IL NUOVO "REGOLAMENTO EUROPEO"

Il nuovo "**Regolamento Europeo sulla Protezione dei dati Personali**", che sostituirà l'attuale Direttiva 95/46/CE e, supererà l'attuale Codice della Privacy (D.Lgs 196/03), è stato pubblicato in Gazzetta Ufficiale UE il 04 Maggio 2016 e, diventerà definitivamente applicabile, in via diretta, in tutti i Paesi UE, a partire dal **25 Maggio 2018**, quando i titolari e i responsabili del trattamento dei dati (le aziende, i professionisti, gli enti pubblici, etc...) dovranno garantire il pieno rispetto degli adempimenti previsti dal nuovo Regolamento Europeo. Il nuovo Regolamento Europeo avrà un "approccio più dinamico" rispetto alla normativa vigente e, opererà come un "Sistema di gestione", più simile a quello tipico del "sistema di gestione della sicurezza delle informazioni", descritto dalla ISO 27001. Il nuovo Regolamento Europeo conferma alcuni adempimenti già previsti dalla vigente normativa Privacy, da aggiornare alla luce del nuovo impianto normativo (a titolo di esempio non esaustivo, nomina dei responsabili e degli ex incaricati del trattamento dei dati, informativa agli interessati e raccolta del consenso, etc...), e introduce una serie di novità, tra le quali Vi segnaliamo le seguenti:
Di seguito un breve riepilogo delle principali novità che verranno introdotte dal nuovo Regolamento Europeo:

- Le tutele previste dal nuovo Regolamento si applicheranno alle sole **PERSONE FISICHE**, in relazione al trattamento dei loro dati personali.

- Alcune **DEFINIZIONI** subiranno una modifica sostanziale. Ad esempio, il vecchio "incaricato del trattamento", il cui termine veniva utilizzato per indicare le figure con mansioni esecutive, non troverà più una esatta definizione, se non quella di "*chiunque agisca sotto l'autorità del Titolare o del Responsabile del trattamento*". Quindi quest'ultima definizione sostituirà quella attuale di incaricato.

- Gli "**EX DATI SENSIBILI**" e gli "**EX DATI GIUDIZIARI**" troveranno posto solo in parte nell'articolo dedicato alle definizioni; a loro vengono dedicati due articoli ad hoc (Art. 9 e Art. 10).

- Saranno soggetti al nuovo Regolamento anche i trattamenti dei dati personali effettuati da un titolare del trattamento o da un responsabile del trattamento non stabilito nell'Unione ma, che riguardino interessati stabiliti nell'Unione Europea.

- L'**INFORMATIVA** dovrà contenere più elementi rispetto al passato (a titolo di esempio non esaustivo, l'identità e le coordinate di contatto del titolare del trattamento e del suo eventuale rappresentante; le coordinate di contatto dell'eventuale responsabile della protezione dei dati; le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale; il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare questo periodo; i diritti che l'interessato può esercitare, etc…) ma, le informazioni dovranno essere coincise, facilmente accessibili e comprensibili, utilizzando un linguaggio semplice e chiaro (ad esempio, inglobando simboli grafici, rendendole accessibili via web, etc…)

- Il **CONSENSO** dovrà essere espresso mediante un'azione positiva inequivocabile con la quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare che i dati personali che lo riguardano siano oggetto di trattamento (ad esempio mediante dichiarazione scritta, anche elettronica, o orale; ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in questo contesto che l'interessato accetta il trattamento proposto). Il consenso, inoltre, dovrà essere dimostrabile, distinguibile in base alle finalità per cui viene richiesto, in forma comprensibile e facilmente accessibile (utilizzando un linguaggio semplice e chiaro), revocabile in qualsiasi momento.
  Per i **MINORI** di 16 anni (o se previsto, per i minori con un età inferiore ma, non al di sotto dei 13 anni) occorre che sia espresso o autorizzato dal titolare della responsabilità genitoriale.

- Vengono rafforzati i **DIRITTI** sinora riconosciuti agli interessati, adeguandoli all'ambiente virtuale e, viene conferito agli interessati un maggiore potere di controllo sui propri dati personali; in particolare, sono sanciti i seguenti diritti:
  - Diritto di accesso dell'interessato
  - Diritto di rettifica
  - Diritto alla cancellazione ("*Diritto all'Oblio*" - la possibilità, cioè, per l'interessato di decidere che siano cancellati e, non sottoposti ulteriormente a trattamento, i propri dati personali non più necessari per le finalità per le quali sono stati raccolti)
  - Diritto di limitazione di trattamento
  - Obbligo di notifica in caso di rettifica, cancellazione o limitazione dei dati
  - Diritto alla portabilità dei dati (il diritto per l'interessato di ricevere in un formato strutturato, di uso comune e leggibile a macchina i dati personali che lo riguardano forniti ad un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora)

