Privacy: il GDPR 1 anno dopo

Laura Marengo

Unione Industriale Torino

Tavolo di lavoro congiunto Protezione dei dati personali – GDPR

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?

- 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.
- 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, e a tal proposito si rammenta anche la nuova normativa che novella la disciplina della protezione dei segreti commerciali (know how), i quali hanno un valore economico finchè l'azienda riesce a mantenerli segreti mediante un'adeguata organizzazione.

Periodo di attenzione di 8 mesi
D.Lgs. 101/2018, art. 22, co 13

- «per i primi 8 mesi (dalla data di entrata in vigore del presente decreto), il Garante per la protezione dei dati personali tiene conto, ai fini dell'applicazione delle sanzioni amministrative e nei limiti in cui risulti compatibile con le disposizioni del GDPR, della fase di prima applicazione delle disposizioni sanzionatorie»

- 8 mesi dal 19 settembre 2018

- NO PROROGA ma … (in linea con alcuni termini utilizzati dal Garante «ragionevolezza» «saggezza» «pragmatismo»)

- **Garante: «tolleranza finita: al via le ispezioni»**

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

- 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

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

I 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

Regole e procedere per la conservazione dei dati

- **Data retention** in assenza di un obbligo di legge o di regolamento o di una base giuridica contrattuale

- Es. **dati marketing**: Provv. del Garante del 2005→ 24 mesi dati ex clienti e potenziali clienti e 12 mesi dati profilazione. Autorizzazioni del Garante ante GDPR → 7 anni beni di lusso e 10 anni automobili. Post GDPR → no verifiche preliminari del Garante ma responsabilizzazione del Titolare del trattamento (eventuale Valutazione di Impatto ex art.35 GDPR)

- **Dati degli ex dipendenti**: obbligo di legge 10 anni dopo la cessazione del rapporto ma … criticità quali le malattie professionali e il danno pensionistico → procedura adeguata per l'archiviazione e motivazione

Gestione dei diritti degli interessati

- Le modalità per l'esercizio di tutti i diritti da parte degli interessati sono stabilite negli artt. 11 e 12 del GDPR.
- **Termine per la risposta**. Per tutti i diritti, ricompreso il diritto di accesso, è di 1 mese, estensibile fino a 3 mesi nelle ipotesi di particolare complessità. Il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.
- **Riscontro**. Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità, e può essere dato oralmente solo se così richiede l'interessato stesso.
- **La risposta fornita dall'interessato**. Deve essere concisa, trasparente e facilmente accessibile, deve utilizzare un linguaggio semplice e chiaro.
- **Misure per agevolare l'esercizio dei diritti**. Il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura, sia tecnica che organizzativa, a ciò idonea. Benché sia il solo titolare a dover dare riscontro in ipotesi di esercizio dei diritti, il responsabile è tenuto a collaborare col titolare ai fini dell'esercizio dei diritti degli interessati.
- **Gratuità per l'esercizio dei diritti**. L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato, ma possono esservi eccezioni.

DIRITTI

- **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!)*
2. 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

Criticità: es dati giudiziari

- **D.Lgs 101/2018, art. 2-*octies***: trattamento consentito solo se autorizzato da legge o regolamento, in attesa del decreto del Ministero della Giustizia di individuazione dei trattamenti leciti

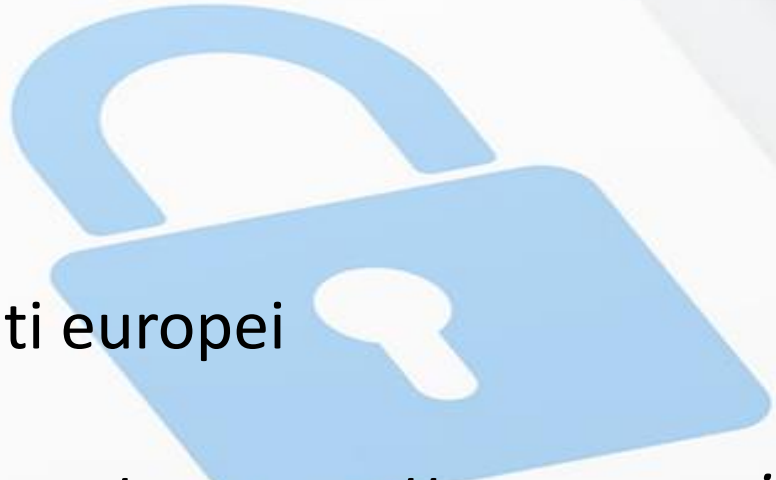
- **GDPR**: sopravvenuta inefficacia dell'autorizzazione generale del Garante n.7/2016 (trattamento dei dati giudiziari da parte di privati, di enti pubblici economici e di soggetti pubblici)

