La nuova Privacy – Aspettative delle imprese

Laura Marengo

Unione Industriale Torino

«Dati: un tesoro da tutelare efficacemente in azienda» - 23 novembre 2018

Quadro normativo italiano

- **Regolamento UE 2016/679, GDPR**: dal 25 maggio quadro normativo unitario UE

- **D.Lgs. 196/2003, Codice della Privacy**, come modificato dal D.Lgs. 101/2018: disposizioni italiane adeguate alla normativa europea

Imprese trattano quotidianamente dati in senso lato

- **Segreti commerciali** (know how): art. 98 D.Lgs. 30/2015, Codice della proprietà industriale
- **Dati personali**: art. 4 GDPR
- **Dati personali**: segreti commerciali + dati personali *(es. banca dati marketing profilazione clienti, banca dati cv per una società di selezione)*
- **Altri Dati**: non dati personali e non dati segreti

Minimo Comune Denominatore

- **Sicurezza dei dati**: fisica, logica e, soprattutto, informatica
- **Organizzazione dei Dati**: Privacy by Design, Privacy by Default, principio di accountability
- **Sistema organizzato di protezione dei dati**: opportunità per le imprese, valorizzazione delle banche dati, fiducia nel terzo (cliente/partner commerciale)
- **Rischio danno all'immagine per l'azienda** – Danno reputazionale
- **Dati: «un tesoro da tutelare efficacemente in azienda»**

Rapporto GDPR e Imprese: superati l'emozione e il panico del 25 maggio 2018 → fenomeno a doppia velocità

- **Multinazionali, imprese più grandi e strutturate, PMI che trattano dati come attività principale**: sistema privacy aziendale→ procedure e modelli di compliance →opportunità / sfida → efficienza e competitività

- **PMI e microimprese**: difficoltà operative ed economiche

Micro, Piccole e Medie Imprese

- **Considerando 13 GDPR**: invito a considerare le esigenze specifiche delle micro, piccole e media imprese nell'applicazione delle nuove regole, al fine di alleggerire il più possibile il peso dei nuovi adempimenti e individuare soluzioni «sostenibili» da parte degli operatori più piccoli

- **Codice Privacy**: attribuisce al Garante la previsione di misure di semplificazione per le MPMI (art. 154-bis). In particolare, il Garante promuove nelle linee guida «**modalità semplificate di adempimento degli obblighi del titolare del trattamento.**»

- Emerge l'attenzione del Legislatore all'esigenza di alleggerire il carico degli adempimenti sugli imprenditori di piccole dimensioni

- Ratio GDPR: sistemi privacy organizzati su misura

Come le imprese hanno iniziato il percorso

Il Titolare deve:

- Inquadrare il livello di rischio dei trattamenti che effettua e adottare tutte le misure adeguate. il Titolare mette in atto misure tecniche e organizzativa adeguate per garantire un livello di sicurezza adeguato al rischio (art. 32 GDPR Sicurezza del trattamento)
- Mappare i propri dati, intervistare i propri dipendenti che trattano dati personali, individuare i trattamenti, le basi giuridiche, le finalità, la tipologia di dato, il supporto informatico o cartaceo
- Evidenziare i flussi di dati all'esterno per impostare la filiera privacy (Responsabili o Titolari autonomi)
- Rivedere tutti i contratti che comportano trattamenti di dati personali
- Prestare attenzione alla comunicazione di dati all'estero soprattutto se extra UE

Organigramma privacy

- Titolare: la società
- Referente/Delegato Privacy o Personal Data Manager *(eventuale Team):* figura consigliata a livello organizzativo, con o senza procura
- Dipendenti autorizzati e istruiti al trattamento dei dati *(incarichi e/o mansionari)*
- Amministratore di sistema *(provvedimento Garante 2008/2009)*
- Responsabile della protezione dei dati (Data protection officer) in posizione apicale solo per alcune realtà

Filiera privacy

- **Titolare** del trattamento: colui che determina le finalità e i mezzi del trattamento
- **Contitolarità**: più titolari, **accordo interno** su ruoli, responsabilità e rapporti con gli interessati
- **Responsabile del trattamento** (art. 28 GDPR): tratta i dati per conto del Titolare senza una propria finalità (contratto o altro atto giuridico), solo esterno *(spesso criticità)*
- Società/Enti terzi ai quali comunico i miei dati in qualità di Titolari autonomi *(rivedere il rapporto contrattuale, cd clausole di outsourcing)*
- Gruppo societario

