SODIET

Ai gentili Sigg. Clienti

URGENTE

CIRCOLARE N. 24/2018

Milano, 17 aprile 2018

Oggetto: novità in tema di trattamento dei dati personali

Introduzione

Il Regolamento UE 2016-679 (di seguito GDPR) del 27 aprile 2016, pubblicato sulla Gazzetta Ufficiale UE del 4 maggio 2016, sarà pienamente esecutivo dal 25 maggio 2018, abrogando la direttiva del '95 sulla protezione dei dati personali che è stata recepita dalla normativa nazionale attuale.

Pur collocandosi in continuità con la normativa precedente, il GDPR introduce alcune rilevanti novità, a partire dalle sanzioni amministrative che configurano un vero e proprio cambio di scala rispetto alla normativa attuale, arrivando, in funzione del tipo di violazione, a prevedere sanzioni fino a 20 milioni di euro o al 4% del fatturato complessivo dell'azienda o del gruppo di aziende.

Le novità del GDPR

La principale novità del GDPR riguarda il principio di *accountability* del Titolare posto alla base della nuova normativa, cioè la responsabilizzazione del Titolare rispetto alle misure, organizzative e tecniche, poste in essere per conformarsi al GDPR. In base a questo principio, al Titolare è riconosciuto un certo livello di discrezionalità nel processo di adeguamento a fronte del quale è posto, però, l'obbligo di documentare le scelte fatte e le ragioni che le hanno motivate nell'ottica dell'adeguamento alla norma.

Vi sono poi alcune importanti misure che innovano la materia, le più importanti delle quali sono rispettivamente:

- nuovi diritti riconosciuti agli interessati e una particolare attenzione alla tutela dei minori;
- redazione e aggiornamento del Registro dei trattamenti, cioè dell'elenco delle operazioni (trattamenti) effettuate dal Titolare che prevedono l'utilizzo di dati personali;
- l'obbligo di definire a priori i termini di conservazione dei dati personali trattati e di dichiarare tale termine nell'informativa comunicata all'interessato;
- nuovi obblighi posti in capo al Titolare, tra cui:
  - l'obbligo di notifica al Garante delle violazioni di sicurezza relative a dati personali e la comunicazione della violazione agli interessati, se necessario;
  - l'obbligo di tenere conto della *Data Protection* fin dalla progettazione, in caso di sviluppo di nuovi servizi o per la revisione di quelli esistenti;
  - l'obbligo di procedere a una analisi approfondita dell'impatto sui diritti e le libertà degli interessati quando l'innovazione comporti rischi particolari anche in virtù delle tecnologie innovative utilizzate;
- la riaffermazione della necessità di basare le misure di sicurezza su un'attenta analisi dei rischi;

Sodiet Consulting Srl
via Montebello, 27
20121 Milano

Reg. Imp. Milano
Cod. Fisc. e P. Iva 07191110969
R.E.A. Milano 1941973
Cap. Soc. Euro 20.000,00 i.v.

Tel +39 02 62694866
Fax +39 02 6595001
Email: sodiet@sodiet.it
www.sodiet.it

- il ridisegno dei rapporti fra il Titolare e i fornitori di servizi che trattano dati personali per conto del Titolare stesso, con la previsione, a determinate condizioni, della responsabilità solidale dei due soggetti per i danni eventualmente provocati;
- la nuova figura del *Data Protection Officer* finalizzata a facilitare la corretta applicazione del GDPR da parte del Titolare.

Le principali prescrizioni del GDPR

Come detto, tra le novità introdotte dal regolamento vi è il principio di "*responsabilizzazione*" (c.d. *accountability*), che attribuisce direttamente ai titolari del trattamento il compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali. In altri termini titolari e responsabili dovranno adottare comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento, decidendo in via autonoma le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Come evidenziato dal Garante uno dei criteri è sintetizzato dall'espressione inglese "*data protection by default and by design*", ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "*al fine di soddisfare i requisiti*" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio e richiede un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili. Si tratta in altri termini di valutare il rischio inerente al trattamento e di adottare le misure idonee a mitigare sufficientemente il rischio.

In questo ambito, le misure di sicurezza devono "*garantire un livello di sicurezza adeguato al rischio*" del trattamento; peraltro, la lista di cui al paragrafo 1 dell'articolo 32 è una lista aperta e non esaustiva ("*tra le altre, se del caso*"). Per lo stesso motivo, non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza (*ex* articolo 33, Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da articolo 32 del regolamento.

In quest'ottica, la nuova disciplina impone ai destinatari un diverso approccio nel trattamento dei dati personali, prevede nuovi adempimenti e richiede un'intensa attività di adeguamento, preliminare alla sua definitiva applicazione a partire dal 25 maggio 2018.

