GDPR (General Data Protection Regulation)

FNA
Federamministratori

UNICOND
FEDERAMMINISTRATORI
CONFAPPI
CONFEDERAZIONE PICCOLA PROPRIETA' IMMOBILIARE

Programma

- Dal Codice Pirvacy al Regolamento Europeo
- I tre pilastri del GDPR

Le sanzioni

Sanzioni da €. 10.000.000 a €. 20.000.000 o dal 2% al 4% del fatturato mondiale nel caso in cui siano violati:

- Principi relativi al trattamento e al consenso
- Disposizioni relative ai diritti dell'interessato
- Disposizioni in materia di trasferimento dati
- Ordine di cessazione del trattamento

Si lascia agli stati membri il compito di disciplinare le regole l'effettiva applicazione delle sanzioni amministrative

Il problema

Dal Codice Privacy al Regolamento Europeo, principi di base e adempimenti di maggior rilievo

L’agonizzante D.Lgs. 196/2003

Nel 1996, attraverso la Legge 675, viene introdotto nel nostro ordinamento un nuovo diritto, il diritto alla protezione dei dati personali.

Nel 2003 tale legge è stata abrogata e sostituita dal D.Lgs. 196/2003, il «Codice in materia di protezione dei dati personali», entrato in vigore il primo gennaio 2004.

Di fondamentale importanza l’articolo d’esordio del Codice in quanto definisce il significato della parola Privacy:

«CHIUNQUE HA DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI CHE LO RIGUARDANO (…)»

Il nuovo Regolamento UE 2016/679

25 Maggio 2018

Entra in vigore il GDPR, nuovo regolamento europeo in materia di protezione dei dati personali (n. 679/2016) in tutti gli stati membri dell'Unione europea.

Chi deve adeguarsi ?

Tutte le Aziende stabilite sul territorio europeo e le Aziende extra UE che vendono beni o prestano servizi sul territorio europeo

Sanzioni

Ammende fino a 20 milioni di euro o fino al 4%

A chi si applica il DGPR?

Oltre ai Soggetti economici stabiliti nell'Unione Europea … il GDPR si applica 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, quando le attività di trattamento riguardano:

- l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
- il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione

E tutti noi coi nostri device?

Il regolamento non si applica ai trattamenti di dati personali: effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico.

Attenzione: rischio richieste risarcimento danni!

Cos’è un «dato personale»?

«Dato personale» è

- Qualsiasi informazione riguardante
- Una persona fisica
- Identificata o identificabile («interessato»);

Ci sono «dati» e «dati» …

Una volta stabilito che un'informazione è un dato personale, dobbiamo individuare la sua categoria di appartenenza, ovvero chiederci se rientra nella categoria dei:

- ✓Dati personali comuni
- ✓Dati personali particolari
- ✓Dati personali giudiziari

Perché mai?

Perché a ciascuna categoria, GDPR e Provvedimenti del Garante riservano:

- ✓Modalità di trattamento
- ✓Profili relativi alla sicurezza differenti

I dati personali di tipo comune

Sono definiti per esclusione, ovvero: sono tutti i dati personali diversi da quelli particolari o giudiziari.

Esempi di dati personali comuni sono i dati anagrafici relativi a una persona fisica o giuridica (nominativo, indirizzo, partita IVA, codice fiscale, indirizzo e-mail, indirizzo web, ecc.)

I dati di tipo «particolare»

I dati particolari, sono i dati personali che rivelino:

- l'origine razziale o etnica
- le opinioni politiche
- le convinzioni religiose o filosofiche
- l'appartenenza sindacale
- dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica
- dati relativi alla salute
- dati relativi alla vita sessuale o all'orientamento sessuale della persona

I dati di tipo giudiziario

Dati personali relativi:

- alle condanne penali e ai reati
- a connesse misure di sicurezza

Quando posso trattare dati comuni?

LE BASI LEGALI DEL TRATTAMENTO

Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore

Quando posso trattare dati particolari?

LE BASI LEGALI DEL TRATTAMENTO

E’ vietato trattare dati particolari!

Il divieto non si applica se si verifica uno dei seguenti casi:

1. l’interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto all’Unione o degli Stati membri dispone che l’interessato non possa revocare il divieto di trattare dati particolari;
2. il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell’interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale (…)

Quando posso trattare dati giudiziari?

LE BASI LEGALI DEL TRATTAMENTO

Il trattamento dei dati giudiziari, deve avvenire soltanto:

- sotto il controllo dell'Autorità Pubblica
- se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'Autorità Pubblica.

Il «consenso» come base legale

«Consenso»: qualsiasi manifestazione di volontà

- libera
- specifica
- informata
- 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

Condizioni del «consenso»

1. Per i dati sensibili, il consenso **DEVE essere «esplicito»** (anche per il consenso a decisioni basate su trattamenti automatizzati, compresa la profilazione – art. 22)
2. **NON deve essere necessariamente «documentato per iscritto», né è richiesta la «forma scritta»,** anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere «esplicito» (per i dati sensibili)
3. il titolare (art. 71) **DEVE essere in grado di dimostrare che l'interessato ha prestato il consenso** a uno specifico trattamento
4. Il **consenso dei minori è valido a partire dai 16 anni**; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

5. **DEVE** essere, in tutti i casi: LIBERO, SPECIFICO, INFORMATO e INEQUIVOCABILE e **NON** è ammesso il consenso tacito o presunto (**no a caselle prespuntate su un modulo**)
6. **DEVE** essere manifestato attraverso **«dichiarazione o azione positiva inequivocabile»**
7. **Il consenso può essere ritirato in qualsiasi momento**

Quando inizia il «trattamento» dei dati?

