CORSO INTRODUTTIVO SUL NUOVO REGOLAMENTO EUROPEO SULLA PROTEZIONE DEI DATI (REG. UE 2016/679)

Claudio Terlizzi
Data Protection Officer

Agenda

- Genesi del GDPR
- Principi generali del Regolamento
- Definizioni e ambiti di applicazione
- Novità rispetto al Codice Privacy (196/2003)
- Impatti operativi

Inquadramento Storico

- Direttiva EU 95/46/CE: nata per armonizzare le leggi tra i vari Stati membri recepita in Italia con l. 675/96
- D.Lgs 196/2003 (Codice Privacy)
- Regolamento Europeo 2016/679 entrato in vigore il 25 maggio 2016 – si applica a decorrere dal 25 maggio 2018
- D.Lgs 101/2018 armonizzazione legislazione italiana al Regolamento EU

Codice Privacy D.LGS 196/2003

Modello basato sulla Compliance

- Misure minime di sicurezza (all.tecnico B)
- Informative ex art.13
- Nomina incaricati e responsabili
- Istruzione agli incaricati
- Mappatura trattamenti e misure minime
- Sanzioni amministrative e penali

GDPR - Principi Generali

- Oggetto e Finalità
- Ambito di applicazione materiale e territoriale
- Definizione di dato personale
  - Indirizzi IP, Cookie, RFID, GPS, Genetica
- Definizione di trattamento ampia
- Definizione di Profilazione
- Definizione di Pseudonimizzazione

GDPR – Profilazione

- Forma di trattamento automatizzato particolarmente invasiva destinata a valutare:
  - Alcuni aspetti della personalità
  - Rendimento professionale
  - Situazione economica
  - Stato di salute
  - Ubicazione
  - Preferenze personali
  - Affidabilità o comportamento
- Diritto dell'interessato a non essere sottoposto unicamente ad un trattamento automatizzato
- L'interessato deve essere informato sul diritto di opporsi alla profilazione in modo chiaro ed evidente

GDPR – Principi applicabili al trattamento

- Liceità, correttezza e trasparenza
  - …i dati personale sono trattati in modo lecito, corretto trasparente nei confronti dell'interessato
- Limitazione delle finalità
  - …sono raccolti per finalità determinate, esplicite legittime…
- Minimizzazione dei dati
  - I dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quelli sono trattati

GDPR – Principi applicabili al trattamento

- Esattezza e aggiornamento
  - I dati personali sono esatti e, se necessario , aggiornati
- Limitazione nella conservazione
  - Devono essere conservati per un tempo non superiore al conseguimento delle finalità per le quali sono trattati
- Integrità e riservatezza
  - Applicazione di misure tecniche e organizzative adeguate per evitare trattamenti non autorizzati, illeciti o la perdita, la distruzione o il danno accidentale

GDPR - I SOGGETTI

GDPR (EN)	GDPR (IT)	Codice Privacy
Data Controller	Titolare del trattamento	Titolare del trattamento
Data Processor	Responsabile del trattamento	Responsabile del trattamento
Persons Authorised to Process	Persona autorizzata al trattamento	Incaricato del trattamento
Data Protection Officer	Responsabile Protezione dei Dati	Non previsto

GDPR - ORGANIGRAMMA

GDPR - Titolari e Contitolari

- Stabiliscono attraverso un accordo gli impegni reciproci e :
  - Finalità
  - Mezzi di trattamento
  - Rispettive responsabilità

GDPR -II RESPONSABILE DEL TRATTAMENTO

- Il titolare del trattamento può designare uno o più responsabili del trattamento
- Il responsabile collabora con il titolare per assicurare:
  - Misure tecniche ed organizzative adeguate
  - Trattamenti conformi a Regolamento
  - Tutela dei diritti dell'interessato

GDPR -II RESPONSABILE DEL TRATTAMENTO

- Il rapporto tra titolare e responsabile deve essere regolato da contratto o altro altro atto giuridico che regoli:
  - I trattamenti disciplinati
  - La durata del trattamento
  - La finalità del trattamento
  - Il tipo dei dati personali trattati
  - Le categorie di interessati
  - Gli obblighi del responsabile
  - La possibilità per gli interessati di esercitare i propri diritti nei confronti del responsabile
  - Penalità in caso di inadempimento
- In contratto che regola il rapporto deve garantire:
  - Che i dati vengano trattati solo su istruzione documentata dal titolare
  - La riservatezza anche per gli eventuali incaricati nominati dal responsabile
  - L'adozione di misure di sicurezza adeguate
  - Che il responsabile metta a disposizione le informazioni necessarie a dimostrare il rispetto degli obblighi previsti da contratto e Regolamento

GDPR - I principi applicati al trattamento Legal Basis

- Liceità:
  - Consenso specifico
  - Necessario all'esecuzione di un contratto
  - Assolvimento obblighi legali
  - Salvaguardia di interessi vitali dell'interessato o di altra persona fisica
  - Esecuzione di un compito di interesso pubblico
  - Perseguimento di un interesse legittimo del titolare

GDPR – Il consenso

Qualsiasi manifestazione di volontà:

- Libera
- Specifica
- Informata
- Inequivocabile
- Esplicita
- Dimostrabile

GDPR – Dati Particolari

- Dati rilevanti l'origine raziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici
- Divieto di trattamento salvo deroghe ex art 9
- Necessarie misure adeguate per minimizzare il rischio di accesso non autorizzato (crittografia)
- Misure di garanzia del Garante (D.lgs 101/18)

