GDPR

Solo quello che devi sapere

INFOTEL

23 maggio 2018
Autore: infotel

GDPR - Solo quello che devi sapere

Cos'è il GDPR?

Il *General Data Protection Regulation* è il regolamento europeo (Regolamento UE 2016/679) per la protezione dei dati personali (ovvero, tutela della privacy). E' nato con l'intento di **uniformare la normativa all'interno dell'Unione Europea** e per i cittadini dell'UE.

In parole povere è **il nuovo regolamento per la privacy riguardo la gestione dei dati personali,** uniforme per tutta l'Unione Europea. Qui trovate la pagina ufficiale del regolamento sul sito dell'UE, tradotta in tutte le lingue, e qui la relativa pagina sul sito del Garante per la privacy italiano (la stessa norma, con l'aggiunta di alcune note esplicative da parte del Garante italiano).

Quando entra in vigore?

Il GDPR entra in vigore a partire dal **25 maggio 2018.**

Ed il nostro caro vecchio codice per la privacy dlgs.n. 196/2003?

Il GDPR si sovrappone al dlgs.n. 196/2003 e, di fatto, ne abroga le norme incompatibili. **In soldoni, da adesso in poi fa fede il GDPR.** Solo per quanto non specificato nel GDPR, rimane in vigore quanto scritto nel dlgs.n. 196/2003.

Il Garante dovrebbe promuovere una nuova normativa italiana di collegamento e armonizzazione. Ancora non pervenuta.

Mini vocabolario essenziale

Supponiamo che *Mario Rossi* compili un form di informazioni sul sito web dell'azienda *ACME*, e che tale sito sia stato fatto e sia gestito dalla Web Agency *Duck Inc* (vedi **art. 2**).

- **Titolare del trattamento:** l'entità (azienda, autorità, professionista) che utilizza i dati personali (ACME)
- **Interessato:** persona fisica identificabile a cui si riferiscono i dati (Mario Rossi)
- **Responsabile del trattamento:** l'entità che tratta i dati personali per conto del titolare del trattamento (Duck Inc).

La filosofia, l'essenza del GDPR

Il GDPR chiede, a chi ottiene e gestisce i dati personali altrui, di (vedi **art. 5**):

- rendere chiaro **a quale fine saranno utilizzati** i dati (per gestire la richiesta inviata, per gestire un contratto sottoscritto, per invio newsletter, per invio sms, whatsapp, per messaggi pubblicitari di terzi, etc)
- trattenere **solo i dati necessari** alle finalità indicate (ovvero non chiedere dati in più, non necessari)
- trattenerli per **il tempo minimo necessario** rispetto alle finalità indicate (per una newsletter ha senso "a vita", per una richiesta di preventivo potrebbero bastare poche settimane)
- **garantire la sicurezza dei dati** (sia rispetto alla riservatezza delle persone, sia custodirli in modo adeguato, anche dal punto di vista tecnico).

Molti obblighi prevedono valutazioni soggettive del titolare del trattamento, ed in sostanza al titolare stesso il regolamento si rimette riguardo la valutazione della congruità di determinate decisioni. Una sorta di auto-responsabilizzazione.

In quali casi posso trattare i dati personali

Il regolamento elenca in modo preciso i casi in cui ho diritto a trattare i dati personali di qualcuno (vedi **art. 6**).

- Ho il **consenso esplicito** dell'interessato per le specifiche finalità per cui li utilizzerò. Attenzione, il consenso è valido solo se l'interessato è maggiore di 16 anni (altrimenti serve il consenso dei genitori, ovviamente).
- Il trattamento è **necessario per l'esecuzione di un contratto** di cui l'interessato è parte (quindi se ha sottoscritto il contratto, posso usare i suoi dati laddove siano necessari per dare seguito al contratto).
- Il trattamento è **necessario per adempiere ad un obbligo legale** (se l'Agenzia delle Entrate da domani impone l'obbligo di comunicare mensilmente tutti i nominativi dei nuovi clienti, posso inviarli).
- Il trattamento è necessario per il perseguimento del **legittimo interesse del titolare** del trattamento, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato.

