Convegno **Associazione ICT Dottori Commercialisti**

IMPRESE E PROFESSIONISTI

«L'UTILIZZO DEI DATI IN AZIENDA TRA NUOVE NORME E TECNOLOGIE»

22/11/2019

Avv. Cristiana Luciani

EVOLUZIONE NORMATIVA

- Il diritto alla privacy viene riconosciuto giurisprudenzialmente negli anni ‘70
- Art. 2 Cost.
- Art.8 CEDU
- Direttiva 95/46/CE
- Lg. 675/96
- Codice privacy d.lgs. 196/2003
- GDPR 2016/679
- D.lgs.101/2018

QUALE DIRITTO?

PRIVACY O PROTEZIONE DEI DATI?

- Diritti distinti
- La protezione dei dati personali può riguardare anche dati non riservati
- Libertà negativa di non subire interferenze nella propria vita privata
- Libertà positiva intesa come diritto alla autodeterminazione informativa

DATO PERSONALE

- Qualsiasi «informazione» riguardante una persona fisica, identificata o identificabile (art.4, punto 1 GDPR)
- Adeguato
- Pertinente
- Aggiornato
- Limitato a quanto necessario rispetto alle finalità per cui è trattato
- I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è conseguibile con dati anonimi o pseudonimizzati (considerando 39).

DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI

- CENTRALE per la difesa delle libertà di ognuno e di tutti
- BILANCIATO con gli altri diritti costituzionalmente garantiti (es. art.41)
- La circolazione dei dati è potenzialmente illimitata
  - Pericoli elevati
  - Sistemi di tutela più raffinati

LA DIRETTIVA «MADRE»

- bilanciamento fra interessi contrapposti
- approccio normativo di armonizzazione
- impostazione di una tutela «statica»
  - Il trasferimento dei dati personali avveniva tra interessato e titolare del trattamento

PERCHÉ IL GDPR?

- le tecnologie digitali 2.0 hanno prodotto cambiamenti radicali nel modo di vivere e, prima ancora, di pensare, di cittadini, professionisti, imprenditori.
- Possibilità di raccogliere, elaborare, gestire, sfruttare, monetizzare grandi masse di dati
- Possibilità di profilare il cliente e di proporgli un prodotto mirato

GDPR

- un moderno approccio normativo che tutela sia il dato personale sia la sua circolazione
- una diversa impostazione della tutela del mercato digitale che accresca la fiducia e sostenga l'economia digitale
- offerta di servizi gratuiti o a prezzo vantaggioso in cambio della concessione in uso dei dati (es. vendita di prodotti online, social networks, vendita di servizi digitali)

UN NUOVO APPROCCIO SOSTANZIALISTA

- non più mera tutela di un diritto del soggetto
- ma disciplina dell'impatto di un trattamento sulla persona
- non più solo dati direttamente identificativi
- ma anche meta-dati, tracce, comportamenti, profilazioni

«LA RIVOLUZIONE COPERNICANA»

il nuovo ruolo del Garante

- valutatore delle valutazioni
- dalle autorizzazioni all'*accountability*
- non più misure di sicurezza predefinite
- non più notificazione (legge di bilancio 2018 art. 1 comma 1022)
- non più verifiche preliminari

GENERAL DATA PROTECTION REGULATION

Sintesi novità più significative:

- previsione espressa del diritto all'oblio
- previsione espressa del diritto alla portabilità
- concetto della protezione dei dati «*by design*» e «*by default*»
- obbligo del DPIA in capo a titolari o responsabili di trattamenti rischiosi
- DPO
- certificazioni di conformità
- inasprimento delle sanzioni

GDPR – AMBITO DI APPLICAZIONE

Sintesi novità più significative:

- ampliamento ambito di applicazione
  - Materiale
    - trattamento interamente o parzialmente automatizzato
    - Trattamento non automatizzato di dati personali contenuti in archivio

