte dell'interessato (art.15) che prevede al comma 3 la possibilità dell'interessato di ricevere copia dei dati trattati;
- **Rettifica e cancellazione** dei dati: diritto di rettifica (art.16), di cancellazione c.d. diritto all'oblio(art.17)e di limitazione del trattamento (art.18) con obbligo di notifica all'interessato in caso di rettifica, cancellazione o limitazione (art.19);
- **Portabilità** dei dati: l'interessato ha il diritto di ricevere in formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano e ha il diritto di trametter questi dati ad altro Titolare (art.20);
- **Diritto di opposizione**: diritto dell'interessato di opporsi al trattamento dei dati che lo riguardano in qualsiasi momento (art. 21) e diritto di non essere sottoposto a un processo decisionale automatizzato, compresa la profilazione (art.22).

UN MODELLO DI RIFERIMENTO PER L'IMPLEMENTAZIONE

Un modello di riferimento per l'implementazione: l'APPENDICE A fornisce un aiuto pratico per l'implementazione del regolamento nelle singole associazioni.

Un possibile modello di governance e di gestione delle azioni previste dal GDPR deve muoversi su 5 direttrici di sviluppo:

1. **Dove e quali sono i dati?**
2. **Quali rischi e quali impatti?**
3. **Quali misure organizzative adottare?**
4. **Quali misure tecniche di sicurezza?**
5. **Quali misure tecniche sugli applicativi?**

Si rimanda all'Appendice A

IL REGIME SANZIONATORIO

Solo poche righe per ricordare che il trattamento illecito dei dati o la perdita di dati prevede sia responsabilità di natura penale per la mancata adozione di misure minime di sicurezza, sia responsabilità di natura civile in quanto l'omissione di misure idonee determina un obbligo risarcitorio di cui all'art.2050 del Codice Civile e ai sensi dell'art.15.del D.Lgs.196/03 sia responsabilità di tipo amministrativo.
In meritoa quest'ultime, il nuovo GDPR (art.83) prevede sanzioni amministrative pecuniarie fino a 10 milioni di euro e per le imprese pari al 2% del fatturato di gruppo mondiale in caso di violazione degli obblighi del Titolare del trattamento (art.8,11 da 25 a 39, 42, 43) e fino a 20 milionidi euro e per le imprese pari al 4% del fatturato di gruppo mondiale in caso di violazione delle condizioni relativeal consenso (art. 5,6,7,9) al rispetto dei diritti dell'interessato (art. da 12 a 22) e dei trasferimenti dati da un Titolare all'altro di Paesi.

LA DOCUMENTAZIONE È DISPONIBILE AL SEGUENTE LINK:

https://www.csvsalerno.it/blog/2021/05/20/guida-per-la-tutela-della-privacy/

SODALIS
CSV SALERNO

Sede centrale: corso Vittorio Emanuele, 58
84123 – Salerno
Telefono: 089 2756511
PEC: csvsalerno@pec.it