Vito SARACINO
Dottore Commercialista
Revisore Contabile

REGOLAMENTO EUROPEO SULLA PROTEZIONE DEI DATI (GDPR) – NOVITA' IN MATERIA DI PRIVACY

a cura del Dott. Vito SARACINO – Dottore Commercialista e Revisore Contabile in Bitonto (BA)

Il 4 maggio 2016 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea (GUUE) il "Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE" (meglio noto come "regolamento generale sulla protezione dei dati" o "GDPR").
Il GDPR si applica a tutte le Organizzazioni (inclusi enti pubblici, imprese private e studi professionali) che a vario titolo trattano dati classificabili come "dati personali", ovvero qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»). Si considera identificabile la persona fisica 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 online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Difficile quindi che un'Organizzazione possa non rientrare nell'ambito di applicazione del GDPR.
Il GDPR diventerà definitivamente applicabile (e sanzionabile) in via diretta in tutti i Paesi UE a partire dal **25 maggio 2018**.

ADEMPIMENTI PREVISTI DAL GDPR

Tra gli adempimenti previsti dal regolamento UE sulla privacy vi sono:

- CHECKLIST PRIVACY;
- INFORMATIVA;
- CONSENSO;
- REGISTRO DEI TRATTAMENTI DI DATI PERSONALI;
- ANALISI DEI RISCHI E VALUTAZIONE D'IMPATTO DEI TRATTAMENTI;
- DATA BREACH;
- NOMINA DPO.

CHECKLIST PRIVACY

La checklist è una lista di controllo contenente tutte le informazioni utili per adeguarsi correttamente al nuovo regolamento UE 2016/679.

INFORMATIVA

L'informativa è adempimento obbligatorio e fondamentale per il trattamento dei dati personali.
L'informativa deve essere fornita per iscritto, leggibile, comunicativa, accessibile, concisa e scritta con linguaggio chiaro e semplice con un numero limitato di riferimenti normativi.
L'informativa ha, appunto, il compito di "informare" il soggetto, prima della raccolta dei suoi dati, su che fine faranno quelle informazioni (come saranno trattate, per quali scopi, con che impatto sulla sua privacy, con che tempi e limiti) e sui diritti che il soggetto potrà esercitare nei confronti di coloro che trattano quelle informazioni.
In particolare l'informativa deve contenere tutte le seguenti informazioni:

- l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante
- i dati di contatto del Responsabile della protezione dei dati, quando previsto

- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento
- qualora il trattamento sia necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, i legittimi interessi perseguiti dal titolare del trattamento o da terzi
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali
- ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale

Oltre a queste informazioni, nel momento in cui sono stati ottenuti i dati dall'interessato, il titolare del trattamento deve dare le seguenti ulteriori indicazioni:

- il periodo di conservazione dei dati
- l'intenzione del titolare del trattamento di trasferire dati personali a un Paese terzo o a un'organizzazione internazionale
- il diritto dell'interessato di proporre reclamo ad un'autorità di controllo
- l'esistenza di un processo automatizzato, compresa la profilazione, e l'indicazione delle logiche utilizzate, dell'importanza e delle conseguenze del trattamento
- il diritto di accesso ai dati da parte dell'interessato
- il diritto di rettifica e di cancellazione
- la limitazione del trattamento o l'opposizione allo stesso
- il diritto alla portabilità
- il diritto di revoca del consenso.

CONSENSO DEI DATI

Il consenso è una manifestazione di volontà che deve essere richiesta dal titolare del trattamento all'interessato per trattare i dati di quest'ultimo.

Il consenso è disciplinato dall'articolo 7 del regolamento ed ha un ruolo decisamente importante nella nuova disciplina. Il titolare del trattamento dei dati, infatti, deve sempre poter dimostrare che l'interessato ha dato il suo consenso liberamente.

Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici.

REGISTRO DEI TRATTAMENTI DI DATI PERSONALI

È possibile definirlo come un documento che dovrà contenere, per legge, una serie di informazioni sulle attività riguardanti il trattamento dei dati personali, quali:

- il nome e i dati di contatto del titolare (ed eventualmente del contitolare) del trattamento, del rappresentante del titolare e del responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali trattati;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi eventualmente i destinatari di paesi terzi non appartenenti all'Unione Europea od organizzazioni internazionali;
- nel caso in cui sia previsto, l'indicazione del fatto che i dati personali saranno trasferiti verso un paese terzo o un'organizzazione internazionale, indicando anche di quale paese od organizzazione internazionale si tratta e, inoltre, la documentazione delle garanzie previste;

- i termini ultimi stabiliti per la cancellazione delle diverse categorie di dati; e infine
- una descrizione generale delle misure di sicurezza tecniche e organizzative individuate al fine di garantire un livello di sicurezza dei dati personali adeguato al rischio cui gli stessi sono esposti.

Il registro delle attività di trattamento si configura come uno strumento fondamentale non soltanto ai fini di eventuali controlli di legittimità da parte del Garante, ma anche perché consente di avere a disposizione un quadro aggiornato dei trattamenti che vengono realizzati nell'azienda, organizzazione o soggetto pubblico.