Continuazione Percorso

- Adeguare e/o impostare con un nuovo approccio *(diversa mentalità)* tutta la documentazione necessaria: informative dipendenti, clienti/utenti, potenziali clienti, candidati (curricula), informative web, eventuali acquisizioni del consenso (consenso inequivocabile)

- Contratti che coinvolgono il trattamento di dati personali

- Procedure/policy interne, ad es. sull'utilizzo dei sistemi informatici , sulla gestione del Data breach, sulla data retention …

- Registro delle attività di trattamento (art. 30 GDPR), obbligatorio o volontario, sempre consigliato *(strumento di lavoro e biglietto da visita),* stesura finale ma documento sempre aperto

- Istruire e formare il personale in ottica GDPR

Aspettative delle imprese

- Riesame da parte dell'Autorità Garante delle autorizzazioni generali, dei Codici di Condotta e di Deontologia ed emanazione di nuove Linee Guida
- Indicazioni/interpretazioni di concetti ricorrenti nel GDPR, quali «su larga scala»
- Elenco dei trattamenti soggetti alla valutazione di impatto (DPIA) → Allegato 1 al provvedimento n. 467 11/10/18
- Raccordo/bilanciamento **normativa privacy** (art. 2-octies Codice Privacy) e **D.Lgs. 231/2001** in materia di responsabilità amministrativa delle persone giuridiche. *Criticità: spesso i modelli organizzativi delle imprese private prevedono procedure idonee a evitare alcuni reati presupposto che richiedono l'acquisizione di dati giudiziari da parte dei propri partner commerciali*
- MPMI → semplificazioni
- Trattamento nell'ambito dei rapporti di lavoro: armonizzazione con i CCNL, bilanciamento tra legittimo interesse del datore di lavoro e diritti degli interessati

Alcune criticità operative

- Condivisione e impostazione della Filiera Privacy (Responsabili del trattamento)
- Data retention relativa ai trattamenti dei dati dei dipendenti o relativa ai dati marketing (criticità)
- Data Breach: informazioni per prevenire e per reagire tempestivamente (rispetto degli art. 33 e 34 GDPR e tutela dei propri dati) → Protocollo Polizia Postale – Unione Industriale di Torino
- DPO interno per le piccole organizzazioni: conflitto di interessi (criticità)
- Misure di sicurezza: talvolta nostalgia del vecchio allegato B … *Ambasciator non porta pena!*

Periodo di attenzione di 8 mesi D.Lgs. 101/2018

- Perfezionare e consolidare il sistema privacy aziendale: procedure/policy/disciplinari
- Concordare la filiera (Responsabile del trattamento o Titolare autonomo?)
- Rivedere i contratti in corso che coinvolgono il trattamento di dati personali
- Formazione: aumento della sensibilità dei singoli operatori (dai livelli più bassi in su)
- Diverso approccio, cambio di mentalità: dal concetto di dato come proprietà dell'interessato a quello di libera circolazione del dato per lo sviluppo dell'economia digitale

Alcune realtà

- **Periodo di attenzione**: proroga per … ahimè, adempimenti al GDPR

- Maggior tranquillità ma, comunque, **positivo aumento della sensibilità per tutti**

Dopo circa 6 mesi dal 25 maggio 2018

Sistema privacy organizzato → percorso intrapreso e/o in corso

Protezione dei dati personali: attività aziendale da presidiare e gestire *(es. TU 81/2008; D.Lgs. 231/2001; …)*

Aumenta la sensibilità e la consapevolezza di coloro che trattano dati

Diminuisce il panico: es. no ansia per i bigliettini da visita, per le comunicazioni commerciali con il proprio cliente o fornitore relative al contratto in corso … → consapevolezza che **le criticità privacy sono altre. In generale, non si deve rinunciare ai trattamenti di dati ma occorre presidiarli!**

Giusto bilanciamento tra le esigenze di tutela dei dati personali e la libertà di impresa nell'economia digitale

Dati: un tesoro da tutelare efficacemente in azienda

Grazie per l'attenzione