Trattamento è

- **qualsiasi operazione** o insieme di operazioni, compiute **con o senza l'ausilio di processi automatizzati** e applicate a dati personali o insieme 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

Le figure coinvolte

I Soggetti del trattamento sono i player, i protagonisti sullo scenario privacy delineato dal GDPR e si chiamano:

1. Interessato
2. Titolare del trattamento – Data Controller
3. DPO – Data Protection Officer
4. Responsabile del trattamento – Data Processor
5. Persone autorizzate al trattamento dei dati personali

L’interessato

E’ la persona fisica a cui si riferiscono i dati personali.

I dati personali **rimangono sempre di proprietà dell’interessato** il quale, alle condizioni indicate nell’Informativa, può concederli «in prestito» ad un determinato Titolare.

Il Titolare del trattamento – Data Controller

Titolare del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina:

- le finalità
- i mezzi del trattamento di dati personali

Il DPO – Il Data Protection Officer

Chi deve nominare un DPO?

La designazione di un DPO è obbligatoria:

- se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;
- se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala, oppure
- se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

Conoscenze e competenze del DPO

Il DPO «è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all’art. 39».

Chi è il DPO?

COMPITI DEL DPO

A) Informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti;
B) Sorvegliare l'osservanza del Regolamento (…), nonché delle policy in materia di protezione dei dati personali, compresi: a) l'attribuzione delle responsabilità; b) la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
C) Fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento: - cooperare con l'autorità di controllo; - fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento

Il Responsabile del trattamento – Data Processor

Il Responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che:

- il trattamento soddisfi i requisiti del GDPR
- garantisca la tutela dei diritti dell'interessato.

Sub Data Processor

Un responsabile del trattamento può nominare un altro responsabile del trattamento?

SI

Il GDPR consente la nomina di sub-responsabili del trattamento da parte di un responsabile per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario;

Il Responsabile primario risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso «non gli è in alcun modo imputabile»

Persone autorizzate al trattamento

Alla luce del principio di «accountability» prevede l'adozione di misure atte a garantire proattivamente l'osservanza del regolamento nella sua interezza, titolari e responsabili del trattamento

mantengono in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento

così come delineatesi negli anni anche attraverso gli interventi del Garante

Ma cosa vuole l'Ordinamento da noi?

IL PRINCIPIO DI «ACCOUNTABILITY»

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché 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 …

… al rischio di «data breach», ovvero, la violazione di sicurezza che comporta accidentalmente o in modo illecito:

- la distruzione
- la perdita
- la modifica
- la divulgazione non autorizzata
- l'accesso ai dati personali trasmessi conservati o comunque trattati

Il Titolare deve dimostrare di rispettare i principi e il GDPR statuisce che questa è sua responsabilità

Come posso dimostrare la compliant?

Il Titolare deve:

a) Implementare idonee misure tecniche ed organizzative in grado di assicurare e dimostrare la compliance. Questo può includere policy interne relative alla protezione dei dati personali quali: STAFF TRAINING; INTERNAL AUDITS DELLE ATTIVITA' DI TRATTAMENTO; REVISIONI DELLE HAR POLICY;
b) Conservare idonea documentazione relativa alle attività di trattamento;

c) Quando opportuno (o necessario) nominare un DPO (Data Protection Officer);

d) Implementare misure che rispettano i principi di PbD (Privacy by Design) e Privacy by Default. Misure che includono: la MINIMIZZAZIONE dei dati personali; la PSEUDONIMIZZAZIONE; la TRASPARENZA; la possibilità per gli interessati di monitorare il trattamento dei dati; creare e migliorare funzionalità di sicurezza in modo continuo.

L’adempimento chiave del GDPR

L’INFORMATIVA ALL’INTERESSATO

L’informativa va sempre resa all’Interessato prima della raccolta dei dati personali.

Nell’Informativa, il Titolare DEVE SEMPRE specificare:

1. I dati di contatto del DPO, ove esistente;
2. La base giuridica del trattamento, qual è il suo interesse legittimo se quest’ultimo costituisce la base giuridica del trattamento;
3. Se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.).

Il Regolamento prevede anche ulteriori informazioni in quanto «necessarie per garantire un trattamento corretto e trasparente»: in particolare, il titolare deve

- specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione
- il diritto di presentare un reclamo all'autorità di controllo.

Se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l'informativa deve specificarlo e deve indicare anche: la LOGICA DI TALI PROCESSI decisionali e le CONSEGUENZE PREVISTE PER L'INTERESSATO.

Modalità dell'Informativa

Il regolamento specifica molto più in dettaglio rispetto al Codice le caratteristiche dell'Informativa

- che deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile;
- occorre utilizzare un linguaggio chiaro e semplice, e per i minori occorre prevedere informative idonee (si veda anche considerando 58).

L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico (soprattutto nel contesto di servizi online: si vedano art. 12, paragrafo 1, e considerando 58), anche se sono ammessi «altri mezzi», quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra (art. 12, paragrafo 1).

Informative multistrato

Il regolamento ammette, soprattutto, l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo «in combinazione» con l'informativa estesa (art. 12, paragrafo 7).

Le icone dovranno essere identiche in tutta l'UE e saranno definite prossimamente dalla Commissione Europea.

Esonero dell'Informativa per dati NON raccolti dall'Interessato

Spetta al titolare, in caso di dati personali raccolti da fonti diverse dall'Interessato, valutare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato (si veda art. 14, paragrafo 5, lettera «b») – a differenza di quanto prevede l'art. 13, comma 5, lettera «c» del Codice.