Pieve di Soligo, 22.03.2018

Informativa n. 5

OGGETTO: 25 MAGGIO 2018, ENTRA IL VIGORE IL NUOVO REGOLAMENTO SULLA PRIVACY

Con la presente Vi informiamo che **a partire dal 25 maggio 2018** entrerà in vigore il Regolamento (UE) 2016/679 *(G.D.P.R. - General Data Protection Regulation)* che prevede nuovi obblighi in materia di PRIVACY. Il Regolamento, come la normativa attualmente in vigore, si applica al trattamento di dati personali di persone fisiche, effettuato nell'ambito di qualsiasi attività d'impresa o professionale; non si applica invece a trattamenti effettuati nell'ambito di attività a carattere esclusivamente personale o domestico.

Le aziende dovranno quindi, prendendo in esame gli adempimenti già attuati fino ad ora sulla base del precedente Codice privacy (D.Lgs. 196/2003), verificare gli aggiornamenti e le integrazioni da effettuare per adeguarsi alle prescrizioni del nuovo Regolamento. Il lavoro di coordinamento fra vecchie e nuove procedure dovrà verificare che le azioni intraprese in questi anni (es. informative, richieste di consensi, policy e regole aziendali, misure di sicurezza, assegnazione password, sistemi di backup dei dati, ecc.) rispondano a quanto richiesto dal nuovo Regolamento. Molto di quel lavoro, se fatto bene, continuerà ad essere efficace.

Alcune novità, o modifiche alla normativa esistente, introdotte dal nuovo Regolamento, sono le seguenti:

- la responsabilizzazione (*accountability*) del titolare del trattamento, in base alla quale il titolare è competente per il rispetto di tutti i principi di legittimità ed è in grado di comprovarlo; ciò prevede l'adozione di comportamenti consapevoli e responsabili e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento;
- l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati; ciò comporta che, una volta realizzato il sistema "privacy" in azienda, esso venga sottoposto a manutenzione e adeguamento (con eventuali correttivi) costanti. Vanno quindi messe in atto misure di sicurezza tecniche ed organizzative, atte a garantire un livello di sicurezza adeguato al rischio, come ad esempio:
  - la "pseudonimizzazione"[1] e la cifratura dei dati personali;
  - la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
  - la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
  - una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

[1] Il trattamento dei dati personali viene effettuato in modo tale da conservarli in un formato che non permetta l'identificazione diretta di un individuo specifico, se non utilizzando informazioni aggiuntive. Andrà quindi sostituito un dato (es. il nome), nella scheda della persona, con un altro dato anonimo (es. un numero), potendo comunque la persona fisica essere ancora identificata in maniera indiretta, tramite un elenco dei dati originali tenuto però separato dalla scheda.

- l'applicazione dei concetti di "privacy by default" (ogni sistema deve tutelare automaticamente la privacy) e di "privacy by design" (ogni sistema deve nascere già predisposto e progettato per la tutela della privacy);
- vengono definite nuove categorie di dati, tra cui quelli genetici e biometrici nonché i dati relativi alla salute (i "dati sanitari": sono dati personali attinenti alla salute fisica o mentale di un interessato, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute);
- obbligo per il titolare di consentire all'interessato l'accesso ai propri dati personali, oggetto del trattamento effettuato dal titolare stesso, con l'estensione delle tipologie di dati a cui dare accesso.
- diritto all'oblio: il titolare ha l'obbligo di soddisfare la richiesta dell'interessato, di cancellare i suoi dati personali e che questi non siano più sottoposti a trattamento se, ad esempio:
  - non sono più necessari per le finalità per le quali sono stati raccolti;
  - viene revocato il consenso al trattamento;
  - i dati personali sono stati trattati illecitamente.
- diritto alla portabilità dei dati: il Titolare del trattamento ha l'obbligo di soddisfare la richiesta dell'interessato di trasferire i dati personali da un Titolare del trattamento ad un altro da lui indicato, senza alcun impedimento da parte del Titolare al quale sono stati forniti in precedenza i dati. I Titolari del trattamento, per rendere effettivo il diritto alla portabilità, dovranno informare gli interessati dell'esistenza di tale nuovo diritto ed adempiere ai propri doveri senza ingiustificato ritardo (in ogni caso, entro un mese dal momento in cui è pervenuta loro la richiesta), avendo sempre l'obbligo di rispondere alle richieste fatte.
  Il diritto alla portabilità dei dati personali comporta per il titolare "originario", di fornire all'interessato:
  - una copia dei propri dati personali trattati in un formato elettronico e leggibili da una macchina (Pc) e possa essere riutilizzato;
  - il salvataggio dei propri Dati personali (per ulteriori usi futuri) su un *device* personale (tablet, cellulare, ecc.).

