

GDPR ed esperienze aziendali di quest'ultimo anno

Laura Marengo

Area Servizi Legali, Compliance e Segreteria
Generale



UNIONE INDUSTRIALI
Torino





Osservatorio Unione Industriali Torino

2.200 aziende associate

20 gruppi merceologici

Filiere:

**DIGITAL INNOVATION
ENERGY AND SUSTAINABLE MOBILITY
ITALIAN LIFESTYLE
LIFE SCIENCES**

PMI: 85% DELLE AZIENDE ASSOCIATE

TAVOLO PRIVACY UNIONE INDUSTRIALI TORINO

GRUPPO DI LAVORO PRIVACY CONFINDUSTRIA

Le nuove FILIERE – Sinergie per il network delle associate



Continua la disomogeneità nell'approccio al GDPR

- **Grandi imprese, multinazionali e imprese anche PMI che investono nei servizi di trattamento dei dati:** GDPR come opportunità (dati organizzati costituiscono un patrimonio aziendale; business; fiducia dei clienti/utenti, assenza di danni reputazionali, ...)
- **Imprese manifatturiere del B2B** che trattano solo i dati necessari all'esecuzione della loro attività manifatturiera **e piccole - micro imprese:** GDPR come adempimento obbligatorio (mancanza di cultura aziendale e, per le piccole, mancanza di risorse)

Nuovo trend normativo

- Difficoltà delle imprese, specie le PMI, nell'implementazione del GDPR e, in particolare, nell'attuazione del principio di *accountability*, nella valutazione del rischio dei trattamenti e nell'individuazione delle misure di sicurezza

Difficoltà che si riscontrano nel nuovo trend normativo: prevenzione mediante organizzazione:

- **D. Lgs. 231/2001**: modelli organizzativi idonei a prevenire reati della specie di quelli verificatosi
- **Regolamento UE 2016/679**: accountability, misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio – Privacy by Design
- **Codice crisi di impresa D.Lgs 14/2019**: adeguati assetti organizzativi ai fini della tempestiva rilevazione dello stato di crisi

Privacy = Attività multidisciplinare da calare nel sistema organizzativo aziendale

- **Analisi dei rischi**
- **Monitoraggio sugli stessi**
- **Piani aziendali di sicurezza organizzativa e tecnica**
- **Disciplinari, policy, procedure, regolamenti aziendali → per fornire regole, per avere la situazione sotto controllo e sanzionare qualora vengano disattese le regole**
- **Formazione**
- **Controlli/audit**

In conclusione deve essere un sistema organizzato e gestito

PMI

- **È necessario un cambiamento culturale che per alcune realtà aziendali richiede un tempo maggiore**
- **Auspicabile l'introduzione di semplificazioni per le PMI**
- **Molto apprezzate le iniziative di formazione dedicate alle imprese (sulla scia del Progetto ARC II promosso dal Garante privacy) e, in generale, le indicazioni operative (linee guida, FAQ, ...) pubblicate sul sito del Garante (come ad es. le FAQ sulla videosorveglianza)**

MOLTE REALTA' HANNO CAPITO COME VALORIZZARE I DATI AZIENDALI

- **I dati personali e non (segreti commerciali) hanno un ruolo sempre più centrale; una corretta organizzazione degli stessi costituisce una sfida e aumenta il valore competitivo di molte realtà**
- **I dati aziendali in senso lato costituiscono il patrimonio di molte imprese, non solo dei colossi dei big data**
- **La smania di raccogliere dati disorganizzati, anche inutili, a tutti i costi, crea inefficienza, bisogna concentrarsi sui trattamenti che servono all'azienda**
- **Un piccolo esempio: è nullo il licenziamento basato su dati acquisiti illegittimamente (Cass. Civ. 25645/2023). Lo stesso trattamento di dati potrebbe essere legittimo se supportato da accordo sindacale e/o policy aziendale e/o adeguata informativa, a seconda del contesto → trattamento presidiato**
- **Il trattamento lecito dei dati è una risorsa, che aumenta e consolida la fiducia dei propri clienti e partner commerciali e aiuta a gestire l'organizzazione aziendale interna**



SFIDE

- **L'accelerazione della trasformazione digitale e dell'uso dell'Intelligenza Artificiale richiede sempre maggiori azioni da adottare per la prevenzione e gestione dei rischi privacy**
- **La protezione dei dati dei dipendenti e dei clienti è un'attività necessaria anche in un percorso per la sostenibilità ESG (Environmental, Social e Governance)**
- **Regole sulla protezione dei dati personali e non entrano sempre più a far parte dei contenuti dei Codici Etici aziendali**
- **In un'ottica di «Equità e Sostenibilità» l'adozione di un modello privacy che garantisce la protezione dei dati di tutti gli stakeholder è fondamentale**
- **L'impresa è al centro di tutti questi processi e grava sull'imprenditore il bilanciamento degli interessi in gioco al fine di avere un Modello Privacy sempre adeguato**



