L'utilizzo dei dati in azienda tra nuove norme e tecnologie

Dati personali e non

GDPR: riflessioni per le imprese

Laura Marengo

Unione Industriale Torino

Nuovo trend normativo

- **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 Desisgn
- **Codice crisi di impresa D.Lgs 14/2019**: adeguati assetti organizzativi ai fini della tempestiva rilevazione dello stato di crisi

Prevenzione mediante organizzazione

- **E’ terminata l’era delle check list**
- **Sistemi organizzativi su misura che corrispondono a principi di razionalità aziendale, adeguatezza e proporzionalità**
- **Ruolo centrale dell’imprenditore e dei suoi manager**
- **Organizzazione *BY DESIGN a 360°***

Attività multidisciplinare

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

Cambiamento culturale

- Percorso inevitabile
- Reputazione aziendale
- Competitività
- Legalmente compliant e competitive sul mercato
- Cambiamento culturale richiede tempo per le PMI

1 anno dopo

- Dopo un anno di confusione e frenesia oggi abbiamo una maggiore consapevolezza delle vere criticità “privacy”.
- Siamo passati dal terrore per il biglietto da visita (considerato il principale trattamento di dati) alla reale comprensione che le vere criticità sono altre: per es. gli algoritmi di profilazione (inizialmente neanche considerati!).
- Il sistema privacy delle aziende è stato impostato e il relativo percorso di adeguamento e aggiornamento deve proseguire.

Cosa fare ora per il sistema privacy aziendale?

- Occorre ora implementare la sostanza che regge il sistema: procedure, policy e formazione sono fondamentali!
- Il modello aziendale conforme alla nuova normativa, fondato sul principio della responsabilizzazione (accountability) del titolare del trattamento dei dati, è un cantiere sempre aperto da aggiornare e gestire come tutte le altre attività aziendali.
- Si tratta di un'attività multidisciplinare che si cala nel sistema organizzativo dell'impresa, nel quale è fondamentale coordinare e fare dialogare i vari processi.

Come valorizzare i dati aziendali per il GDPR?

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

- La smania di raccogliere dati, anche inutili, a tutti i costi, crea inefficienza, bisogna concentrarsi sui trattamenti che servono all'azienda
-
- Il trattamento lecito dei dati è una risorsa, che aumenta e consolida la fiducia dei propri clienti e partner commerciali
-
- I dati aziendali in senso lato costituiscono il patrimonio di molte imprese, non solo dei colossi dei big data

In quale misura il Titolare del trattamento ha fatto quanto ci si aspettava facesse, considerando la natura, le finalità o l'entità del trattamento alla luce degli obblighi imposti dalla normativa?

- **Art. 32 Sicurezza del trattamento**: tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Titolare del trattamento e il responsabile mettono in atto **misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio,** … .

- **Non esiste il sistema privacy perfetto ma esiste il sistema privacy adeguato**

Principi generali del trattamento di dati personali, art. 5 GDPR → alla base di tutti i trattamenti

- Liceità, correttezza e trasparenza
- Limitazione della finalità del trattamento
- Minimizzazione dei dati
- Esattezza e aggiornamento dei dati
- Limitazione della conservazione
- Integrità e riservatezza

- **Il titolare mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR**

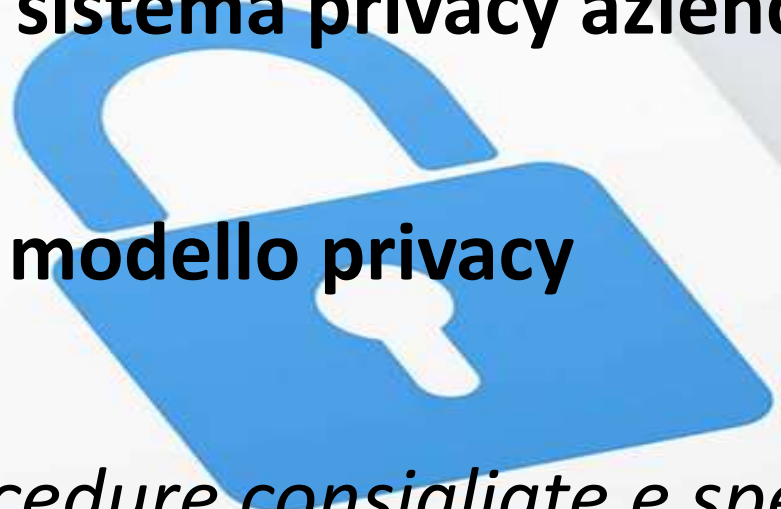
Privacy = attività aziendale multidisciplinare

- **Organigramma**
- **Filiera**
- **Rapporti con i terzi**
- **Registro delle attività di trattamento** obbligatorio o volontario → strumento fondamentale

dati vengono trattati dai dipendenti e dai collaboratori pertanto …

- **Privacy Policy, Disciplinari Tecnici, Procedure aziendali, Formazione del personale: fondamentali per rendere e garantire la conformità del proprio sistema privacy aziendale**

- **Si tratta della sostanza che regge il modello privacy**



Vediamo le principali policy e procedure consigliate e spesso pretese in fase di ispezione!