Con riguardo ai singoli adempimenti si sintetizzano alcune indicazioni metodologiche utili sulle misure organizzative necessarie per adeguarsi alla particolare disciplina:

- il nuovo regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; i fondamenti di liceità del trattamento sono indicati all'articolo 6 del regolamento e coincidono, in linea di massima, con quelli previsti attualmente dal Codice *privacy* - D.Lgs. 196/2003;
- il consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutte le caratteristiche individuate dal regolamento. In caso contrario, è opportuno adoperarsi prima di tale data per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il regolamento, se si vuole

Sodiet Consulting Srl
via Montebello, 27
20121 Milano

Reg. Imp. Milano
Cod. Fisc. e P. Iva 07191110969
R.E.A. Milano 1941973
Cap. Soc. Euro 20.000,00 i.v.

Tel +39 02 62694866
Fax +39 02 6595001
Email: sodiet@sodiet.it
www.sodiet.it

continuare a fare ricorso a tale base giuridica. In particolare, occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato, per esempio all'interno di modulistica. Occorre prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice, chiara. In tale contesto è opportuno che i titolari di trattamento verifichino la rispondenza delle informative attualmente utilizzate a tutti i criteri sopra delineati, con particolare riguardo ai contenuti obbligatori e alle modalità di redazione, in modo da apportare le modifiche o le integrazioni eventualmente necessarie ai sensi del regolamento;

- vanno individuati i responsabili del trattamento e anche gli incaricati. Al riguardo il regolamento:
  - fissa più dettagliatamente (rispetto al Codice) le caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento attribuendogli specifici compiti: deve trattarsi, infatti, di un contratto e deve disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'articolo 28 al fine di dimostrare che il responsabile fornisce "garanzie sufficienti" – quali, in particolare, natura, durata e finalità del trattamento o dei trattamenti assegnati, e categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento;
  - consente la nomina di *sub*-responsabili del trattamento da parte di un responsabile;
  - prevede obblighi specifici in capo ai responsabili del trattamento, in quanto distinti da quelli pertinenti ai rispettivi titolari (tenuta del registro dei trattamenti svolti, l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti, la designazione di un DPO).

  All'uopo andrà all'uopo verificato che i contratti o altri atti giuridici che attualmente disciplinano i rapporti con i rispettivi responsabili siano conformi a quanto previsto, in particolare, dall'articolo 28, paragrafo 3, del regolamento.

  Pur non prevedendo espressamente la figura dell'"incaricato" del trattamento, il regolamento non ne esclude la presenza in quanto fa riferimento a "*persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile*". Per gli incaricati occorre una nomina contenente peraltro le istruzioni operative per i trattamenti;
- andrà valutata la designazione di un "responsabile della protezione dati" (DPO) per l'attività esercitata. Il regolamento tratteggia le caratteristiche soggettive e oggettive di questa figura (indipendenza, autorevolezza, competenze manageriali: si vedano articoli 38 e 39). Il DPO coopera con l'Autorità (e proprio per questo, il suo nominativo va comunicato al Garante e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali (articoli 38 e 39 del Regolamento). Secondo le indicazioni del Regolamento, la nomina del DPO è obbligatoria:
  - se il trattamento è svolto da un'Autorità pubblica o da un organismo pubblico, con l'eccezione delle autorità giudiziarie nell'esercizio delle funzioni giurisdizionali; oppure
  - se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure
  - se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati;

Sodiet Consulting Srl
via Montebello, 27
20121 Milano

Reg. Imp. Milano
Cod. Fisc. e P. Iva 07191110969
R.E.A. Milano 1941973
Cap. Soc. Euro 20.000,00 i.v.

Tel +39 02 62694866
Fax +39 02 6595001
Email: sodiet@sodiet.it
www.sodiet.it

- a partire dal 25 maggio 2018, tutti i titolari dovranno notificare all'Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati. Pertanto, la notifica all'autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazioni anche gli interessati, sempre "senza ingiustificato ritardo". All'uopo sarà necessario predisporre protocolli organizzativi che consentano di intervenire tempestivamente e procedere senza ritardo alla comunicazione al Garante;
- tutti i titolari di trattamento dovranno in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati.

Si rimane a disposizione per ogni ulteriore chiarimento.

Cordiali saluti,

Sodiet Consulting S.r.l.

Sodiet Consulting Srl
via Montebello, 27
20121 Milano

Reg. Imp. Milano
Cod. Fisc. e P. Iva 07191110969
R.E.A. Milano 1941973
Cap. Soc. Euro 20.000,00 i.v.

Tel +39 02 62694866
Fax +39 02 6595001
Email: sodiet@sodiet.it
www.sodiet.it