Insomma, per quanto riguarda il caso generale, **dovete richiedere il consenso esplicito all'interessato** (tutto come prima).

Come ottenere il consenso esplicito

Il consenso esplicito dell'interessato (vedi **art. 7**):

- deve essere fornito con una **azione positiva ed inequivocabile** (no a caselle prespuntate… devono essere tutte spuntate con azione manuale dell'interessato)
- deve essere fornito per **ogni specifica finalità** del trattamento, con selezione separata e distinguibile dalle altre finalità del trattamento (una casella per la gestione della richiesta di informazioni, una casella per l'iscrizione alla newsletter, una casella per l'invio di promozioni via sms, etc)
- deve riguardare lo specifico servizio richiesto o indicato. Ovvero l'erogazione di un servizio non può essere subordinato all'azione di fornire il consenso al trattamento di altri dati ad altre finalità

non necessarie allo svolgimento del servizio (in soldoni, non puoi obbligare l'utente ad iscriversi alla newsletter per avvalersi degli altri tuoi servizi).

Cosa deve contenere la richiesta del consenso esplicito

Quando si richiede il consenso esplicito, **si devono fornire all'interessato** (ovvero, devi esibire nell'informativa) le seguenti informazioni (vedi **art. 13**).

- L'identità e i dati di contatto del titolare del trattamento (ragione sociale, magari partita iva, telefono, email)
- L'identità e i dati di contatto del responsabile del trattamento
- I dati di contatto del DPO. Questo NON riguarda il 99% delle PMI e delle web agency (vedi paragrafo dedicato al DPO più avanti).
- Le finalità del trattamento
- Gli eventuali destinatari dei dati, o quantomeno le categorie degli eventuali destinatari (in caso di cessione a terzi).
- Il periodo di conservazione dei dati. Ove non possibile, almeno i criteri per determinare tale periodo.
- Citare il diritto di accesso ai dati, rettifica dei dati, cancellazione dei dati.
- Citare il diritto di proporre reclamo alle autorità di controllo (il Garante della Privacy)
- Specificare se la comunicazione di dati personali è un obbligo legale, o un obbligo contrattuale, o se è necessario per la conclusione di un contratto. Eventualmente, specificare le conseguenze del mancato consenso (tutto come prima: avvisare che "senza prestare questo consenso non sarà possibile erogare il servizio o dare seguito al contratto")
- Informare dell'eventuale utilizzo automatizzato dei dati… insomma la temuta profilazione. E specificare le conseguenze di tale trattamento (ricorda un po' gli avvisi sui pacchi di sigarette).

Se hai acquisito i dati da terzi

Se hai avuto accesso al trattamento dei dati da terzi (quando prendi legalmente i dati da banche dati), devi fornire all'interessato, entro un mese dall'acquisizione, più o meno gli stessi dati del paragrafo precedente (vedi **art. 14**).

Il registro delle attività di trattamento

Il temutissimo registro in cui i titolari segnano tutti i dati di contatto di titolare, contitolare, responsabile, del trattamento, le finalità, le categorie di interessati. I responsabili del trattamento segnano tutti i titolari per conto dei quali agiscono, i loro dati, le categorie di trattamenti effettuati, le misure di sicurezza adottate, etc.

Ecco, tutto questo **NON vi riguarda se avete meno di 250 dipendenti.**

Se, invece, avete più di 250 dipendenti, andatevelo a studiare all'**art. 30**: qui non verrà trattato.

Responsabilità del titolare del trattamento

Il titolare del trattamento deve garantire la sicurezza dei dati e la conformità del trattamento rispetto al regolamento… e deve dimostrare di aver agito in tal senso (vedi **art. 24**).

Ne possono essere dimostrazione eventuali codici di condotta (art. 40) e certificazioni inerenti (vedo art. 42)… che ancora non esistono.