Procedura per la conservazione dei dati (Data Retention)

- I dati personali hanno una scadenza → no conservazione all'infinito

- All'interno delle organizzazioni aziendali è molto difficile tenere sotto controllo la situazione → procedure/policy → adozione di regole sui tempi e sulle modalità di conservazione e di archiviazione dei dati → successivi audit

Gestione dei diritti dell'interessato

- **Diritto di accesso (art. 15)**
- **Diritto di cancellazione o diritto all'oblio (art.17)**
- **Diritto di limitazione del trattamento (art. 18)**
- **Diritto alla portabilità dei dati (art. 20)**

- ***Mancata o insoddisfacente risposta all'interessato → reclamo al Garante → anticamera del procedimento***

Procedura consigliata, es.

La nostra società ha adottato la seguente procedura aziendale per la gestione dei diritti degli interessati

1. Esercizio dei diritti da parte del personale dipendente, stagisti, collaboratori, candidati: tutte le richieste devono essere inoltrate, entro e non oltre 2 giorni, all'ufficio personale, che, previa consultazione del delegato privacy e/o del DPO, provvederà alla corretta gestione delle stesse; *(nb personale competente e formato!)*

1. Esercizio dei diritti da parte di terzi (referenti aziendali di clienti, fornitori, partner commerciali, interessati in generale): tutte le richieste dovranno essere inoltrate, entro e non oltre 2 giorni, al responsabile ufficio commerciale che, previa consultazione del delegato privacy e/o del DPO, provvederà alla corretta gestione delle stesse.

- .....

Diritto di accesso e dati valutativi dei dipendenti

- La valutazione delle prestazioni lavorative di un dipendente effettuata da un supervisore e archiviata nel fascicolo personale del dipendente, costituisce un insieme di dati personali dello stesso dipendente.
- Ciò è vero anche se potrebbe riflettere, in tutto o in parte, solo il parere personale del superiore come, per esempio, «il dipendente non si impegna nel lavoro», e non fatti concreti, come «il dipendente è stato assente per 5 settimane negli ultimi 6 mesi.

Da: «Manuale sul diritto europeo in materia di protezione dei dati» dell'Agenzia dell'UE per i diritti fondamentali

- Dati oggettivi / dati soggettivi

- Cass. Civ. n.32533 del 14.12.2018, BNL spa / Garante

Protocollo di risposta al Data Breach: Procedure aziendali

Adottare una policy aziendale per gestire il data breach

- Formare, educare e sensibilizzare il personale
- Prevedere idonee clausole contrattuali nelle designazione dei Responsabili esterni del trattamento (vigilare)
- E naturalmente, alla base di tutto, rispettare l'art. 32 GDPR **Sicurezza del trattamento**
- **UI CONTRAST: Protocollo di Intesa con la Polizia Postale.** *Informazioni preventive per prevenire attacchi e successive per valutare la gravità dell'attacco e l'impatto che questo potrebbe avere sui trattamenti dei dati effettuati dall' impresa*

Data Breach Policy esempio

- Organigramma privacy *(trasparenza e chiarezza dei ruoli)*

- Obbligo di comunicare il DB immediatamente (nel più breve tempo possibile) al Privacy Team o al referente/delegato Privacy o al responsabile IT *(dipende dalle organizzazioni)*

- Valutazione dell'accaduto, conformemente al principio di responsabilizzazione del Titolare *(accountability):*

a) è improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche → Registro delle violazioni

b) entro 72 ore Notifica al Garante

c) eventuale comunicazione agli interessati *(non appena ragionevolmente possibile)*

d) Registro delle violazioni

Disciplinare/Regolamento Tecnico per l'utilizzo dei sistemi informatici aziendali

- Ha l'obiettivo di regolamentare l'utilizzo dei sistemi informatici aziendali (pc, cellulari, tablet …)
- Le regole si pongono l'obiettivo di fornire agli utenti **idonee misure di sicurezza e linee di comportamento adeguate** per utilizzare in modo conforme e non rischioso i sistemi informatici aziendali. Il Disciplinare è conforme al Provvedimento del Garante per la tutela dei dati personali del 1° marzo 2007.
- Fondamentale per una corretta organizzazione del sistema

Infine

- **Formazione**: diversa per livelli
- **Istruzioni operative**: su misura
- **Sensibilizzazione del personale**: dal centralino al Titolare
- **Dossier privacy** (Registro attività di trattamento, incarichi/autorizzazioni al trattamento, informative, procedure, designazioni …): necessario anche per il principio di rendicontazione, non è statico, occorre gestirlo e soprattutto deve essere conosciuto da coloro che trattano i dati personali aziendali

Cambio di mentalità

- **Tutela dei trattamenti e Libera circolazione dei dati → competitività delle imprese in un'economia digitale**
- **Percorso inevitabile**
- **Privacy → fattore reputazionale per le imprese**

Grazie per l'attenzione

Laura Marengo

Unione Industriale Torino