Vengono inoltre confermati i seguenti adempimenti:

- Raccolta del consenso dall'interessato: il consenso deve essere specifico per un trattamento di dati e manifestato attraverso un dichiarazione inequivocabile e libera; non è ammesso il consenso tacito o presunto. Per i dati "sensibili" il consenso deve essere "esplicito";
- L'informativa sul trattamento dei dati, va fornita all'interessato per iscritto e preferibilmente in formato elettronico; deve essere concisa, trasparente, intelligibile e facilmente accessibile; va utilizzato un linguaggio chiaro e semplice; deve contenere alcune informazioni obbligatorie come, ad es., l'identità del Titolare, le finalità del trattamento ed il diritto dell'interessato di opporsi al trattamento dei Dati personali;
- La normativa privacy continua ad applicarsi, come già indicato in precedenza, solo al trattamento dei dati personali relativi a persone fisiche e non al trattamento dei dati delle persone giuridiche (come le società). Il trattamento dei dati personali e dei dati cosiddetti "sensibili" continua ad avere diverse procedure (più stringenti nel secondo caso).

Tra le attività che le aziende dovranno attuare, o verificare se porre in essere, entro il 25 maggio 2018, vi segnaliamo in particolare le seguenti:

- **Predisposizione del "Registro delle Attività di Trattamento"**: i titolari del trattamento dovranno tenere un registro delle operazioni di trattamento sotto la propria responsabilità: sia ai fini dell'eventuale controllo da parte del Garante (anche attraverso la Guardia di Finanza), sia per disporre di un quadro aggiornato dei trattamenti in essere all'interno dell'azienda. Il registro dovrà avere forma scritta o elettronica e dovrà essere esibito su richiesta al Garante; **le imprese con meno di 250 dipendenti sono esonerate dalla tenuta del registro dei trattamenti** (il Garante della privacy però ne consiglia comunque l'adozione), a meno che il trattamento 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 sensibili o i dati relativi a condanne penali.
- **Valutazione d'impatto sulla protezione dei dati personali ("*Data Protecion Impact Analysis*" o "DPIA")**: il Regolamento Europeo prevede che, quando un determinato trattamento – che preveda l'uso di nuove tecnologie - tenuto conto della sua natura, dell'oggetto, così come del contesto e delle finalità, possa presentare un rischio elevato per i diritti e libertà delle persone fisiche, il Titolare debba anche effettuare una valutazione d'impatto sulla protezione dei dati, per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio. L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il regolamento. Questa valutazione è sempre richiesta quando si è in presenza di:
  - trattamenti automatizzati, compresa la profilazione;
  - trattamenti su larga scala di categorie particolari di dati (sensibili);
  - viene effettuata una sorveglianza sistematica, sempre su larga scala, di zone accessibili al pubblico.
- **Responsabile della Protezione dei Dati - Data Protection Officer ("DPO"):** tale figura è dotata di una specifica formazione culturale e professionale ed assiste il titolare del trattamento, e lo coadiuva, nel conformare alla disciplina del regolamento, le attività svolte sui dati personali. Dovrà avere quindi una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati, nel controllo del rispetto a livello interno del Regolamento. Dovrà essere obbligatoriamente designato in tutte le aziende dove i trattamenti presentino particolari rischi: aziende nelle quali sia richiesto un monitoraggio regolare e sistematico degli "interessati" su larga scala (ad esempio ogni forma di tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale) oppure aziende che trattano "dati sensibili, genetici e biometrici" e "giudiziari".
  Il DPO potrà essere un dipendente della società titolare del trattamento o un soggetto esterno avente con la società un contratto di servizi: in ogni caso dovrà essere un professionista in possesso di specifici requisiti quali competenza, esperienza, indipendenza e autonomia di risorse.
  Ogni azienda dovrà rendere noti i dati di contatto del proprio DPO al "Garante per la protezione dei dati personali". Il Responsabile della Protezioni Dati dovrà riferire direttamente ai vertici gerarchici dell'azienda, senza intermediazioni e con grande autonomia e indipendenza.
- **Obbligo di comunicazione al Garante in caso di violazione dei dati personali (*data breach*):** tutte le imprese dovranno notificare al Garante, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne sono venute a conoscenza, ogni violazione di dati personali subita all'interno del proprio sistema informatico. La "violazione di dati personali" si configura quando sia avvenuta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trattati. Esempi di tali