- Diritto di opposizione
- Diritto di non essere sottoposto a un processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione

- La nuova figura del "**TITOLARE DEL TRATTAMENTO**" (in inglese "Data controller") avrà l'obbligo di:
  - mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente al presente regolamento –> (viene introdotto il c.d. principio dell'"***Accountability***").
    Dette misure sono riesaminate e aggiornate qualora necessario –> (non verranno previsti intervalli prestabiliti di aggiornamento).
  - l'obbligo di trattare i dati secondo il principio della "***Privacy By Design***" (tenendo, cioè, in considerazione le tematiche relative alla protezione dei dati, sin dalla fase di progettazione dei sistemi che permettono il trattamento dei dati personali).
  - l'obbligo di trattare i dati secondo il principio della "***Privacy By Default***" (mettendo, cioè, in atto meccanismi per garantire che siano trattati, di default, solo i dati personali necessari per ciascuna finalità specifica del trattamento e che, in particolare, la quantità dei dati raccolti e la durata della loro conservazione non vadano oltre il minimo necessario per le finalità perseguite).

- viene introdotta la figura del c.d. "**CONTITOLARE**" (in inglese, "*Joint Controller*") quando, cioè, due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento dei dati personali.

- viene introdotta la figura del c.d. "**RAPPRESENTANTE DI TITOLARI DEL TRATTAMENTO NON STABILITI NELL'UNIONE"**, quando, cioè, il trattamento dei dati personali di interessati che si trovano nell'Unione viene effettuato da un titolare del trattamento o responsabile del trattamento che non è stabilito nell'Unione.

- la nuova figura dell'"**RESPONSABILE DEL TRATTAMENTO**" (in inglese, "Data processor") dovrà presentare garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessato.
  Il responsabile del trattamento non potrà ricorrere ad un altro responsabile senza il previo consenso scritto, specifico o generale, del titolare del trattamento.

- Permane l'obbligo di nomina e di istruzione degli "**EX INCARICATI DEL TRATTAMENTO**": infatti, "*chiunque agisca sotto l'autorità del Titolare del trattamento o del Responsabile del trattamento, e che abbia accesso a dati personali, non può trattare tali dati se non è istruito in tal senso dal responsabile del trattamento*".

- Viene introdotto l'obbligo di redigere i c.d. "**REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO**" dove andranno inserite numerose informazioni sul trattamento dei dati (si tratta di una sorta di ex Documento Programmatico sulla Sicurezza).
  Tali Registri devono contenere tutte le seguenti informazioni:
  a) il nome e i dati di contatto del titolare del trattamento e, se del caso, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
  b) le finalità del trattamento;
  c) una descrizione delle categorie di interessati e delle categorie di dati personali;
  d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
  e) se del caso, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle appropriate garanzie;
  f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
  g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

  I registri sono tenuti in forma scritta, anche in formato elettronico.
  Tale obbligo **NON** si applica alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o il trattamento di dati relativi a condanne penali e a reati di cui all'articolo 10. (il principio dell'"*Accountability*" renderà consigliabile per tutti i titolari/responsabili del trattamento di adottare uno strumento simile).

- **"MISURE DI SICUREZZA"**:
  - La loro adozione sarà obbligatoria per tutti i titolari/responsabili del trattamento.
  - Tutti i titolari del trattamento/responsabili del trattamento dovranno mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono tra l'altro, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che

trattano i dati personali; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; d) una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

- Nel valutare l'adeguato livello di sicurezza, occorrerà tener conto in special modo dei rischi presentati da trattamenti di dati derivanti in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, memorizzati o comunque trattati.
- Scompaiono, quindi, le c.d. "Misure minime di Sicurezza", lasciando spazio a misure adeguate al rischio, opportunamente individuate attraverso una adeguata, preventiva e personalizzata Analisi del Rischio ("***Risk Assessment***")

- Viene introdotto l'obbligo di rispettare specifici accorgimenti in caso di eventuale "**DATA BREACH**": il titolare del trattamento, cioè, dovrà segnalare all'autorità di controllo (entro 72 ore, dal momento in cui ne è venuto a conoscenza) eventuali violazioni dei dati personali; qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrà comunicare la violazione anche agli interessati.

- viene introdotto l'obbligo di svolgere la c.d. "**VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI"** (Data Protection Impact Assessment - DPIA) per i trattamenti che prevedono, in particolare, l'uso di nuove tecnologie, e che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
  - Tale valutazione è richiesta nei seguenti casi :
    a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata sul trattamento automatizzato, compresa la profilazione, e da cui discendono decisioni che hanno effetti giuridici o incidono allo stesso modo significativamente su dette persone fisiche;
    b) il trattamento, su larga scala, di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
    c) la sorveglianza sistematica di una zona accessibile al pubblico su larga scala.
  - L'autorità di controllo redigerà e renderà pubblico un elenco delle tipologie di trattamenti soggetti al requisito della valutazione d'impatto sulla protezione dei dati; come pure, l'autorità di controllo potrà redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati.

- Questo adempimento sostituisce, di fatto, la ex “Notifica al Garante” (che non esisterà più) senza, però, che vi sia l’obbligo di invio telematico della comunicazione all’Autorità di Controllo.
- Qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenta un rischio elevato, in assenza di misure adottate dal titolare del trattamento per attenuare il rischio, il titolare del trattamento, prima di procedere al trattamento dei dati personali, deve consultare l'autorità di controllo (procedura di “**PRIOR CONSULTATION**”) –> si tratta di una sorta di ex “Verifica Preliminare”.

- Viene introdotto l’obbligo di designazione del “Responsabile della Protezione dei Dati” (**DATA PROTECTION OFFICER - DPO**) nei seguenti casi:
  a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali, oppure
  b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, campo di applicazione e/o finalità, richiedono il controllo regolare e sistematico degli interessati su larga scala, oppure
  c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.
  - Ovviamente la nomina di un “Responsabile della Protezione dei Dati” può essere fatta anche su base facoltativa.
  - Il Responsabile della Protezione dei Dati:
    - dovrà possedere qualità professionali, in particolare la conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati, e la capacità di adempiere ai compiti previsti dal Regolamento.
    - potrà essere un membro del personale del titolare del trattamento o del responsabile del trattamento oppure adempiere ai suoi compiti in base a un contratto di servizio.
    - dovrà essere coinvolto in tutte le questioni riguardanti la protezione dei dati personali.
    - il titolare del trattamento o il responsabile del trattamento dovranno sostenere il responsabile della protezione dei dati nell'esecuzione dei compiti, fornendogli le risorse necessarie per adempiere a tali compiti nonché l'accesso ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.
    - non dovrà ricevere alcuna istruzione per quanto riguarda l'esecuzione dei propri compiti.
    - non sarà rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti.

- riferirà direttamente ai massimi superiori gerarchici del titolare del trattamento o del responsabile del trattamento.
- sarà tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.
- potrà svolgere altri compiti e funzioni che non diano adito a un conflitto di interessi.
- dovrà svolgere almeno i seguenti compiti:
  a) informare e consigliare il titolare del trattamento o il responsabile del trattamento nonché i dipendenti che trattano dati personali in merito agli obblighi derivanti dal presente regolamento nonché, da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
  b) sorvegliare l'osservanza del regolamento, delle altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e gli audit connessi;
  c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
  d) cooperare con l'autorità di controllo;
  e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento di dati personali, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni su qualunque altra questione.
- Nell'eseguire i propri compiti il responsabile della protezione dei dati dovrà considerare debitamente i rischi inerenti al trattamento, tenendo conto della natura, del campo di applicazione, del contesto e delle finalità del medesimo.

- verrà promossa l'elaborazione di "**CODICI DI CONDOTTA"** destinati a contribuire alla corretta applicazione del nuovo Regolamento, in funzione delle specificità settoriali e delle esigenze specifiche delle micro, piccole e medie imprese.
  Inoltre, verranno incentivati i processi di "**CERTIFICAZIONE**" o l'acquisizione di "**MARCHI**" o "**BOLLINI**" che garantiscano la correttezza e serietà del trattamento.

- Saranno previste regole stringenti in caso di "**TRASFERIMENTO ALL'ESTERO DEI DATI**", al fine di valutare se il paese di destinazione dei dati fornisce adeguate garanzie in termini di protezione dei dati.

- Verrà introdotto il principio del "**ONE-STOP-SHOP**", cioè la possibilità per i cittadini europei di rivolgersi ad una sola delle Autorità Garanti per la protezione dei dati, in caso di violazioni da parte di imprese multinazionali.

- Verranno sanciti i seguenti ulteriori diritti:
  - Diritto di proporre **RECLAMO ALL'AUTORITÀ DI CONTROLLO**
  - Diritto a un **RICORSO CONTRO L'AUTORITÀ DI CONTROLLO**
  - Diritto a un **RICORSO CONTRO IL TITOLARE DEL TRATTAMENTO O IL RESPONSABILE DEL TRATTAMENTO**
  - Diritto al **RISARCIMENTO** (Chiunque subisca un danno materiale o immateriale cagionato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, se dimostra che l'evento dannoso non gli è in alcun modo imputabile (viene introdotto un principio simile a quello proposto dal D.Lgs 231/2001).

- Vengono introdotte **SANZIONI**, in funzione delle circostanze di ogni singolo caso, molto più pesanti rispetto al passato: in particolare potranno essere irrogate **sanzioni amministrative pecuniarie fino a 20.000.000 EURO, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.**