GDPR – AMBITO DI APPLICAZIONE TERRITORIALE

- Territoriale: criterio dello stabilimento
  - La giurisdizione europea si applica nei confronti di una società extra UE ma che svolge attività effettiva e reale nel quadro di un'organizzazione stabile in UE
  - Il GDPR si applica ai trattamenti effettuati dai titolari del trattamento stabiliti in UE a prescindere dal fatto
    - Che il trattamento sia effettuato o meno in UE
    - Indipendentemente dalla nazionalità o residenza degli interessati
  - Il GDPR si applica ai trattamenti effettuati dai titolari del trattamento NON stabiliti in UE
    - se il trattamento riguarda un'offerta di beni e servizi in UE
    - Quando il trattamento costituisce un monitoraggio del comportamento (che ha luogo nell'UE) degli interessati

GDPR - PRINCIPI

- Liceità (il trattamento deve essere conforme alla legge)
- Correttezza (le caratteristiche del trattamento devono essere rese note agli interessati)
- Trasparenza (rende l'interessato consapevole delle caratteristiche essenziali del trattamento)

GDPR - PRINCIPI

- Proporzionalità
- Necessità
- Minimizzazione (il trattamento del dato deve essere ridotto al minimo)
- Limitazione della conservazione
- Finalità (i dati devono essere raccolti per finalità specifiche)
- Accountability o responsabilizzazione

GDPR – LICEITA'

Bilanciamento tra il diritto alla protezione dei dati personali e gli interessi potenzialmente confliggenti

Il trattamento è LECITO

- Se è conforme alla legge
- Se persegue uno scopo legittimo
- Se è necessario, in una società democratica per perseguire uno scopo legittimo

GDPR - ACCOUNTABILITY

- Principio più innovativo del GDPR
- Deriva dalla cultura anglosassone tradotto (impropriamente) in «Responsabilizzazione»: responsabilità, affidabilità, obbligo di rendicontazione
- Pilastro del nuovo impianto normativo
- Il protagonista diventa il titolare del trattamento
  - Adotta tutte le misure tecniche ed organizzative adeguate
  - Registro dei trattamenti (250 dip. o ipotesi specifiche)
  - Ha una visione completa ed integrata, informatica, giuridica ed organizzativa e piena consapevolezza di tutto ciò che avviene nella struttura
  - E' in grado di dimostrare che il trattamento dei dati personali degli interessati è effettuato nel rispetto del GDPR

TITOLARE DEL TRATTAMENTO

Il titolare:

- Definisce ogni tipologia di trattamento nelle sue linee essenziali
- Acquisisce consapevolezza delle attività di trattamento necessarie per svolgere il proprio lavoro
- Rende subito evidente all'Autorità di controllo quali siano le linee fondamentali dei trattamenti effettuati dall'azienda

REGISTRO DEI TRATTAMENTI ART.30 GDPR

Il titolare tiene un registro delle attività di trattamento svolte sotto la propria responsabilità in cui devono essere indicati:

- Dati di contatto (titolare, responsabile, DPO)
- Finalità
- Termini di cancellazione
- Categorie di interessati e di dati personali
- Categorie di trattamenti effettuati
- Categorie di destinatari
- Trasferimenti in paesi terzi
- Termini di cancellazione
- Misure di sicurezza

VALUTAZIONE DI IMPATTO (DPIA) ART.35 GDPR

Rappresenta un «percorso obbligatorio» che il GDPR ha previsto per tutti i trattamenti particolarmente rischiosi:

- Valutazione sistematica e globale di aspetti personali (es. profilazione), su cui si fondano decisioni che producono effetti sul piano giuridico o personale
- Trattamento su larga scala di particolari categorie di dati
- Sorveglianza sistematica su larga scala di una zona accessibile al pubblico

VALUTAZIONE DI IMPATTO (DPIA) WP29 LINEE GUIDA 4/04/2017

9 criteri da utilizzare per valutare se svolgere o meno una DPIA (dovrebbero concorrere almeno 2)

1. Assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico
3. Monitoraggio sistematico
4. Dati sensibili
5. Trattamento dati su larga scala
6. Creazione di corrispondenze o combinazioni di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazioni di nuove soluzioni tecnologiche
9. Quando il trattamento in sé impedisce agli interessati l'esercizio di un diritto

RUOLO DEL DATA PROTECTION OFFICER (DPO) ART.37 GDPR

Novità introdotta da GDPR anche se si tratta di una figura professionale già conosciuta nei paesi anglosassoni.

