ASSOLOMBARDA
Confindustria Milano Monza e Brianza

REGOLAMENTO UE 2016/679 SULLA PROTEZIONE DEI DATI PERSONALI

Angelo Ventimiglia - Monza

9 maggio 2018

Il Regolamento UE 2106/679 relativo alla protezione dei dati personali, nonché alla loro libera circolazione, entrerà in vigore dal 25 maggio 2018.

E' noto anche con il nome di GDPR «General Data Protection Regulation».

Il GDPR abroga la previgente normativa privacy europea contenuta nella Direttiva 95/46/Ce, da cui ha avuto origine il nostro Codice Privacy D.Lgs. 196/2003.

Il GDPR è direttamente applicabile, quindi non necessita di nessun recepimento.

Da un punto di vista tecnico giuridico, quindi, l'intervento del legislatore italiano non sarebbe stato indispensabile, ma l'Italia ha ritenuto doveroso un intervento di raccordo tra la nuova normativa europea e quella interna.

Lo schema di Decreto Legislativo approvato dal Consiglio dei ministri il 21 marzo 2018 attua questo raccordo.

L'approccio del Regolamento rivoluziona quello adottato, ormai più di vent'anni fa, dalla Direttiva. Si passa da un modello di trattamento autorizzatorio a un regime basato sull'accountability, cioè sulla responsabilizzazione.

Il titolare del trattamento diventa primario centro di responsabilità e deve dimostrare di avere adottato misure giuridiche, organizzative, tecniche, adeguate per la protezione dei dati personali.

Il GDPR come il vigente Codice Privacy 196/2003 non è applicabile al trattamento dei dati riferibili esclusivamente alle persone giuridiche.

Ciò significa che gli adempimenti previsti dal Regolamento non si applicano ai dati esclusivamente riferibili al bilancio delle società, né ai dati relativi alla sede o di contatto dell'impresa.

Il Regolamento non si applica ai disegni industriali o ai progetti, sempre a patto che non comprendano dati personali.

La filiera Privacy

1. ***Titolare del trattamento:*** *la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.*

2. ***Contitolare del trattamento:*** *due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento che dovranno definire i loro obblighi e responsabilità nel trattamento dei dati attraverso un accordo interno.*

La filiera Privacy

3. Responsabile del trattamento: la persona fisica o giuridica che tratta dati personali per conto del titolare del trattamento. Nel codice Privacy si faceva riferimento alla nomina del responsabile da parte del titolare, internamente o esternamente alla organizzazione del titolare. Nel Regolamento, che pur non esclude il ricorso a figure manageriali interne, ci si riferisce a soggetti esterni.

La filiera Privacy

3. L'interessato: è il titolare dei diritti, è la persona fisica la cui protezione è lo scopo sostanziale dell'osservanza delle regole del trattamento dei dati.

4. Rappresentante del titolare: qualifica che riguarda i titolari o responsabili del trattamento che non sono stabiliti nell'UE e sono soggetti agli obblighi di cui al GDPR. Il rappresentante deve essere stabilito in un Paese dell'UE dove si trovano interessati i cui dati sono trattati dal titolare/responsabile ed agisce come interlocutore del Garante

Tipologie di dati

1. ***Dato personale**: qualsiasi informazione concernente una persona fisica identificata o identificabile (interessato); si considera identificabile la persona 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 on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.*

2. ***Dato particolare**: è una categoria di dato personale che rivela l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.*

Le principali novità

1) ***INFORMATIVA***
2) ***CONSENSO***
3) ***DIRITTI DEGLI INTERESSATI***
4) ***REGISTRO DEI TRATTAMENTI***
5) ***DATA PROTECTION OFFICER (DPO)***
6) ***PRIVACY BY DESIGN E BY DEFAULT***
7) ***VALUTAZIONE D'IMPATTO PRIVACY(DPIA)***
8) ***DATA BREACH (VIOLAZIONI DEI DATI PERSONALI)***
9) ***CERTIFICAZIONI – CODICI DI CONDOTTA***
10) ***TRASFER***
11) ***SANZIONI***

Le principali novità

1) INFORMATIVA

Il GDPR impone a tutti i titolari del trattamento di revisionare ed aggiornare l'informativa privacy da fornire agli interessati.

In vigenza del Codice Privacy, è previsto che l'informativa indichi le finalità e le modalità del trattamento, la natura obbligatoria o facoltativa del conferimento dei dati, gli estremi identificativi del titolare, i diritti dell'interessato.

Le principali novità

Il GDPR arricchisce il contenuto dell'informativa con ulteriori indicazioni che il titolare deve fornire all'interessato, in modo trasparente, chiaro e conciso, prima di procedere al trattamento.

