Grant Thornton
An instinct for growth™

General Data Protection Regulation

Marzo 2017

Creare, proteggere e incrementare il valore della vostra azienda

Il nuovo GDPR e le possibili implicazioni per le vostre attività

Il *General Data Protection Regulation* (GDPR) dovrà essere adottato entro maggio 2018. È la fase più recente del programma europeo di tutela dei cittadini e salvaguardia dei loro dati personali ed è mirato a introdurre nuovi diritti per le persone fisiche, rafforzare le misure di protezione esistenti e imporre requisiti più rigidi per tutte quelle attività aziendali che implicano il trattamento di dati personali. Il GDPR avrà un impatto significativo sulle attività di business, sia per i titolari sia per i responsabili del trattamento, e la sua definitiva applicazione è ormai alle porte. Il GDPR sostituisce la vigente Direttiva Europea 46/95 EC dalla quale deriva l'attuale Codice Privacy (D. Lgs. 196/03) e amplia gli obblighi già efficaci.

È necessario che le imprese esaminino attentamente e valutino in modo critico questo cambiamento normativo, per comprendere a fondo come influirà sulle operazioni aziendali. I processi operativi aziendali, e i relativi sistemi informatici a supporto, dovranno conformarsi totalmente alla nuova normativa.

Il quadro giuridico in materia di protezione dei dati è in rapida evoluzione e questo comporta molte sfide per le Autorità Pubbliche e per le aziende, in particolar modo per quelle a diretto contatto con il consumatore, per quelle che operano online e nel settore dei servizi finanziari, per quelle che trattano dati sensibili e, in generale, per tutte le aziende che attraverso i dati esercitano un controllo regolare e sistematico degli interessati.

L'ammontare delle sanzioni previste per la violazione del Regolamento Europeo è aumentato considerevolmente, fino ad arrivare a €20 milioni, o al 4% del fatturato del gruppo a livello mondiale.

Le aziende dovranno pertanto agire senza indugio per evitare di incorrere in sanzioni potenzialmente elevate a causa della propria inadempienza.

I Professionisti di Grant Thornton Financial Advisory Services specializzati in *Business risk services* e *Cyber-security* forniscono servizi integrati per creare, proteggere e incrementare il valore della vostra azienda in linea con il nuovo GDPR.

Principali cambiamenti introdotti dal GDPR

Accountability

Accountability è una delle parole chiave del GDPR. Il Titolare del trattamento è "*accountable*" per l'adeguamento al GDPR in tutte le materie, legali, organizzative e tecniche; si richiede infatti che il Titolare sia in grado di dimostrare (comprovare) la conformità ai principi enunciati nel Regolamento Europeo.

Estensione dell'ambito di applicazione territoriale e trasferimento transfrontaliero di dati personali

Il GDPR si applica anche a quelle imprese stabilite al di fuori dell'Unione Europea le cui attività sono connesse all'offerta di beni o servizi o al controllo del comportamento di un interessato all'interno dell'UE, indipendentemente dal fatto che il trattamento dei dati abbia luogo fuori dall'UE o meno. Se un'azienda ha intenzione di trasferire dati fuori dai confini dell'Unione Europea deve necessariamente seguire un'apposita procedura; tutti i titolari del trattamento sono tenuti a rivedere i presupposti in base ai quali i suddetti dati sono trasferiti e assicurarsi che siano in atto protezioni adeguate.

Sicurezza dei trattamenti

Il titolare del trattamento deve effettuare l'Analisi del Rischio del trattamento di dati personali per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al regolamento e, quindi, in funzione dei "rischi (distruzione accidentale o illegale o perdita dei dati personali, modifica, rivelazione dei dati o accesso agli stessi non autorizzati) aventi probabilità e gravità diverse", adottare le "misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio".

Nomina di un *Data Protection Officer* - Responsabile della Protezione dei Dati (DPO - RPD)

I titolari del trattamento e i responsabili del trattamento le cui attività principali consistono in operazioni di trattamento che richiedono il monitoraggio periodico e sistematico di interessati su vasta scala sono tenuti a nominare un Responsabile della Protezione dei Dati, il quale deve avere una conoscenza specialistica delle leggi e delle procedure in materia di protezione dei dati.

Privacy by default e *Privacy by design*

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita (*by default*), solo i dati personali necessari per ogni specifica finalità del trattamento (quantità dei dati raccolti, portata del trattamento, periodo di conservazione e accessibilità limitata ai dati a un numero definito di persone fisiche).
Sia al momento di determinare i mezzi del trattamento (*by design*) sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

Tenuta di registri delle attività di trattamento

Il GDPR richiede ai titolari del trattamento di tenere un registro di tutte le categorie di attività di trattamento sotto la propria responsabilità. Questo registro deve contenere informazioni quali, tra le altre, la finalità del trattamento, il tipo di dati trattati, le categorie di destinatari e una descrizione generale delle misure di sicurezza tecniche e organizzative (Sicurezza dei trattamenti).

Valutazione d'impatto sulla protezione dei dati

La normativa richiede alle aziende di svolgere una valutazione d'impatto sulla protezione dei dati nel caso in cui il trattamento possa presentare un rischio elevato per i diritti delle persone e, in particolare, nel caso in cui si utilizzino nuove tecnologie, tenendo conto della natura, dell'ambito di applicazione, del contesto e dello scopo del trattamento. Tale valutazione deve essere effettuata prima di procedere al trattamento.

Segnalazione di violazioni dei dati personali (*data breach*)

La normativa introduce l'obbligo di segnalare tutte le violazioni di dati ad alto rischio all'Autorità di controllo entro 72 ore e/o agli interessati senza indebito ritardo. Le imprese dovrebbero essere preparate per un evento di questo tipo, accertando che siano in essere politiche e procedure di risposta alla violazione dei dati.

Diritti degli interessati

L'interessato ha diritto a ottenere maggiori informazioni circa il trattamento, ad esempio i destinatari (o le categorie) a cui i dati saranno comunicati, l'esistenza di un processo decisionale automatizzato (compresa la profilazione), la rettifica o l'integrazione dei dati personali che lo riguardano e, nei casi previsti, ha il diritto di ottenere la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo («diritto all'oblio»)

L'interessato ha inoltre il diritto di trasmettere i propri dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora il trattamento si basi sul consenso o su un contratto e sia effettuato con mezzi automatizzati.

L'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

Sanzioni

Ai sensi del GDPR, l'Autorità di controllo può imporre sanzioni molto elevate nel caso di una violazione dei dati personali. Le sanzioni possono raggiungere i €20 milioni o il 4% del fatturato annuo (calcolato a livello di gruppo, non di singole controllate) applicando tra le due opzioni la più elevata.

In sintesi

L'adeguamento al GDPR richiede un approccio con competenze legali, organizzative e tecniche che, partendo dalla tipicità dei trattamenti di dati personali e dei servizi offerti, dall'ambito territoriale e dalle infrastrutture tecnologiche utilizzate per lo sviluppo e l'erogazione dei servizi, porti alla costituzione di un modello di Privacy Governance, definendo ruoli, responsabilità e processi di gestione.

Ciò si renderà indispensabile nel momento in cui verranno definiti gli schemi di certificazione; l'applicazione di un meccanismo di certificazione approvato, infatti, potrà essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento previsti dal GDPR.

Come possiamo supportarvi

Il nostro team multi-disciplinare, con competenze legali, organizzative e informatiche, possiede una vasta esperienza in incarichi in ambito di protezione dei dati personali e privacy.

Siamo convinti che la gestione dei dati personali effettuata dalla Vostra azienda costituisca un rischio d'impresa al pari delle altre attività. Il nostro team di esperti è in grado di aiutarvi a gestire questo rischio adottando un approccio olistico e integrato per una tematica multidimensionale. Può lavorare insieme a voi per identificare e implementare soluzioni concrete e su misura per la vostra realtà. Il nostro supporto è volto a:

- comprendere i principali cambiamenti introdotti dal GDPR;
- valutare l'attuale struttura dei dati trattati dalla vostra organizzazione, l'attuale livello di conformità al GDPR e definire una roadmap per l'implementazione di un'adeguata struttura normativa e di compliance (GDPR *Check-up*);
- proporre soluzioni affinché la gestione dei rischi connessi al trattamento dei dati personali sia integrata nella struttura generale di *risk management* della vostra azienda;
- comprendere e mantenere una mappatura del flusso di dati personali;
- sviluppare modelli e procedure di Governance per la gestione dei dati personali;
- supportare il DPO nell'adempimento degli obblighi previsti dal ruolo e nel monitoraggio dei fattori interni ed esterni che possono avere un impatto sul modello di Governance definito;
- condurre valutazione d'impatto sulla protezione dei dati;
- valutare le vostre attività di adeguamento alla normativa;
- aiutarvi a sviluppare un piano di risposta in caso di violazione dei dati;
- valutare le vostre esigenze di formazione sulla protezione dei dati.

Contatti

Stefano Salvadeo

CEO, Head of Growth and Advisory Services

T +39 02 783 351
M +39 347 83 95 792
E stefano.salvadeo@bgt.it.gt.com

Alessandro Leone

Partner
T +39 02 783 351
M +39 347 72 35 017
E alessandro.leone@bgt.it.gt.com

Renato Sesana

Partner
T +39 02 783 351
M +39 347 98 39 309
E renato.sesana@bgt.it.gt.com

Grant Thornton
An instinct for growth™

www.bgt-grantthornton.it

Uffici

Milano

Via Melchiorre Gioia, 8
20124 Milano
T +39 02 783 351

Roma

Lungotevere Michelangelo, 9
00192 Roma
T +39 06 397 344 95

Padova

Galleria Europa, 4
35137 Padova
T +39 049 738 8290

Brescia

Piazza Paolo VI, 21 (Piazza Duomo)
25121 Brescia
T +39 030 240 4798

Staff location

Trento

Via Brennero, 139
38121 Trento
T +39 0461 828 368

Trieste

Piazza Silvio Benco, 1
34122 Trieste
T +39 040 363 006

Torino

Corso Re Umberto, 2
10121 Torino
T +39 011 071 2899