NOTA INFORMATIVA IN MATERIA DI PRIVACY E TRATTAMENTO DEI DATI PERSONALI ALLA LUCE DELLE NOVITA' INTRODOTTE DAL REGOLAMENTO EUROPEO *"GENERAL DATA PROTECTION REGULATION – GDPR (REGOLAMENTO UE 2016/679)".*

PREMESSA

Il nuovo Regolamento europeo **General Data Protection Regulation** *(Regolamento UE 2016/679)* **in vigore dal prossimo 25 maggio 2018 impone obblighi stringenti sul trattamento e la gestione dei dati dei cittadini europei e avrà un impatto legale, tecnologico ed organizzativo per aziende, professionisti ed enti non profit.**

LE NOVITA' INTRODOTTE DAL REGOLAMENTO EUROPEO PER LA PROTEZIONE DEI DATI

Fino ad oggi la tutela dei dati era affidata alla direttiva 46 del 1995, che necessitava di essere recepita da ogni stato membro con una propria normativa locale (In Italia il Codice Privacy D. Lgs 196 del 2003), creando però una disparità nel trattamento dei dati da paese a paese.
Per rendere il livello di protezione più omogeneo si è quindi deciso di utilizzare il Regolamento europeo, **immediatamente obbligatorio** in tutte le sue disposizioni, con efficacia diretta e immediata, e non prevede la possibilità di apportare modifiche o deroghe al testo originario da parte degli stati membri.
Non cambiano i principi sulla modalità di raccolta dei dati già in vigore. I dati devono essere:

- raccolti per finalità esplicite e legittime
- trattati in modo coerente con le finalità dichiarate nelle informative
- adeguati, pertinenti e non eccedenti rispetto a quanto è necessario al trattamento
- sempre corretti ed aggiornati
- conservati e trattati per garantire un'adeguata sicurezza e protezione anche con l'adozione di misure tecniche e organizzative

Nuovi principi:

Accountability

Il dato diventa un bene che va tutelato a sé, e il titolare diventa il solo responsabile dei trattamenti e deve dimostrare di aver valutato i rischi connessi al trattamento dei dati e di aver adottato tutte le misure idonee a garantire la tutela del dato: tenendo conto degli strumenti tecnologici a disposizione del titolare, dei costi di attuazione e dei rischi, il titolare dovrà mettere in atto misure tecniche e organizzative adeguate a garantire la protezione dei dati (trattare solo i dati necessari alle proprie finalità e limitarne l'accesso alle sole persone che ne fanno uso per la propria attività all'interno dell'organizzazione).
Per dimostrare la conformità del trattamento il titolare deve adottare la **Privacy by default**, cioè un sistema di corretta organizzazione, documentazione e tracciabilità durante il trattamento dei dati (processi gestionali e policy interne, il registro dei trattamenti o l'adesione a codici di condotta o meccanismi di certificazione), e la **Privacy by design,** cioè l'uso di sistemi informatici con il quale vengano trattati dati personali che dev'essere progettato e realizzato in modo tale da garantire la tutela del dato stesso.

Il Regolamento Europeo per la Protezione dei Dati introduce nuovi diritti dell'interessato:
Diritto all'oblio
Ottenere dal Titolare del trattamento la cancellazione, senza ingiustificato ritardo (non oltre i 30 giorni) dei dati personali che lo riguardano, quando non sussistono legittimi motivi per mantenerli (es. non sono più necessari rispetto alla finalità per cui erano stati conferiti, l'interessato revoca il consenso, i dati sono trattati in modo illecito o l'interessato si oppone al trattamento.). La cancellazione può essere rifiutata quando si abbia a che fare con il diritto di espressione o informazione, quando il trattamento adempie un obbligo legale, per motivi di pubblico interesse nella sanità o nella ricerca, per finalità statistiche o di archivio storico, o per consentire al titolare di esercitare il diritto di difesa in sede giudiziaria.

