UESE International Ltd
Financial services, IT security, certifications

Riforma dell'Unione Europea sulla Protezione dei Dati
Regolamento UE 2016/679

A partire dal **25 maggio 2018**, con l'entrata in vigore del Regolamento Generale dell'Unione Europea sulla Protezione dei Dati (GDPR), esisterà un'**unica serie di norme sulla protezione dei dati per tutte le imprese che operano nell'UE** - indipendentemente dalla loro sede - e questo consentirà uno svolgimento più agevole delle attività commerciali. Avere norme più severe in materia di protezione dei dati significa maggior controllo sui dati personali e condizioni di parità per le imprese. I vantaggi della riforma non riguardano solo le grandi imprese, anche le piccole e medie imprese (PMI) beneficeranno della semplificazione normativa prevista dal Regolamento.

Tra le principali novità proposte dal nuovo Regolamento UE 2016/679 riteniamo opportuno segnalarvi in particolare quanto segue:

- ✓ Registro delle attività di trattamento
- ✓ Valutazione di impatto sulla protezione dei dati personali per il trattamento ad alto rischio, mediante un approccio *risk based*
- ✓ Responsabile della Protezione dei Dati - RPD (o Data Protection Officer - DPO) [le imprese che dovranno avvalersi del RPD non saranno tenute ad assumere un dipendente a tempo pieno, ma potranno nominare un consulente qualificato ad hoc]
- ✓ Comunicazione in caso di violazione dei dati personali
- ✓ Diritto all'oblio
- ✓ Diritto alla portabilità dei dati

È bene precisare che l'applicazione del Regolamento sulla Protezione dei Dati non dipende dalle dimensioni dell'azienda bensì **dalla natura delle sue attività**, con un focus specifico sui rischi per i diritti e le libertà delle persone.

La mission è **proteggere i diritti delle persone che forniscono i propri dati**, ma quali i principali adempimenti che interesseranno le Piccole e Medie Imprese?

- o Individuare il **Titolare del Trattamento (Data Controller)**: è colui che stabilisce le finalità e le modalità del trattamento ed è responsabile giuridicamente dell'ottemperanza degli obblighi previsti dalla normativa. Può essere la **persona fisica** (si pensi all'imprenditore individuale) o **giuridica** (ad esempio, la società) che tratta i dati (con la raccolta, la registrazione, la comunicazione o la diffusione)
- o Qualora il Titolare del Trattamento intenda delegare la gestione del trattamento, è obbligato a individuare il **Responsabile del Trattamento (Data Processor)**: è colui che elabora i dati personali per conto del Titolare del Trattamento. In tal caso **il rapporto tra Titolare e Responsabile dovrà essere disciplinato tramite un contratto scritto**. Occorre scegliere persone fisiche od organismi che per esperienza, capacità ed affidabilità, forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia. In ogni caso il Titolare del Trattamento rimane responsabile della gestione

BULGARIA
Uese International Ltd
address: Bulgaria – 1324 Città di Sofia, Lyulin 8
Phone +35 987 742 41 58

admin@ueseint.eu
privacy@ueseint.eu
info@ueseint.eu
www.ueseint.eu

effettuata dal Responsabile del Trattamento, dovendo garantire che le sue decisioni siano conformi alle leggi

- Le aziende con meno di 250 dipendenti **non sono obbligate a tenere un registro delle loro attività di trattamento**; a meno che il trattamento dei dati personali non sia un'attività regolare, costituisca una minaccia per i diritti e le libertà individuali o riguardi dati sensibili o casellari giudiziari
- Le PMI **non sono tenute a nominare un Responsabile della Protezione dei Dati (RPD)**, a meno che la loro attività non presenti rischi specifici in materia di protezione dei dati, come il trattamento di dati sensibili su larga scala [*per approfondimenti sull'argomento consulta l'apposita informativa "**Il Responsabile per la Protezione dei Dati**"*]
- **Le aziende sono tenute a notificare ogni violazione di dati** e ad attuare misure tecniche e organizzative adeguate per evitare possibili violazioni dei dati di cui sono responsabili, al fine di non incorrere nella violazione della riservatezza, della disponibilità o dell'integrità. Nel caso si verifichi una violazione, che costituisca un rischio per i diritti e le libertà di una persona, **è necessario informare l'Autorità di Vigilanza** (si tratta di autorità pubbliche indipendenti che vigilano, tramite i poteri investigativi e correttivi, sull'applicazione della normativa sulla protezione dei dati. Forniscono consulenza specialistica sulle questioni legate alla protezione dei dati e gestiscono i reclami presentati contro le violazioni del Regolamento Generale sulla Protezione dei Dati e delle leggi nazionali pertinenti. Ne esiste una per ogni Stato membro dell'UE, in Italia è il **Garante della Privacy**: www.garanteprivacy.it) entro le 72 ore successive alla presa di conoscenza del fatto. Se la violazione dei dati comporta un rischio elevato per le persone interessate, costoro dovranno essere informate (a meno che non siano state adottate misure efficaci di protezione tecnica e organizzativa o altre misure che garantiscano che il rischio non si verifichi più). Le autorità per la protezione dei dati dispongono di strumenti diversi in caso di inosservanza:
  - nel caso di una possibile violazione, può essere emesso un avvertimento
  - nel caso di una violazione, le possibilità comprendono un ammonimento, un divieto temporaneo o definitivo di trattamento e una sanzione pecuniaria fino a 20 milioni di Euro o fino al 4 % del fatturato totale annuo mondiale dell'azienda (delle due, la più ingente)

- **Diritto all'oblio**: il Titolare ha l'obbligo di dar corso alla richiesta dell'interessato di cancellazione dei suoi dati personali e che questi non siano più sottoposti a trattamento quando non più necessari per le finalità per le quali sono stati raccolti, così come quando abbia ritirato il consenso o si sia opposto al trattamento o il trattamento dei dati personali non sia stato conforme al Regolamento Europeo
- Il **codice di condotta** e la **certificazione**: sono strumenti volontari e spetta all'azienda decidere se aderire a un determinato codice di condotta o richiedere la certificazione. L'azienda deve comunque rispettare il GDPR, ma è possibile prendere in considerazione l'adesione a tali strumenti nel caso di un provvedimento di esecuzione nei tuoi confronti per una violazione del GDPR
- **Diritto alla portabilità dei dati**: il Titolare ha l'obbligo di dar corso alla 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 di provenienza. 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

- **Informativa Privacy**: dev'essere concisa, trasparente, intellegibile, facilmente accessibile ed espressa con un linguaggio semplice e chiaro deve delineare chi richiede i dati, perché sta trattando quei dati, per quanto tempo verranno conservati e chi li riceverà [*per approfondimenti sulla redazione dell'Informativa Privacy consulta la circolare "**Informativa privacy e Regolamento Europeo**"*]
- Attuazione di un approccio **Risk Based** che implica di tenere in considerazione lo stato di avanzamento della tecnologia, con la conseguenza di dover adattare il trattamento nel corso del tempo. In tal senso vi sono due diverse concezioni basate sulla valutazione del rischio:
  - **Privacy by Design**: le aziende, in fase di progettazione del sistema, dovranno valutare il rischio inerente alle loro attività e mettere in atto misure tecniche e organizzative prima che il trattamento inizi. Lo scopo principale è salvaguardare sin dall'inizio i principi di tutela della vita privata e di protezione dei dati personali (in presenza di un trattamento che coinvolge dati di minori gli obblighi dovranno essere più stringenti, poiché il rischio è maggiore).
  - **Privacy by Default**: le aziende devono garantire che i dati personali siano trattati nella misura necessaria e sufficiente per le finalità previste, e per il periodo strettamente necessario a tali fini. Il sistema di trattamento di dati, per impostazione predefinita, dovrebbe assicurare la non eccessività dei dati raccolti e la massima tutela della vita privata.

  L'introduzione di questi principi richiede una valutazione d'impatto sulla protezione dei dati ogni volta che il trattamento può comportare un **rischio elevato** per i diritti e le libertà delle persone.

Di seguito riportiamo alcuni accorgimenti che la tua aziende deve attuare, nel rispetto del GDPR:

- Ottenere il consenso esplicito dell'interessato per trattare i dati. Nel caso di minori, verifica il limite d'età per il consenso dei genitori
- Se usi la **profilazione** per trattare le richieste di accordi giuridicamente vincolanti, come i prestiti, devi informare i clienti e assicurarti che sia una persona (non una macchina) a controllare la procedura d'informazione, qualora la domanda venga rifiutata e garantire al richiedente il diritto a opporsi al trattamento
- Garantisci alle persone il **diritto di rinunciare al marketing diretto** che fa utilizzo dei loro dati personali
- Utilizza **misure di salvaguardia aggiuntive** (es: trattamenti con strumenti informatici dotati di sistemi di autenticazione forte, database residenti su hardware ridondato, backup schedulati con opportuna frequenza) per le informazioni circa la salute, l'appartenenza etnica, l'orientamento sessuale, le credenze religiose e politiche
- **Trasferimento di dati al di fuori dell'UE**: concludi accordi giuridici qualora tu trasferisca i dati in Paesi che non sono stati approvati dalle autorità dell'UE
- Prevedi dispositivi di sicurezza per la protezione dei dati (es: sistema di autenticazione informatica, sistema di autorizzazione, backup dei dati, software antivirus e firewall) nei tuoi prodotti e servizi fin dalle prime fasi dello sviluppo

- Se ti occupi di trattamento dei dati per un'altra azienda, assicurati di firmare un contratto inoppugnabile, che esponga l'elenco delle responsabilità di ciascuna parte

Il GDPR offre alle imprese la flessibilità di cui hanno bisogno per utilizzare in modo innovativo i Big Data (informazioni, sempre più strutturate e organizzate, che possono essere incrociate in maniera sofisticata, permettendo alle imprese di lavorare in maniera sempre più precisa. Il trend si potenzierà con sistemi che oltre a incrociare i dati, li interpretano secondo parametri e modelli consolidati e funzionali), tutelando al contempo i diritti fondamentali delle persone.

Integrare salvaguardie per la protezione dei dati in prodotti e servizi sin dalle prime fasi di sviluppo è ormai un principio essenziale dell'attività d'impresa, che incoraggia le imprese a innovare e sviluppare nuove idee, metodi e tecnologie per la protezione e la sicurezza dei dati personali. Il nuovo Regolamento ridurrà la burocrazia, eliminando, ad esempio, l'obbligo per le imprese di informare del trattamento diverse autorità nazionali per la protezione dei dati. Tutte le società che offrono servizi o prodotti e trattano i dati personali di persone stabilite nell'UE dovranno rispettare le norme dell'Unione in materia di protezione dei dati. In sostanza **la riforma consentirà alle imprese di beneficiare pienamente dell'economia digitale in tutto il mercato unico digitale dell'Unione Europea**.

Tenuto conto della complessità dell'argomento, la presente informativa viene fornita esclusivamente con carattere divulgativo per rendere nota la nuova norma senza che tale possa essere interpretata come una prestazione di consulenza professionale, conseguentemente nessuna responsabilità nei confronti di chiunque può essere imputata alla nostra Associazione per decisioni o provvedimenti adottati facendo affidamento sulle informazioni contenute nella presente circolare.

A.L.IM. è disponibile a fornire alle Aziende/Professionisti Associati la necessaria consulenza per adempiere alle nuove disposizioni in materia di privacy. Si invitano pertanto gli Associati che intendano incaricare l'Associazione a **prendere contatto in tempo utile sulla scadenza del 25 maggio 2018** al fine di definire le modalità di incarico per la consulenza in oggetto.