Occorre che l'informativa contenga:

a) i dati di contatto, se designato, del Responsabile per la protezione dei dati o DPO (Data Protection Officer);

b) la base giuridica del trattamento (per es. il consenso, il legittimo interesse del titolare, l'esecuzione di un contratto di cui è parte l'interessato, ecc.)

Le principali novità

c) Il periodo di conservazione dei dati o «data retention»

E' il termine entro il quale il dato sarà cancellato. Tale novità normativa non deve essere sottovalutata dalle imprese. I nominativi dei potenziali clienti che hanno chiesto un preventivo devono essere CANCELLATI una volta superato il periodo di tempo previsto.

Per i dati dei dipendenti in informativa si potrebbe indicare il termine decennale dalla cessazione del rapporto di lavoro. Si auspicano chiarimenti da parte del Garante.

Le principali novità

L'informativa deve essere fornita all'interessato prima di effettuare la raccolta dei dati, se i dati sono raccolti presso l'interessato.

Se i dati personali non sono raccolti presso l'interessato l'informativa deve essere fornita entro 1 mese dalla raccolta, oppure al momento della comunicazione dei dati a terzi o all'interessato.

Le principali novità

2) CONSENSO

Rappresenta una condizione che legittima il trattamento dei dati.

Il considerando 32 del GDPR definisce il consenso come un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale.

Non configura consenso, il silenzio, l'inattività o la preselezione di caselle.

Il consenso può essere revocato in qualsiasi momento e la revoca non pregiudica la liceità del trattamento basato sul consenso prima della revoca.

Le principali novità

In caso di consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutte le caratteristiche sopra individuate. In caso contrario, è opportuno adoperarsi per raccogliere nuovamente il consenso degli interessati.

Il consenso non è necessario se il trattamento è lecito, nell'ambito di un contratto o ai fini della conclusione di un contratto, se il trattamento è effettuato in conformità ad un obbligo legale

Le principali novità

Il consenso non è richiesto se il trattamento è lecito, se esiste un legittimo interesse del titolare al trattamento del dato, a condizione che non prevalgano gli interessi o di diritti e le libertà fondamentali dell'interessato.

Le principali novità

3) I diritti degli interessati

Il GDPR introduce nuovi diritti a quelli già esistenti di :

- ***Trasparenza;***
- ***Informativa;***
- ***Accesso;***
- ***Rettifica;***
- ***Opposizione del trattamento***

Le principali novità

3) DIRITTI DEGLI INTERESSATI

Il GDPR introduce nuovi diritti di oblio, limitazione del trattamento e portabilità dei dati.

a) oblio:
l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo ed il titolare ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

Le principali novità

- i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

- ***l'interessato revoca il consenso su cui si basa il trattamento e non sussiste altro motivo legittimo per trattare i dati;***
- ***l'interessato si oppone al trattamento dei dati personali e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;***
- ***i dati sono stati trattati illecitamente;***
- ***i dati devono essere cancellati per adempiere ad un obbligo legale previsto dal diritto dell'Unione Europea o degli Stati Membri cui è soggetto il titolare del trattamento.***

Le principali novità

b) Limitazione del trattamento

Il diritto di limitazione del trattamento riconosce all'interessato la possibilità di richiedere la sospensione momentanea di ogni trattamento dei propri dati, ad esclusione della conservazione, in alcune specifiche situazioni.

La restrizione ha natura temporanea e deve essere esplicitamente formulata al titolare del trattamento. La limitazione può essere concessa per precisi motivi:

Le principali novità

- ***per verificare l'esattezza dei dati;***
- ***su richiesta dell'interessato in caso di trattamento illecito;***
- ***per l'esercizio di un diritto in sede giudiziaria o***
- ***nelle more di un bilanciamento tra gli opposti interessi del titolare e dell'interessato.***

Le principali novità

c) Portabilità

E' il diritto dell'interessato di ricevere dal titolare i propri dati personali in un formato strutturato e leggibile da dispositivo automatico, ove il trattamento sia effettuato con mezzi automatizzati e ricorrano le altre condizioni stabilite nell'articolo 20.

Le principali novità

4) REGISTRO DEI TRATTAMENTI

L'attività di controllo sulle modalità del trattamento si traducono in un obbligo di trasparenza interna del titolare effettuato anche attraverso il Registro dei Trattamenti (RdT).

Il RdT è una mappatura delle modalità di trattamento dei dati personali da parte dell'azienda, in continuo aggiornamento per poter fornire un quadro fedele dei trattamenti effettuati.