- **Dati dipendenti - Art. 8 Statuto Lav.**: È fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore.
- **DPR 313/2002**: obbligo di richiedere il certificato del casellario giudiziale in capo al soggetto che **intenda impiegare al lavoro** una persona per lo svolgimento di attività … che comportino contatti diretti e regolari con i minori *(in vigore dal 2014, lavoratori già in forza? Lacuna?)*

- **Modelli organizzativi ex d.lgs. 231/2001:** richiesta dati giudiziari a collaboratori e partner commerciali (???)

Quadro normativo Data Breach

- Art. 33 GDPR Notifica di una violazione dei dati personali all'autorità di controllo
- Art. 34 GDPR Comunicazione di una violazione dei dati personali all'interessato
- GDPR Considerando 85, 86, 87 e 88
- Linee Guida Gruppo di lavoro art.29 Garanti europei
- *Obbligo di notifica al Garante era già presente per: settore comunicazioni elettroniche, biometria, dati sanitari inseriti in Dossier e dati comunicati fra PA.*



Sicurezza dei dati

- **Fisica** *(locali, armadi, stampanti, …)*

- **Logica/organizzativa** *(policy aziendali, accordi di riservatezza, incarichi al trattamento dei dati, istruzioni, formazione…)*

- **Informatica** *(cyber security)*

Sicurezza del trattamento, art. 32 GDPR: misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio → responsabilizzazione del Titolare (accountability)

Notifica al Garante, art. 33 GDPR

- Titolare del trattamento: notifica al Garante violazione dei dati personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche *(responsabilizzazione del titolare)*

- Se la notifica non è effettuata entro le 72 ore → deve essere corredata dei motivi del ritardo

Comunicazione di una violazione dei dati personali all'interessato, art. 34 GDPR

- Quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo

- La comunicazione non è richiesta se è soddisfatta una delle seguenti condizioni:

a) misure tecniche e organizzative adeguate

b) misure atte a scongiurare il sopraggiungere di un rischio elevato per gli interessati

c) detta comunicazione richiederebbe sforzi sproporzionati, in tale caso si procede con una comunicazione pubblica o misura analoga

Il Garante può richiedere che venga effettuata la comunicazione

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**

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

- Il presente documento, ha l'obiettivo di regolamentare l'utilizzo dei sistemi informatici aziendali per gli utenti di tali servizi nell'ambito della struttura aziendale

- Le presenti 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 adottato in conformità al Provvedimento del Garante per la tutela dei dati personali del 1° marzo 2007.

RESPONSABILITÀ E SANZIONI

- L'utente, al fine di non esporre sé stesso e l'Azienda a rischi sanzionatori, è tenuto ad adottare comportamenti puntualmente conformi alla normativa vigente ed alla regolamentazione aziendale.

- Gli utenti sono responsabili del corretto utilizzo dei servizi di Internet e Posta Elettronica e dei dispositivi aziendali. Pertanto, gli utenti sono responsabili per i danni cagionati al patrimonio e alla reputazione della Società.

- Tutti gli utenti sono tenuti ad osservare e a far osservare le disposizioni contenute nel presente Disciplinare, il cui mancato rispetto o la cui violazione, costituendo inadempimento contrattuale potrà comportare:

– per il personale dipendente oltre che l'adozione di provvedimenti di natura disciplinare previsti dal Contratto Collettivo Nazionale di Lavoro, le azioni civili e penali eventualmente previste dalla normativa vigente;

– per i collaboratori oltre che la risoluzione del contratto le azioni civili e penali eventualmente previste dalla normativa vigente.

Criticità e sfide

- **Filiera privacy** (es. consulente del lavoro, medico competente …)
- Automatismi efficaci per la conformità del sistema
- Web marketing e social marketing
- Algoritmi di profilazione
- Marketing Etico (bilanciamento tra il «legittimo interesse degli imprenditori e il «diritto alla privacy» dei consumatori»)
- Internet of things e intelligenza artificiale

KEEP CALM AND COMPLY WITH GDPR

https://blog.ui.torino.it/2019/04/17/gdpr-1-anno-dopo-imprese/

Privacy → fattore reputazionale per le imprese

Grazie per l'attenzione

Laura Marengo