L'art. 30 del regolamento UE precisa che il registro delle attività di trattamento dei dati dovrà essere tenuto in forma scritta, su supporto tangibile oppure, e preferibilmente, in formato elettronico, e dovrà inoltre essere messo a disposizione su richiesta dell'autorità di controllo (nel caso dell'Italia, il Garante per la protezione dei dati personali).

Un'adeguata predisposizione del registro delle attività di trattamento potrà essere, infatti, un elemento importante al fine di realizzare un corretto trattamento dei dati personali, in linea quindi con l'obiettivo di responsabilizzazione (la c.d. accountability), che, come precisato in più occasioni in questo Speciale di approfondimento sul GDPR, è uno dei principi fondamentali che il legislatore europeo ha voluto incentivare maggiormente e su cui fonda l'intera disciplina del Regolamento.

ANALISI DEI RISCHI E VALUTAZIONE D'IMPATTO:

Attraverso un'analisi dei flussi informativi la valutazione d'impatto è volta all'individuazione dei rischi derivanti dal trattamento e, quindi, dei mezzi e degli strumenti da adottare per contrastarli.
Con tale valutazione si determina la misura di responsabilità del titolare o del responsabile del trattamento, tenendo conto della natura, della portata, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità dei rischi per i diritti e le libertà degli utenti.
Quindi, il rischio inerente al trattamento è da intendersi come l'impatto negativo sulle libertà e i diritti degli interessati.

PROCESSO DI DATA BREACH;

Il GDPR disciplina il data breach prevedendo espressamente un obbligo di notifica e comunicazione in capo al titolare, in presenza di violazioni di dati personali che possano compromettere le libertà e i diritti dei soggetti interessati. Il nuovo Regolamento attribuisce alla notifica una funzione essenziale di tutela degli interessati ed estende tale obbligo alla generalità dei titolari di trattamento.
L'art. 33 impone al titolare di notificare la violazione all'autorità di controllo entro 72 ore dal momento in cui ne viene a conoscenza. Il tempo di riferimento da cui iniziano a decorrere i termini della notifica viene individuato quindi nel momento in cui il titolare acquisisce consapevolezza dell'avvenuta violazione.

NOMINA DPO

Il DPO è una figura che deve essere designata dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e controllo, nonché consultive, formative e informative, relativamente all'applicazione del Regolamento Ue 2016/679 – di seguito solo GDPR. Coopera con l'Autorità Garante e, nel contempo, è il punto di contatto per tutte le questioni connesse al trattamento dei dati personali, anche nei confronti degli interessati.

Il DPO deve possedere un'approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento. Deve essere in grado di offrire, con il grado di professionalità adeguato alla complessità del compito da svolgere, la consulenza necessaria per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, offrendo un solido e adeguato supporto al titolare, per l'osservanza della nuova normativa che impone l'adozione di un complesso di misure (anche di sicurezza) e garanzie adeguate al contesto in cui è chiamato a operare.

Il DPO deve essere, inoltre, una figura capace di agire in piena indipendenza e autonomia, senza ricevere istruzioni da alcuno, e con il potere di riferire direttamente ai vertici aziendali. Deve disporre di tutte le risorse (personale, locali, attrezzature, ecc.) necessarie per l'espletamento dei propri compiti.

Sono obbligatoriamente tenuti alla designazione del DPO il titolare e il responsabile del trattamento le cui principali attività consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; o in trattamenti su larga scala di categorie particolari di dati personali (dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni filosofiche o religiose, o l'appartenenza sindacale, oltre al trattamento di dati genetici, dati biometrici al fine dell'identificazione univoca di una persona fisica, e di dati relativi alla salute, alla vita sessuale o all'orientamento sessuale di una persona fisica) o di dati relative a condanne penali e a reati.

In base all'articolo 37, paragrafo 1, lettere b) e c) del RGPD, il concetto di trattamenti 'larga scala', deve intendersi come il trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato.

Si deve, in ogni caso, tener conto dei seguenti fattori al fine di stabilire se un trattamento sia effettuato su larga scala: il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; la durata, ovvero la persistenza, dell'attività di trattamento; la portata geografica dell'attività di trattamento.

A titolo esemplificativo sono state individuate le seguenti categorie di soggetti certamente tenuti alla nomina di un DPO:

- istituti di credito;
- imprese assicurative;
- sistemi di informazione creditizia;
- società finanziarie;
- società di informazioni commerciali;
- società di revisione contabile;
- società di recupero crediti;
- istituti di vigilanza;
- partiti e movimenti politici;
- sindacati; caf e patronati
- società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas);
- imprese di somministrazione di lavoro e ricerca del personale;
- società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione;
- società di call center;

- società che forniscono servizi informatici;
- società che erogano servizi televisivi a pagamento.

In tutti gli altri casi, la designazione del responsabile del trattamento non è obbligatoria. Ad esempio, in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale; agenti, rappresentanti e mediatori operanti non su larga scala; imprese individuali o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti.

SANZIONI

In caso di inosservanza della materia in oggetto, le sanzioni possono arrivare fino a 20 milioni di € o per le imprese fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente.

Bitonto,15 maggio 2018

Dott. Vito SARACINO
Dottore Commercialista in Bitonto (BA)
info@studiosaracino.it
www.studiosaracino.it