IL NUOVO REGOLAMENTO EUROPEO SULLA PRIVACY

(GDPR – REG. UE 2016/679)

Spett. Azienda,

il 4 maggio 2016 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il testo del **nuovo Regolamento europeo sulla privacy (Reg. (UE), 27 aprile 2016, n. 2016/679**); stante la natura della norma, regolamento e non direttiva, non è richiesta una legge nazionale di recepimento ed è quindi **immediatamente esecutivo**.

Le nuove **norme del Regolamento (General Data Protection Regulation - GDPR) si applicheranno improrogabilmente a partire dal 25 maggio 2018, per consentire ad** enti pubblici e privati, imprese e professionisti, di adeguarsi ai nuovi adempimenti.

Dato personale.

Il nuovo regolamento introduce innanzitutto un ampliamento del concetto di "**dato personale**". Il GDPR considera dati personali tutti quelli che possono servire ad identificare un individuo compresi: dati riguardanti la sua "*identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*".

La liceità del consenso.

Il Regolamento conferma, rispetto al Codice della privacy (D.lgs 196/2003), che il trattamento dei dati debba innanzitutto trovare fondamento nella **liceità**, pertanto il consenso raccolto prima del 25 maggio 2018 resta valido solo se possiede detta caratteristica. In caso contrario, occorrerà raccogliere nuovamente il consenso, verificando che la richiesta di consenso sia chiaramente distinguibile da altre richieste rivolte all'interessato, per esempio all'interno di una modulistica (art. 7.2.). Rilevante sarà prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice, chiara (art. 7.2).

L'informativa.

(Il **contenuto**). Il contenuto dell'informativa è indicato in maniera tassativa dagli art. 13 par. 1 e 14 par. 1 del Regolamento; in particolare, rispetto alla normativa previgente, il titolare deve sempre specificare:

- i dati di contatto del DPR-DPO (Responsabile della protezione dei dati - Data Protection Officer), ove esistente,

- la base giuridica del trattamento,

- qual è il suo interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento,
- se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti,
- il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione,

- il diritto di presentare un reclamo all'autorità di controllo.

Nel caso di dati personali non raccolti direttamente presso l'interessato (art. 14 del Regolamento), l'informativa deve essere fornita entro un termine che non può superare un mese dalla raccolta, oppure al momento della comunicazione dei dati (a terzi o all'interessato).

(La **forma**). Il Regolamento si occupa, inoltre, di specificare molto più in dettaglio rispetto al Codice le caratteristiche dell'informativa, che deve essere:

- concisa,
- trasparente,
- intelligibile per l'interessato,
- facilmente accessibile,

- scritta con un linguaggio chiaro e semplice.

In linea generale l'informativa viene resa per iscritto e preferibilmente in formato elettronico (soprattutto nel contesto di servizi on-line anche se sono ammessi "*altri mezzi*" (quindi – si ritiene - anche oralmente, fermo restando il rispetto delle caratteristiche di cui sopra – art. 12, paragrafo 1- e l'onere più gravoso, in tal caso, di dimostrare l'avvenuto rispetto dei medesimi requisiti). Il Regolamento ammette l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "*in combinazione*" con l'informativa estesa (art. 12, paragrafo 7); queste icone dovranno essere identiche in tutta l'U.E. e saranno definite prossimamente dalla Commissione europea.

Così come statuito anche in precedenza dal Codice della privacy, l'informativa deve essere fornita all'interessato **prima** di effettuare la raccolta dei dati (se raccolti direttamente presso l'interessato); se, invece, i dati non sono raccolti direttamente presso l'interessato, l'informativa deve comprendere anche le categorie dei dati personali oggetto di trattamento.

In ogni caso, il titolare deve specificare:

la propria identità e quella dell'eventuale• rappresentante nel territorio italiano,

le finalità del trattamento,•

i diritti degli interessati (compreso il diritto alla• portabilità dei dati), se esiste un responsabile del trattamento e la sua identità,

• quali sono i destinatari dei dati.

Modalità per l'esercizio dei diritti.

Il Regolamento ha introdotto la novità per cui il termine per la risposta all'interessato è di 1 mese, estendibile fino a 3 mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego. La risposta fornita all'interessato, oltre ad essere intelligibile, deve essere anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

(Il **diritto di accesso)**. Il regolamento, all'art. 15, ha introdotto il diritto di accesso, prevedendo il diritto di ricevere una copia dei dati personali oggetto di trattamento ed ha precisato che fra le informazioni che il titolare deve fornire non rientrano le "*modalità*" del trattamento, mentre occorre indicare il periodo di conservazione previsto o, se non è possibile, i criteri utilizzati per definire tale periodo, nonché le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi. Si evidenzia come i titolari possano consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali.

(Il **diritto di cancellazione-diritto all'oblio**). Per quanto concerne il diritto di cancellazione (o diritto all'oblio – art. 17) è stato introdotto l'obbligo per i titolari di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati. Questo diritto ha un campo di applicazione più esteso se si considera che l'interessato ha diritto di chiedere la cancellazione dei propri dati anche dopo la revoca del consenso al trattamento.