Portabilità dei dati
Ai cittadini europei sarà garantito un diritto di accesso più facile ai propri dati personali e potranno ottenerne copia (in un formato elettronico e strutturato, di uso comune, sul cui formato è lasciato al Titolare il compito di valutare quale sia il più adeguato) per trasferire gli stessi dati da un ambiente informatico ad un altro (ad esempio da un social network ad un altro). I dati personali in questione non sono solo quelli relativi a nome ed indirizzo, ma possono essere, ad esempio, la libreria online o la playing list ascoltata in streaming. Si fa riferimento anche ai dato raccolti prima dell'entrata in vigore del Regolamento. Il diritto è esercitabile quando i dati sono stati ottenuti dal Titolare attraverso sistemi automatizzati, attraverso il consenso o per l'esecuzione di un contratto.
Il Titolare non è tenuto a verificare la conformità al Regolamento del soggetto a cui trasmette i dati, ma deve imporre contrattualmente al responsabile a cui trasferisce i dati di poter adempiere alle richieste di portabilità dell'interessato.

Nuovi strumenti a disposizione del Titolare:

Data Privacy Impact Assessment (DPIA)
Prima di procedere al trattamento, il titolare deve svolgere un'analisi dei rischi generati in concreto dal trattamento dei dati, soprattutto se il trattamento prevede l'uso di nuove tecnologie (privacy by design).
Questa analisi deve:

- Considerare l'intero ciclo di vita dei dati, dalla raccolta alla cancellazione
- Descrivere in dettaglio tutte le operazioni di trattamento
- Descrivere le misure previste per affrontare i rischi connessi al trattamento
- Indicare le garanzie e le misure di sicurezza adottate per ridurre il rischio
- Essere formalizzata in un documento

Registro dei trattamenti
Il Regolamento prevede che i Titolari ed i Responsabili tengano un registro delle attività di trattamento. Sebbene rappresenti un obbligo solo per alcune tipologie di imprese o organizzazioni (quelle con oltre 250 dipendenti, quelle con meno di 250 dipendenti che trattino in modo non occasionale dati particolari, giudiziari ecc.), l'Autorità Garante ne consiglia la tenuta per tenere costantemente monitorati i flussi e quindi i rischi.

La novità è rappresentata dalla necessità di indicare – ove possibile – il termine ultimo per la cancellazione delle diverse categorie di dati, ovvero di indicare i criteri per individuare il predetto termine.

Nel caso di associazioni con più sedi sul territorio italiano, se esiste una "capogruppo" che impartisce linee guida alle altre sedi, il registro potrà essere tenuto solo dalla capogruppo e sarà sufficiente la nomina di un solo DPO; la capogruppo dovrà però impartire regole chiare e omogenee a tutte le sedi, e dovrà verificare con cadenza regolare (1 o 2 volte all'anno) che le regole siano scrupolosamente rispettate.

Nuove regole per il Data Breach (violazione dei dati)

Il Data Breach è ogni violazione di sicurezza che accidentalmente o in modo illecito comporta la distruzione, la perdita, la modifica o la divulgazione e accesso non autorizzati ai dati personali trattati

Entro 72 ore dalla scoperta il Titolare deve informare l'Autorità indicando le circostanze relative alla violazione, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Quando la violazione dei dati personali presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento deve comunicare la violazione all'interessato senza ingiustificato ritardo

La figura del DPO (responsabile della protezione dei dati)

E' obbligatoria solo in alcuni casi:

- Se il titolare è un soggetto pubblico;
- Se l'attività principale del Titolare consiste in trattamenti che, per loro natura, ambito di applicazione o finalità comportano il monitoraggio regolare e sistematico degli interessati "su larga scala";
- Se l'attività principale del Titolare consiste in trattamenti regolari e sistematici di dati particolari o giudiziari.

La nomina del DPO non dipende dal numero di soci, ma dalla tipologia di trattamento effettuata e dal rischio cui si espongono i dati. Deve essere un soggetto esterno all'azienda, deve avere requisiti di professionalità e di esperienza commisurati alla sensibilità, complessità e quantità di dati trattati e deve godere di indipendenza ed autonomia di spesa.

Ha compiti specifici:

- Informare e fornire consulenza al Titolare del trattamento nonché ai dipendenti che eseguono il trattamento
- Predisporre relazioni periodiche per il management
- Sorvegliare l'osservanza del Regolamento e di tutte le altre disposizioni anche nazionali in materia di protezione dei dati
- Vigilare che il Titolare ed il Responsabile conferiscano nomine a soggetti adeguati
- Verificare l'adozione di policy adeguate
- Sensibilizzare e formare il personale che partecipa ai trattamenti e alle attività di controllo
- Assistere il Titolare nello svolgimento della valutazione di impatto
- Predisporre e mantenere aggiornato il registro dei trattamenti

- Cooperare con l'Autorità di controllo

Per questo l'organizzazione dovrà mettere a disposizione del DPO un budget specifico.