- Obbligo per gli organismi pubblici
- Qualora i trattamenti riguardino il monitoraggio sistematico o su larga scala
- Particolari categorie di dati
- Può essere un dipendente interno o collaboratore esterno all'azienda con contratto di servizi

RUOLO DEL DATA PROTECTION OFFICER (DPO) ART.38/39 GDPR

- Alta professionalità giuridica ed informatica
- Assoluta indipendenza
- Consulente del titolare del trattamento
- Fornisce pareri (DPIA)
- E' tenuto al segreto e alla riservatezza
- Ufficio e risorse economiche a disposizione
- Coopera con l'Autorità di controllo
- Punto di contatto con gli interessati

AUTORITÀ DI CONTROLLO

Novità introdotte:

- integrazione di compiti e poteri
- ampliamento della competenza
- Autorità capofila
- meccanismi di cooperazione fra Autorità
- meccanismo di coerenza

- reclamo: unico strumento di tutela

AUTORITÀ DI CONTROLLO

Compiti e poteri nuovi:

- adozione di clausole contrattuali *standard* (artt. 28, p. 8 e 46, p. 2, lett. *d)*)
  - designazione di un responsabile da parte di un titolare
- elencazione trattamenti soggetti e non soggetti alla DPIA (art. 35, pp. 4-6)
  - trattamenti ad elevato rischio per i diritti e le libertà delle persone fisiche
  - concretizzazione del principio della «*privacy by design*»
- consultazione a titolari e responsabili su DPIA (art. 36)
  - elevato «rischio residuo»
  - quasi-autorizzazione

AUTORITÀ DI CONTROLLO

Compiti e poteri nuovi:

- elaborazione di codici di condotta (art. 41, p. 1)
  - Destinati a contribuire alla corretta applicazione del GDPR
  - diversa natura rispetto ai codici di deontologia e buona condotta del Codice che il legislatore ha chiamato «regole di condotta»
    - Interni allo Stato Italiano
    - Carattere cogente ed integrativo della disciplina primaria
    - Devono essere rispettate obbligatoriamente
    - Condizione essenziale per la liceità e la correttezza del trattamento dei dati personali
  - adesione come prova di *compliance* e di garanzie sufficienti

AUTORITÀ DI CONTROLLO

Compiti e poteri nuovi:

- accreditamento organismi certificatori e di controllo dei codici di condotta (artt. 41, p. 1 e 43, p. 1)
  - certificazione come prova di *compliance* e di garanzie sufficienti
  - Rilasciata da un ente terzo certificatore
  - validità di 3 anni (revocabile)
  - responsabilità del certificato e del certificatore
  - Non riduce la responsabilità del titolare, ma può essere utilizzata come elemento per dimostrare il rispetto degli obblighi da parte del titolare.

AUTORITÀ DI CONTROLLO

Cooperazione :

- meccanismo dello sportello unico (*one-stop-shop*) (art. 60)
- assistenza reciproca (art. 61)
- operazioni congiunte (art. 62)

Coerenza (art. 63):

- DPB (artt. 68-76)
- parere del Board (art. 64)
- composizione delle controversie da parte del *Board* (art. 65)

NUOVO REGIME SANZIONATORIO

Il Regolamento in materia di sanzioni:

- il Legislatore nazionale DEVE prevedere sanzioni amministrative pecuniarie
  - entro il limite massimo previsto dal Regolamento
- il Legislatore nazionale PUO' prevedere «altre sanzioni»
  - in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie