PRIVACY: COSA CAMBIA DAL 25 MAGGIO 2018

B.C.O. Consulting srl
Viale Lombardia 20
20131 Milano

GDPR

- Il GDPR (General Data Protection Regulation) entrerà in vigore il 25 Maggio 2018. Il regolamento, che impone obblighi stringenti sul trattamento e la gestione dei dati, interessa tutte le aziende dell'Unione Europea.
- Il GDPR a differenza dell'attuale Normativa sulla Privacy disciplinata dal Decreto Legislativo 196/2003 che indica quali sono le misure minime di sicurezza, lascia piena libertà al titolare dell'azienda, nonché titolare del trattamento dei dati, di scegliere quali azioni adottare per proteggere i suoi dati.
- Al titolare pertanto è richiesta un'azione personale e l'approccio è basato sul rischio: dato che il titolare dei dati personali è responsabilizzato, prima deve fare un assessment, cioè sapere quali dati personali tratta la sua azienda, e poi creare il registro dei trattamenti facendo la valutazione di rischio per ciascuno di essi.

B.C.O. Consulting srl
Viale Lombardia 20
20131 Milano

GDPR

- In questo contesto non esiste più il rischio minimo, ma il concetto di misura di sicurezza necessaria allo scopo.
- **Dati sensibili e non:** Ora diventa dato personale anche un identificativo online, oltre alle solite categorie di dati sensibili. Non sono ritenuti sensibili i dati economici e l'età. I dati genetici e biometrici lo sono.
- La normativa cita per la prima volta il **diritto all'oblio** : sancisce cioè il diritto ad ottenere la cancellazione dei propri dati personali.

GDPR

- Altra novità contenuta nella norma: attachi, furti, smarrimenti. Quando si subisce un attacco, va trasmessa al Garante la cosiddetta **Data breach** notification. Non si tratta solo di attacco informatico ma diventa Data breach notificabile anche la banale perdita di computer: entro le 72 ore successive all'evento anche questa va notificata al Garante, con il dettaglio di quanto successo e sulle attività di mitigazione. Ma, ad esempio, se il computer era criptato l'obbigo non scatta.
- Rispetto all'attuale Normativa sulla privacy, il GDPR parla di formazione: gli addetti al trattamento dei dati devono essere formati.
- Importante è sottolineare l'aspetto sanzionatorio : dal 2% al 4% del fatturato annuo dell'esercizio precedente.

COSA FARE IN CONCRETO?

- Individuare le figure coinvolte (Titolare del trattamento, Responsabile del trattamento e ove previsto/necessario, il DPO)
- Preparare il registro dei trattamenti scritto.
- Verificare le informative e i consensi.
- Fare un risk assessment
- Verificare di avere predisposto misure di sicurezza adeguate
- Adottare le procedure necessarie in caso di perdita dei dati, portabilità e di richieste da parte degli utenti interessati (es. diritto all'oblio), che sono da soddisfare entro 30 giorni dall'arrivo della richiesta.

B.C.O. Consulting srl
Viale Lombardia 20
20131 Milano