Nuove sanzioni amministrative

Mentre rimangono invariate le sanzioni penali, le sanzioni pecuniarie amministrative subiranno un deciso incremento. Tenendo conto delle esigenze delle micro, piccole e medie imprese e organizzazioni, le sanzioni amministrative devono essere **effettive, proporzionate e dissuasive**, e sono suddivise in due scaglioni:

- Fino a 10 milioni di euro (o, per le imprese fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore)
- Fino a 20 milioni (o, per le imprese fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore)

Nell'applicazione delle sanzioni le Autorità Garanti dovranno valutare il tipo e durata della violazione, le misure di sicurezza adottate dal titolare, la natura doloso o colposa della condotta.

Cosa cambia per le organizzazioni NON PROFIT

L'Autorizzazione generale n. 3/2016 consentiva fino ad oggi il trattamento dei dati sensibili alle associazioni, fondazioni, comitati e altri organismi di tipo associativo, che possono trattare i dati sensibili senza richiedere uno specifico consenso per perseguire gli scopi determinati dalla legge, dall'atto costitutivo o dallo statuto (in particolare scopi culturali, religiosi, politici, sindacali, sportivi o agonistici non professionisti e di istruzione, di formazione, di ricerca scientifica, patrocinio, tutela dell'ambiente, salvaguardia dei diritti civili, nonché assistenza sociale o socio sanitaria o beneficienza).

Il prossimo 24 maggio 2018 l'Autorizzazione generale n. 3 / 2016 diventerà inefficace e sarà necessario attendere che il Comitato indichi i trattamenti che si ritiene improbabile possano presentare un rischio elevato. Fino ad allora anche le organizzazioni non profit dovranno adeguarsi al regolamento europeo. In sintesi, tutti i soggetti pubblici e privati che trattano dati di cittadini europei sono soggetti al regolamento, quindi anche tutte le associazioni indistintamente.

COSA FARE QUINDI?

Da un punto di vista prettamente operativo le operazioni da compiere partono da una prima analisi della situazione interna e per motivi di semplificazione, a nostro avviso, è conveniente e opportuno affidarsi ad un partner specializzato (società apposite di servizi informatici e collegati o *software house*) che possa seguire almeno tutta la fase di analisi e implementazione delle *compliance* con la normativa.

I passi da seguire possono essere così schematizzati:

- Effettuare un *assessment* per individuare la tipologia di dati raccolti, i tipi di trattamenti effettuati e le finalità per le quali i dati sono raccolti;
- Individuare chi tratta i dati e aggiornare le nomine;

- Dotarsi di procedure interne per limitare al massimo i rischi connessi al trattamento dei dati particolari;
- Dotarsi di sistemi IT adeguati a limitare al massimo i rischi connessi al trattamento dei dati, sfruttando anche il *cloud*;
- Accertarsi che i prodotti installati siano coperti dal supporto del produttore e che essi siano sempre aggiornati, altrimenti il rischio di esposizione di dati e informazioni è elevato. Si parte anche semplicemente dalla verifica dei sistemi operativi in azienda e dal controllo del loro periodo di. Sarà importante automatizzare il più possibile la gestione degli aggiornamenti per potere dimostrare di essere coperti dalle vulnerabilità appena vengono pubblicate e aver così ridotto per quanto è possibile i *breach* all'infrastruttura. E' fondamentale l'aggiornamento e il controllo non solo delle infrastrutture aziendali, ma di qualsiasi dispositivo utilizzato. Anche per smartphone e tablet in dotazione ci si deve porre gli stessi interrogativi, verificarne l'aggiornamento, studiare un modo per gestire la flotta.
- Predisporre informative aggiornate ed adeguate;
- Implementare sistemi efficaci per la raccolta del consenso per il trattamento di dati particolari.

Vi consigliamo dunque di prendere contatti con i vostri consulenti informatici per avere maggiori informazioni operative in merito, in modo da adempiere alle novità previste entro la scadenza del **25/05/2018** prossimo.

Roma, 12/04/2018 Studio Sanguigni