Le principali novità

Contenuto minimo:

- ***nome e dati di contatto del titolare ed eventuale contitolare, rappresentante del titolare e DPO, se designato;***
- ***finalità del trattamento;***
- ***descrizione delle categorie di interessati e delle categorie di dati personali;***
- ***categorie di destinatari i cui dati personali sono stati o saranno comunicati, compresi destinatari esteri ed organizzazioni internazionali***

Le principali novità

Contenuto minimo:

- ***Eventuali trasferimenti di dati personali verso Paesi terzi od organizzazioni internazionali (per i trasferimenti verso Paesi terzi che non forniscono garanzie adeguate sul trattamento dei dati personali, occorre anche la documentazione che attesti la base giuridica del trasferimento, come le clausole contrattuali standard);***
- ***i termini ultimi previsti per la cancellazione delle diverse categorie dei dati;***
- ***una descrizione generale delle misure di sicurezza tecniche ed organizzative.***

Le principali novità

Non è obbligatorio per le società con meno di 250 dipendenti, a meno che non siano trattati dati sensibili o relative a condanne penali. Ma lo stesso GDPR ne raccomanda l'adozione ad ogni società: senza un registro dettagliato, sarà difficile dimostrare di aver un controllo sul corretto trattamento dei dati personali, non sarà possibile illustrare i trattamenti nelle informative privacy, sarà difficile identificare i trattamenti che devono essere oggetto di valutazione d'impatto o DPIA.

Le principali novità

E' obbligatorio per chi agisce come responsabile del trattamento. In tal caso, il livello di dettaglio richiesto è minore, ma i fornitori dovranno poter mappare in tale registro i trattamenti effettuati per conto di ciascun soggetto che li ha nominati come responsabili del trattamento.

Le principali novità

L'art. 37 del GDPR impone ad alcuni soggetti la nomina del Responsabile per la protezione dei dati meglio noto con l'acronimo inglese di Data Protection Officer (DPO).

I soggetti obbligati sono le autorità e gli organismi pubblici ed i soggetti che effettuano come attività principale trattamenti su larga scala di particolari categorie di dati (come i dati sensibili e biometrici) o trattamenti che richiedono un monitoraggio regolare e sistematico degli interessati su larga scala.

Le principali novità

Il DPO potrà essere interno (per es. un dipendente del titolare) o esterno (un professionista o una società di consulenza). Secondo la prassi europea, il ruolo del DPO potrà essere assunto da una persona giuridica o da un team interno all'organizzazione del titolare. In questo caso si preferisce che sia sempre individuata una persona fisica di riferimento.

Il GDPR consente ai gruppi aziendali di nominare un unico DPO, a condizione che sia facilmente raggiungibile da ciascun stabilimento. Analogamente, in ambito pubblico sarà possibile nominare un unico DPO per più enti.

Le principali novità

Il DPO dovrà essere adeguatamente qualificato, deve possedere competenze giuridiche e tecnico-informatiche. Non sono richieste iscrizioni in albi o attestazioni varie di partecipazioni a corsi di specializzazione.

Il DPO interno o esterno che sia non deve essere in conflitto di interessi con altri incarichi manageriali di vertice.
Il ruolo non può essere assunto dall'amministratore delegato, dal responsabile operativo, dal responsabile finanziario, dal direttore mkt o delle risorse umane, dal responsabile IT, nonché da ogni altro soggetto che detrmini le finalità ed i mezzi di trattamento dei dati.

Le principali novità

In sostanza, il DPO è una sorta di Garante interno alla struttura del titolare o del responsabile del trattamento.

La valutazione della sua competenza e capacità è affidata al titolare che dovrà valutarne il percorso formativo tenendo conto delle specificità dei trattamenti effettuati.

L'obbligo di legge non è quindi assolto dalla semplice nomina del DPO, ma occorre che quest'ultimo disponga dei requisiti formativi e curriculari in grado di comprovarne competenze e capacità.

Le principali novità

6) Privacy by design e by default

Il GDPR obbliga il titolare a cambiare l'approccio in relazione alla compliance privacy.

La norma impone di azionare la procedura privacy sin dalla progettazione o sviluppo di ogni nuovo trattamento di dati personali (privacy by design).

Il principio di privacy by default stabilisce, invece, che per impostazione predefinita le imprese dovrebbero trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini. Occorre, quindi, progettare il sistema di trattamento di dati garantendo la non eccessività dei dati raccolti.

L'introduzione di tali due principi obbliga, ovviamente, le imprese a predisporre una valutazione di impatto privacy ogni volta che avviano un progetto che prevede un trattamento di dati (DPIA)

Le principali novità

7) Data Breach

Nel GDPR la sicurezza delle informazioni personali non si limita più ad un elenco di strumenti tecnici di salvaguardia, non esiste un disciplinare tecnico.

Nel GDPR il principio di accountability (responsabilizzazione) deve ispirare il titolare nell'individuare misure di sicurezza adeguate per fronteggiare i rischi che gravano sui dati.

Con il termine data breach si identifica una falla nel sistema di sicurezza in cui i dati sensibili e protetti vengono rubati quindi consultati, copiati, trasmessi.

La normativa (GDPR) prevede l'obbligo di comunicare alle autorità di controllo la violazione dei dati per i fornitori di servizi di comunicazione elettronica accessibili al pubblico, ma solo se il titolare ritiene probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati. Tutti i titolari del trattamento sono soggetti alla norma. La notifica dovrà avvenire entro 72 ore e comunque "senza ingiustificato ritardo".

Le principali novità

Se il titolare ritiene che il rischio per i diritti e le libertà degli interessati è elevato, allora si dovranno informare anche gli interessati, sempre "senza ingiustificato ritardo". Non è richiesta la comunicazione all'interessato quando:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

Le principali novità

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

*c) la **comunicazione richiederebbe sforzi sproporzionati**. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.*

Le principali novità

9) CERTIFICAZIONI E CODICI DI CONDOTTA

Il GDPR consente ed incoraggia le associazioni e le altre organizzazioni che rappresentano categorie di titolari o responsabili del trattamento ad elaborare CODICI DI CONDOTTA che guidino le imprese nella corretta applicazione di questa normativa.

Il rispetto dei CODICI DI CONDOTTA determina una presunzione di conformità, senza escludere l'intervento del Garante che potrà ugualmente irrogare le sanzioni di legge ove risultino accertate le violazioni.

Le principali novità

Il GDPR incoraggia altresì meccanismi di CERTIFICAZIONE che consentano agli interessati di valutare rapidamente il livello di protezione dei propri dati offerti da un titolare o da un responsabile del trattamento.

La CERTIFICAZIONE è volontaria ed accessibile tramite una procedura trasparente.

L'adozione della CERTIFICAZIONE non riduce la responsabilità del titolare del trattamento riguardo alla conformità al GDPR, lascia impregiudicati i poteri di verifica e di controllo dal parte del Garante.

Le principali novità

10) TRASFERIMENTO DEI DATI PERSONALIVERSO PAESI TERZI

Il GDPR prevede che il Paese Terzo verso cui i dati sono diretti abbia ottenuto una decisione di adeguatezza da parte della Commissione UE in cui si accerti che il livello di protezione del Paese sia adeguato e compatibile con il livello di protezione europeo.

Un trasferimento può avvenire anche quando siano presenti garanzie adeguate o per i trasferimenti infra-gruppo, il gruppo societario adotti norme vincolanti d'impresa (le c.d. Binding corporate rules).

In assenza di decisione di adeguatezza o di garanzie adeguate il trasferimento dei dati personli verso un Paese Terzo è ammesso se si verificano una delle seguenti condizioni

Le principali novità

10) TRASFERIMENTO DEI DATI PERSONALIVERSO PAESI TERZI

In assenza di decisione di adeguatezza o di garanzie adeguate il trasferimento dei dati personli verso un Paese Terzo è ammesso se si verificano una delle seguenti condizioni:

- ***se il trasferimento è occasionale e necessario in relazione ad un contratto o ad un'azione legale;***
- ***se sussistono motivi di rilevante interesse pubblico previsti dal Diritto dell'Unione Europea.***

Le principali novità

11) SANZIONI

In materi di sanzioni il GDPR ragiona in milioni di euro. Questo per chiarire il ruolo che il legislatore europeo assegna al provvedimento.

Si distinguono violazioni che hanno una sanzione massima pari ad una multa di 10 milioni di euro o il 2% del fatturato mondiale annuo e violazioni punite nel massimo con una multa di 20 milioni di euro o il 4% del fatturato. Non c'è un minimo.

Le principali novità

Violazioni soggette al rischio di una sanzione massima di 10 mln o il 2% del fatturato mondiale annuo, se superiore:

- ***Violazioni in tema di offerte commerciali;***
- ***Consenso;***
- ***Tenuta del Registro dei Trattamenti;***
- ***Misure di sicurezza del trattamento;***

Violazioni soggette al rischio di una sanzione massima di 20 mln o il 4% del fatturato mondiale annuo, se superiore:

- ***Violazione dei principi base del trattamento (artt. 5, 7 e 9);***
- ***Inosservanza di un ordine di un'autorità di controllo***

ASSOLOMBARDA
Confindustria Milano Monza e Brianza

www.assolombarda.it
www.assolombardanews.it
Seguici su