Il Responsabile del trattamento

Il titolare del trattamento, qualora non sia autonomo nella gestione del trattamento dei dati, ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti (dal punto di vista tecnico e organizzativo) per soddisfare il regolamento e tutelare i diritti dell'interessato (vedi **art. 28**).

In soldoni, se il trattamento dei dati del tuo sito è in mano ad uno squinternato, la mala gestione è colpa tua.

L'incarico di **Responsabile del trattamento** dei dati deve essere **disciplinato da un contratto,** in cui devono essere specificati:

- la materia disciplinata (l'ambito a cui si fa riferimento)
- la durata del trattamento
- la natura e la finalità del trattamento
- il tipo di dati personali
- le categorie di interessati
- gli obblighi e i diritti del titolare del trattamento.

Dal canto suo, il responsabile del trattamento:

- tratta i dati personali solo su richiesta documentata del titolare (quindi non sono valide le richieste verbali/telefoniche)
- garantisca che le persone autorizzate al trattamento dei dati abbiano un obbligo legale di riservatezza (i dipendenti che accedono ai dati devono avere delle clausole di riservatezza)
- cancella o restituisce i dati al termine del contratto.

Sicurezza del trattamento

Il titolare ed il responsabile del trattamento dei dati devono garantire un adeguato livello di sicurezza dei dati. Cosa voglia dire adeguato non è specificato: fa parte delle valutazioni soggettive demandate al titolare del trattamento (vedi **art. 32**).

In questi aspetti il regolamento ha un sapore piuttosto anglosassone: la valutazione riguardo l'aderenza o meno alla norma è demandata al buon senso.

In ogni caso, vanno valutate la situazione tecnologica ed il reale livello rischio legato ai dati trattati: un conto è proteggere un IBAN, un conto è proteggere la città della sede legale.

Il DPO - Responsabile della Protezione dei Dati

Il *Data Protection Officer*, o *Responsabile della Protezione dei Dati*, la funzione più temuta del regolamento: dovrebbe essere indipendente dal titolare e dal responsabile, avere pieno accesso ai dati ed alle procedure ed azioni di titolare e responsabile, avere budget sufficiente per operare, garantire e verificare la sicurezza dei dati, etc.

Beh, nel 99% dei casi… non serve. Serve solo per autorità pubbliche, trattamento su larga scala (big data), e per dati particolarmente sensibili (vedi le definizioni esatte agli articoli 9 e 10).

Il Garante della Privacy è in ritardo?

Come successe per la *Cookie Privacy*, la percezione netta è che il Garante per la Privacy italiano sia in netto ritardo (in questo caso forse lo è tutta la UE).

Il Garante dovrebbe promuovere e farci pervenire una nuova legge che riscriva la 196/2003 per armonizzarla a questo regolamento.

Gli articoli 41, 42 e 43 fanno riferimenti ad enti, organi e certificazioni che ancora non esistono: devono essere definiti ed istituiti dal Garante.

Nel regolamento si fa cenno sia ad una "informativa tipo" che dovrebbe essere messa a disposizione dal Garante, sia a delle icone standard per una informativa semplificata e di più immediata lettura, che dovrebbero essere fornite direttamente dall'autorità europea (in modo da essere omogenee in tutta la UE). Entrambe, ad oggi, non esistono.

DPIA (Valutazione Impatto)

La DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali.

QUANDO LA DPIA E' OBBLIGATORIA?

In tutti i casi in cui un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Il Gruppo Art. 29 individua alcuni criteri specifici a questo proposito:

- trattamenti valutativi o di scoring , compresa la profilazione ;

- decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni); - monitoraggio sistematico (es: videosorveglianza);

- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);

- trattamenti di dati personali su larga scala;

- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);

- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);

- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT , ecc.);

- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.

QUANDO LA DPIA NON E' OBBLIGATORIA?

Secondo le Linee guida del Gruppo Art. 29, la DPIA NON è necessaria per i trattamenti che:

- non presentano rischio elevato per diritti e libertà delle persone fisiche;

- hanno natura , ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA ;

- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;

- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;

- fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA