Grant Thornton

An instinct for growth™

GDPR

General Data Protection Regulation

LE NOVITA' SULLA TUTELA DEI DATI PERSONALI IN AZIENDA ALLA LUCE DEL REGOLAMENTO COMUNITARIO N. 679/2016

Grant Thornton Consultants

Roma, Febbraio 2018

Regolamento Generale sulla protezione dei dati (UE)

Introduzione

Il 4 maggio 2016 è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il «**Regolamento (UE) 2016/679**» ormai comunemente definito "GDPR"

Il GDPR è entrato in vigore il 24 maggio 2016

L'obbligo di applicazione negli Stati membri decorrerà dal **25 maggio 2018**

Il GDPR ha concesso **due anni** di tempo ai soggetti dei Paesi membri della UE per attuare gli adeguamenti necessari

GDPR - Principali novità

Sintesi

Garanzia dei diritti dell'interessato – il diritto ad opporsi a certi tipi di profilazione e processi decisionali automatici, il diritto di accesso, all'oblio, di limitazione al trattamento, alla portabilità dei dati.

Incremento degli obblighi per le organizzazioni – quali la dichiarazione agli interessati dei trattamenti eseguiti sui dati, l'informazione degli interessati sui propri diritti di protezione dei dati, le modalità di utilizzo dei dati e il periodo.

Richiesta del consenso al trattamento dettagliata – **il consenso deve essere esplicito**, fornito attivamente e liberamente per lo specifico trattamento e **facile da revocare**.

Segnalazione di violazioni dei dati personali (Data Breach) – «la violazione di sicurezza che comporta **accidentalmente** o in modo **illecito** la **distruzione**, la **perdita**, la **modifica**, la **divulgazione non autorizzata** di dati personali trasmessi, conservati o comunque trattati» - le violazioni gravi **devono essere segnalate** alle autorità **entro 72 ore**.

GDPR - Principali novità

Sintesi

Verifica degli impatti sulla privacy – le società devono gestire un **processo di analisi dei rischi**, in particolare per i nuovi processi con l'obbligo di eseguire il **DPIA** (*Data Protection Impact Assessment*) per i processi ad alto rischio.

Privacy by design – le società devono gestire la definizione delle misure di protezione dei dati nei requisiti dei nuovi processi e di quelli esistenti.

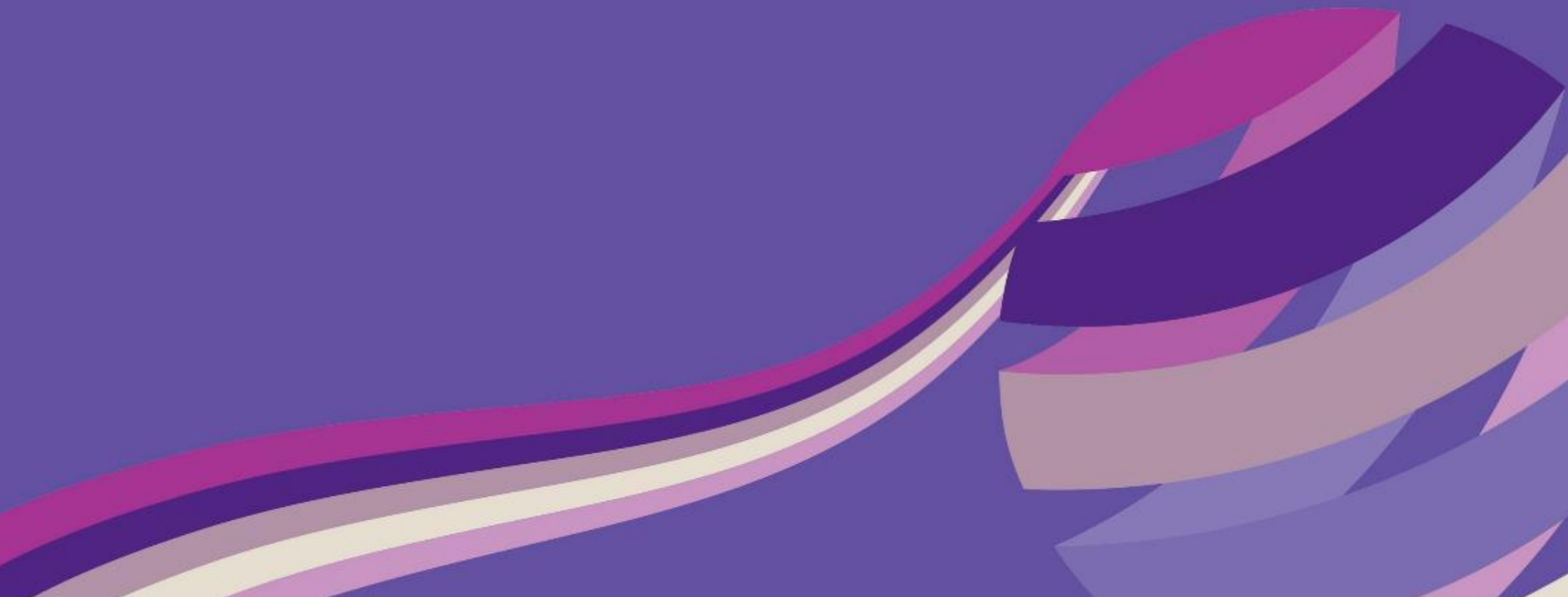
Registro dei trattamenti – le società devono tenere un registro dettagliato dei trattamenti, in cui indicare l'owner del dato, la scadenza, la tipologia, ecc...

Sanzioni – ai sensi dell'art. 83 del Reg. UE/2016/679 le sanzioni devono avere carattere di effettività, proporzionalità e dissuasività. Possono raggiungere i €20 milioni o il 4% del fatturato annuo, il maggiore dei due.

Nomina del DPO (Data Protection Officer) – la nomina è obbligatoria per enti pubblici e società che trattano un grande ammontare di dati personali in modo ricorrente.

Estensione dell'ambito di applicazione – il Nuovo regolamento si applica sia a chi detiene i dati che a chi effettua i trattamenti, inoltre viene esteso l'ambito territoriale includendo i **trasferimenti dei dati in paesi terzi**.

La metodologia Grant Thornton



La metodologia Grant Thornton

Overview

Data protection Quick Check
- Verifica dell'attuale architettura dei dati nella società, dei processi, dei rischi e della conformità alla nuova normativa Europea

Comprensione dei principali cambiamenti introdotti dal regolamento

Analisi dei risultati
- Verifica del grado di maturità delle misure esistenti rispetto al GDPR

Roadmap per l'implementazione
- Sviluppo di un piano di implementazione delle misure

Implementazione
- Identificazione e documentazione dei trattamenti dei dati;
- Realizzazione del DPIA;
- Sviluppo di un piano di risposta ai Data Breach;
- Implementazione dei diritti degli interessati;
- Dove necessario, nomina del DPO ed esternalizzazione della figura

Audit dell'efficacia delle misure introdotte
- Verifica dell'efficacia operativa dei controlli implementati

DPMS
(Data Protection Management System)

- Audit sulla GDPR
- Aggiornamento DPIA
- Formazione continua

La metodologia Grant Thornton

Approccio integrato (Consultant + Legal + ICT)

Il nuovo Regolamento Europeo GDPR ha impatti per l'impresa che coprono sia gli aspetti organizzativi, Legali e di Compliace, sia quelli tecnologici e di trattamento dei dati. Al fine di adeguarsi ai nuovi requisiti, le imprese necessitano di un **approccio integrato**, che affronti in modo coordinato tutti gli aspetti delle aree coinvolte.

GDPR Consultant

Il consulente si occupa degli aspetti organizzativi e procedurali, coordinando il progetto di adeguamento ai requisiti del GDPR: referenti aziendali, legal e ICT. Si occupa inoltre dell'attività di Risk Assessment relativa a probabilità e impatto di eventi dannosi in tema di privacy che deve essere documentato *(**DPIA** - Data Protection Impact Assessment);* eventuali violazioni ai sistemi e ai dati personali devono essere comunicate al Garante entro 72 ore, e questo richiede la predisposizione di una procedura affidabile di '*Incident response*'.

Legal

Il GDPR introduce nuovi requisiti e sfide per la funzione Legale e quella Compliance delle imprese. In molti casi si dovrà nominare un *Data Protection Officer* (DPO), L'enfasi posta sugli aspetti di responsabilità (*Accountability*) a livello organizzativo richiede un approccio proattivo, consistente ed efficace alla governance in materia di Privacy. Ciò richiedere uno sforzo di tipo legale ed organizzativo al fine di riscrivere e gestire il modo con cui si tratta la Privacy.

ICT, Security e trattamento dei dati

Le tecnologie e processi operativi e di business che supportano sono disegnati e gestiti secondo il principio *Privacy by Design*. Le funzioni che si occupato della gestione e della creazione dei dati nell'impresa (come il Data Base Administrator, o il Responsabile delle Operations) devono assicurare un governo chiaro ed efficace sul dove e come sono memorizzati e archiviati i dati personali (*Data storage*) e rispondere in modo adeguato ai requisiti del nuovo regolamento: i) per garantire un accesso più semplice ai dati degli individui; ii) diritto alla trasferibilità dei dati; iii) diritto all'oblio; iv) diritto di sapere quando i propri dati sono stati violati.

Esternalizzazione del DPO

Il servizio di DPO esternalizzato

Il GDPR, improntato sul rispetto del principio di responsabilizzazione (*accountability*), ha definito la portata della figura del DPO la quale, da mera scelta affidata alla discrezionalità della singola organizzazione, è stata innalzata a vero e proprio guardiano della privacy, obbligatoria in alcuni casi e volontaria in tutti gli altri.

- **Una figura centrale**: il GDPR pone il DPO al centro del nuovo quadro normativo come uno degli elementi chiave all'interno del sistema di *governance* dei dati, potendo questo sia favorire l'osservanza degli obblighi normativi sia fungere da interfaccia fra i soggetti coinvolti dai trattamenti di dati personali, quali: l'autorità di controllo, gli interessati o le divisioni operative all'interno di un'azienda o di un ente.
- **Competenze ed esperienza**: non basta nominare un DPO solo quando è obbligatorio, ma anche quando è opportuno. Occorre sempre, e specialmente quando la nomina è obbligatoria, che il titolare si assicuri che il DPO abbia competenze giuridiche, informatiche, di risk management e di analisi dei processi oltre a l'esperienza adeguata per poter svolgere la funzione tenendo conto del tipo di azienda, del tipo di trattamenti, delle finalità e delle attività dell'impresa o del soggetto pubblico interessato. Si sottolinea che se il DPO è inadeguato ai suoi compiti il titolare risponde della cattiva scelta fatta nominandolo con sanzioni (specie se obbligatorio) che possono essere elevate.
- **Indipendenza**: il DPO deve essere in grado di **svolgere, in modo autonomo ed indipendente, i compiti specifici del DPO**, fra i quali: informare e fornire consulenza al Titolare, al Responsabile nonché ai dipendenti, sorvegliare l'osservanza del GDPR o cooperare con l'autorità di controllo. Particolare attenzione va' quindi posta all'atto della nomina sul potenziale **conflitto di interessi** che potrebbe derivare dall'assegnazione della funzione del DPO ad un referente interno dell'azienda.

GTC offre la professionalità e le competenze dei suoi professionisti esperti di risk management, privacy e compliance al servizio delle imprese per l'assunzione del ruolo di **DPO esternalizzato**, come previsto dal regolamento.

Un'organizzazione Internazionale

Il Supporto necessario per soddisfare ogni esigenza

Con oltre 42.000 persone in oltre 130 paesi, siamo un'organizzazione veramente globale.

Quale sia la tua organizzazione o quanto grande siano le sfide che vuoi affrontare, abbiamo le risorse giuste per aiutarti.

Lavoriamo con alcune delle più grandi organizzazioni del mondo.

Siamo classificati tra le prime sette aziende in 105 mercati di tutto il mondo e siamo presenti in tutti i principali business centers e nei mercati emergenti.

42,000
people

over
130
countries

$4.6bn
revenue in 2015 (USD)

Grant Thornton | An instinct for growth™

Contatti

Gianpaolo Neri

GDPR Team Leader
Grant Thornton Consultants - Italy

M: +39 335 123 0339
E: gianpaolo.neri@gtc.it.gt.com

Francesco Pastore

Managing Partner
Grant Thornton Consultants - Italy

M: +39 392 098 5993
E: francesco.pastore@gtc.it.gt.com