Temi oggetto delle più frequenti riflessioni in questo ultimo anno

Organizzazione interna:

- **Sistemi di videosorveglianza**
- **Controllo e tutela dei sistemi informatici aziendali**
- **Indagini interne all'azienda**
- **Smart working**
- **Selezione del personale** (verifica dei dati dei propri dipendenti)
- **Trattamenti connessi all'Intelligenza Artificiale** (tools aziendali)
- **Whistleblowing**

Tutte attività che hanno un forte impatto sul trattamento di dati personali e che sono legalmente conformi solo se inserite in un adeguato sistema privacy che deve prevedere idonee informative, policy aziendali, formazione, misure di sicurezza organizzative e informatiche e altri adempimenti variabili a seconda del singolo contesto



Whistleblowing

Il Whistleblowing prevede **nuovi trattamenti di dati personali** (comuni, sensibili e giudiziari), di conseguenza, richiede un aggiornamento del **Modello Privacy aziendale**

Il **Decreto 24/2023** prevede espressamente e implementa principi della normativa Privacy

All'art.13, comma 6), il Decreto prevede che i soggetti del settore pubblico e i soggetti del settore privato definiscano **il proprio modello di ricevimento e gestione delle segnalazioni interne**, individuando **misure tecniche e organizzative idonee** a garantire un livello di sicurezza **adeguato** agli specifici rischi derivanti dai trattamenti effettuati, **sulla base di una valutazione di impatto sulla protezione dei dati (DPIA)**, e disciplinando il rapporto con eventuali **fornitori esterni** che trattano dati personali per loro conto ai sensi dell'art. 28 del Regolamento UE 2016/679 (GDPR)

Inoltre il **trattamento illecito di dati personali** rientra nell'ambito oggettivo di applicazione della norma e, pertanto, può essere oggetto di segnalazioni WB

Sistema privacy → cantiere sempre aperto



Attività commerciale

- **Trasferimento dati all'estero fuori dall'UE:** nuove clausole contrattuali standard della Commissione UE per i Paesi extra UE
→ occorre rivedere gli accordi tra Titolari autonomi e tra Titolari e Responsabili del trattamento
- **USA:** il 9 luglio us il Consiglio Europeo ha votato a favore della decisione di adeguatezza, quindi a breve lo farà anche la Commissione e si aprirà una nuova finestra di legittimità per i trasferimenti di dati personali verso gli Stati Uniti. Purtroppo questa decisione politica potrebbe essere nuovamente messa in discussione
- **GOOGLE ANALYTICS:** legato alla criticità del trasferimento dati negli Stati Uniti
- **Marketing:** gestione del «nuovo marketing» (profilazione, social, trasparenza, legal design)
- **Marketing «etico e sostenibile»:** conforme alle norme di legge ma anche quale opportunità commerciale. Stop al marketing selvaggio e senza regole!
- **Social media policy:** è notevolmente aumentato l'utilizzo dei social per finalità di marketing. Necessità di adottare regole per tutelare l'immagine e la reputazione dell'impresa e per garantire i diritti del dipendente e del terzo in caso di pubblicazione di immagini e informazioni personali
- **Informative e privacy policy:** più chiare e più snelle (*tendenza virtuosa al legal design*)

Sicurezza informatica

- **Priorità strategica per la tutela dei dati**
- **Cybersecurity e Privacy viaggiano spesso in parallelo ma per un'adeguata ed efficace protezione dei dati ci deve essere convergenza tra le due attività**
- **I target degli hacker non sono solo più le grandi aziende ma anche le realtà più piccole, meno organizzate e prive di un piano contro gli attacchi**
- **Confindustria, l'Agenzia per la Cybersicurezza Nazionale e Generali hanno recentemente stipulato un Protocollo d'Intesa per diffondere la cultura della protezione digitale tra le imprese e contribuire ad alzare la soglia di attenzione delle PMI al fine di favorire una transizione digitale sicura**





Qualche consiglio

- Non limitarsi agli aspetti formali di adeguamento alla normativa privacy ma sfruttare le opportunità che si presentano
- Minimizzazione: trattare solo i dati personali necessari alla propria attività, pulizia e riordino degli archivi cartacei e informatici
- Formazione: spesso i trattamenti illeciti sono imputabili alla mancata conoscenza delle regole e delle procedure da parte del proprio personale (dal centralino al Titolare)
- Un adeguato Sistema Privacy è un'occasione per organizzare e valorizzare il patrimonio dei dati aziendali e per essere pronti alla trasformazione digitale e sostenibile dell'impresa «Forte»





grazie

Laura Marengo

Area Servizi Legali, Compliance e Segreteria
Generale



UNIONE INDUSTRIALI
Torino