accadimenti possono essere: la perdita di un disco non cifrato oppure l'attacco di un ransomware con richiesta di riscatto. Qualora la violazione possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, è previsto anche l'obbligo di comunicazione nei confronti di tutti gli interessati coinvolti.

- **Adozione di codici di condotta e di certificazioni:** è possibile adottare codici di condotta (una serie di regole da seguire) e/o ottenere certificazioni da organismi accreditati, per attestare l'adeguatezza delle misure di sicurezza adottate.
- **Privacy nei rapporti con i dipendenti:** il titolare del trattamento (datore di lavoro) dovrà riverificare, a seguito dell'entrata in vigore del nuovo regolamento, i diritti del lavoratore che sono stati rafforzati dal Regolamento, tra i quali:
    - il diritto ad essere informato (il datore di lavoro deve informare il lavoratore su come saranno trattati i suoi dati);
    - il diritto di accesso (anche dopo la conclusione del rapporto di lavoro, il dipendente ha diritto di accedere al proprio fascicolo);
    - il diritto di rettifica delle informazioni errate o non più attuali
    - il diritto all'oblio

  Il datore di lavoro è tenuto quindi ad informare in maniera esauriente e chiara i lavoratori sulle modalità di raccolta, trattamento e conservazione dei loro dati e su quali sono le finalità del trattamento. Vanno quindi riviste le proprie procedure interne, uniformandole a quanto previsto dal nuovo regolamento

Sanzioni: il regolamento prevede sanzioni maggiori, rispetto alla legge precedente, per i casi di violazione e non conformità; in particolare sono fissate sanzioni differenziate:

- per la mancata osservazione degli obblighi del Titolare e/o Responsabile, inclusi quelli in tema di notifica del *data breach* e di implementazione delle misure di sicurezza (***sanzioni amministrative pecuniarie fino a € 10.000.000, o fino al 2 % del fatturato totale annuo dell'esercizio precedente, se superiore***);
- per la violazione dei principi di base del Trattamento, comprese le condizioni relative al consenso, e dei diritti degli Interessati (***sanzioni amministrative pecuniarie fino a € 20.000.000, o fino al 4 % del fatturato totale annuo dell'esercizio precedente, se superiore***).

Informiamo infine che in data 21.03.2018 il Consiglio dei Ministri ha emesso un comunicato con il quale annuncia:

- la prossima pubblicazione di un decreto legislativo che adeguerà la normativa nazionale alle disposizioni del Regolamento Europeo;
- l'abrogazione della attuale normativa privacy (D.Lgs. 196/2003), a far data dal prossimo 25.05.2018.

Tenuto conto della delicatezza, complessità e tecnicità della materia trattata, suggeriamo di consultare un esperto "privacy", per la verifica preliminare della attuale situazione in azienda e per gli adeguamenti da effettuare **prima** della scadenza del 25 maggio prossimo.

Cordiali saluti. Studioconsulenza.