Il diritto di limitazione del trattamento è stato ampliato, rendendolo esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento. Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (es: consenso dell'interessato, accertamento diritti in sede giudiziaria).

(Il **diritto alla portabilità dei dati).** Il diritto alla portabilità dei dati (art. 20) è uno dei nuovi diritti previsti dal regolamento, applicabile soltanto ai dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato stesso. Non si applica, invece, ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili solo i dati che siano stati forniti dall'interessato al titolare. Inoltre, il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

Novità in termini di adempimenti da parte di titolari e responsabili del trattamento.

Il titolare ed il responsabile del trattamento cooperano, su richiesta, con il Garante nell'esecuzione dei suoi compiti. L'art. 32 sez. 2 prevede, in particolare, che le due figure dovranno:

- avere la capacità di assicurare riservatezza, integrità, disponibilità, resilienza dei sistemi e dei servizi di trattamento;
- avere la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

- adottare una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Sia il titolare che il responsabile dovranno far sì che chiunque agisca sotto la loro autorità ed abbia accesso ai dati personali non tratti tali dati se non sia stato **preventivamente istruito** dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Registro delle operazioni di trattamento.

Tutti i titolari e i responsabili di trattamento, tranne gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (v. art. 30, paragrafo 5), devono tenere un **Registro delle operazioni di trattamento** i cui contenuti sono indicati all'art. 30. Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante della privacy, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – indispensabile per ogni valutazione e analisi del rischio. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Data breach.

Dall'entrata in vigore del regolamento, tutti i titolari dovranno notificare all'Autorità di controllo le violazioni di dati personali (**data breach**) 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. La notifica all'Autorità dell'avvenuta violazione è quindi subordinata alla valutazione del rischio per gli interessati, che spetta al titolare. 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 veda art. 33, paragrafo 5); tale obbligo non è diverso, nella sostanza, da quello attualmente previsto dall'art. 32-bis, comma 7, del Codice. Si raccomanda, pertanto, ai titolari di trattamento di adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Per quanto riguarda la figura del responsabile della protezione dei dati, tra i suoi compiti è stata introdotta la sensibilizzazione e la formazione del personale" e la sorveglianza sullo svolgimento

della valutazione di impatto di cui all'art. 35. La sua designazione è obbligatoria in alcuni casi (si veda art. 37), e il regolamento tratteggia le caratteristiche soggettive e oggettive di questa figura (indipendenza, autorevolezza, competenze manageriali: si vedano art. 38 e 39).

Le Sanzioni

Il GDPR ha introdotto un quadro sanzionatorio **ben più severo** rispetto al precedente Codice della privacy, non soltanto per quanto riguarda l'entità degli importi, ma anche per quanto concerne le ipotesi per cui possano essere comminate le sanzioni (amministrative pecuniarie e/o penali). Nonostante il GDPR focalizzi la propria attenzione, prevalentemente, sulle violazioni di tipo amministrativo, all'interno del Considerando 149 è stabilito che gli Stati Membri "*dovrebbero poter stabilire disposizioni relative a sanzioni penali*" come strumento di attuazione e tutela della nuova disciplina, pur sempre in ossequio al principio del *ne bis in idem*. All'interno del GDPR è presente anche un margine di discrezionalità circa la possibilità di infliggere una sanzione e la determinazione dell'importo della stessa. Ciò non implica un'autonomia gestionale delle sanzioni in capo alle Autorità nazionali competenti, ma fornisce, a queste ultime, alcuni criteri su come interpretare le singole circostanze del caso. Nello specifico, i criteri per la determinazione delle sanzioni amministrative pecuniarie, di cui all'articolo 83 paragrafo 2 sono: (i) natura, gravità e durata della violazione; (ii) carattere doloso o colposo della violazione; (iii) grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi.

Da quanto esposto sopra emerge dunque che con il nuovo Regolamento sono state **ampliate** notevolmente le regole già esistenti in tema di tutela dei dati personali. Partendo da un allargamento del concetto stesso di "dati personali", si è poi passati ad un ampliamento dei **diritti** dei titolari degli stessi, così come, dall'altra parte, degli **obblighi** invece gravanti sui soggetti titolari del relativo trattamento; il tutto completato da un **meccanismo sanzionatorio** anch'esso intensificato sotto vari profili.

Ne consegue la necessità di porre una attenzione maggiore al tema in esame che, come si è visto, gli organismi europei, ora ancor più che in passato, hanno inteso valutare e regolamentare con maggiore interesse.

Per ovvie esigenze di spazio la presente guida non può avere contenuto esaustivo, ma per una analisi più approfondita della questione sarà possibile per gli interessati fare riferimento, oltre che – ovviamente – al testo della norma comunitaria che ha introdotto il GDPR, ai chiarimenti forniti dallo stesso **Garante per la protezione dei dati personali** (http://www.garanteprivacy.it).

Rimanendo a disposizione, porgiamo i più cordiali saluti.

Il Direttore

(dott. Gianluca Ghini)