GDPR – I diritti dell'interessato

- Trasparenza e completezza delle informazione sul trattamento
- Informativa concisa, trasparente, intellegibile e facilmente accessibile, con un linguaggio chiaro e semplice
- Informativa in forma scritta, anche con mezzi elettronici e sono se richiesto dal titolare, in forma orale

GDPR Informazioni obbligatorie

- Identità e dati dal titolare del trattamento
- Dati di contatto del DPO
- Finalità del trattamento
- I legittimi interessi perseguiti dal titolare
- Destinatari o categorie di destinatari a cui posso essere comunicati i dati
- Il periodo di conservazione dei dati
- Tutti i diritti garantiti all'interessato dalla normativa compreso il diritto di revocare il consenso
- La presenza di processi automatizzati di trattamento compresa la profilazione

GDPR Diritti dell'interessato

- Diritto di accesso
- Diritto di rettifica
- Diritto all'oblio
- Diritto alla limitazione del trattamento
- Obbligo di notifica
- Diritto alla portabilità
- Diritto di opposizione alla profilazione
- Diritto di opposizione al trattamento automatizzato

GDPR Il Titolare del trattamento

- A tutela dei diritti dell'interessato ed al fine di soddisfare i requisiti del regolamento il titolare:
  - Adotta misure tecniche ed organizzative adeguate a contenere il rischio di trattamenti non conformi
  - Deve dotarsi di un modello organizzativo in grado di applicare i principi del regolamento su ogni processo che implica un trattamento di dati personali (Privacy by Default) e nelle fasi iniziali della sua progettazione (Privacy by Design)
  - Adotta un sistema in grado di fornire l'evidenza di aver adempiuto agli obblighi previsti (Accountability)

GDPR Il registro dei Trattamenti

- Gestito in forma scritta, anche elettronica, contiene l'elenco dei trattamenti effettuati e deve essere mantenuta a disposizione dell'Autorità Garante che ne faccia richiesta
- Art 30 stabilisce il contenuto minimo
- Deve essere tenuto dal Titolare e dal Responsabile del trattamento
- Obbligatorio per aziende con più di 250 dipendenti

GDPR Sicurezza del Trattamento

- Risk assessment; valutazione del rischio per i diritti e le libertà delle persone (DPIA)
- Adozione di misure per il contenimento del rischio
- Quali tra le altre:
  - Pseudonimizzazione e cifratura
  - Misure per garantire riservatezza, integrità, disponibilità e resilienza dei sistemi
  - Capacità di rispristinare tempestivamente la disponibilità e l'accesso ai dati personali
  - Procedure per testare e verificare e valutare regolarmente l'efficacia delle misure adottate.

GDPR Data Breach

- Violazione dei dati personali, violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trattati
- Obbligo di notifica ex art 32 entro 72 ore
- Comunicazione agli interessati ex art 34

GDPR dal Prior Check al Prior consultation

- DPIA, valutazione di impatto sulla protezione dei dati richiesta prima dell'inizio del trattamento quando:
  - Valutazione sistematica di dati con trattamento automatizzato (profilazione)
  - Trattamento su larga scala di categorie particolari di dati
  - Sorveglianza sistematica di una zona accessibile al pubblico

GDPR Data Protection Officer

- Nuova figura di garanzia introdotta da GDPR obbligatoria:
  - le pubbliche amministrazioni
  - trattamenti che prevedono un monitoraggio su larga scala degli interessati
  - trattamenti su larga scala di categorie particolari di dati
- Supporta in titolare nella gestione delle tematiche inerenti la privacy
- Coopera con l'autorità di controllo

GDPR Le sanzioni

- Diritto ad ottenere al risarcimento del danno subito in violazione del Regolamento dal titolare o dal responsabile del trattamento
- Sanzioni amministrative
  - 10 milioni di euro, oppure, se superiore, fino al 2% del fatturato totale al livello mondiale
  - 20 milioni di euro, oppure se superiore, 4% del fatturato totale al livello mondiale
- Sanzioni penali (ex D.lgs 101/2018)
  - il trattamento illecito di dati personali;
  - l'acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala
  - comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala
  - false dichiarazioni rese al Garante
  - inosservanza dei provvedimenti del Garante
  - La violazione del comma 1 dell'art. 4 Stat. Lav.

GDPR Le sanzioni

- Nella modulazione del valore della sanzione si deve valutare:
  - Natura, gravità e durata della violazione
  - Carattere doloso o colposo della stessa
  - Misure adottate per attenuare il danno
  - Tipo di misure tecnico-organizzative adottate
  - Eventuali precedenti violazioni
  - Grado di cooperazione con l'Autorità di controllo
  - Categoria di dati personali interessati
  - Il rispetto di eventuali provvedimenti precedenti dell'Autorità di controllo
  - Adesione a codici di condotta o certificazioni

GDPR Impatti operativi

- Procedure e sistemi per il Data Breach
- Nomina di un DPO
- Aggiornamento Informative e gestione del consenso
- Diritto all'oblio e alla portabilità
- Ridefinire i rapporti contrattuali tra titolari e responsabili
- Gestire il registro dei trattamenti

GDPR – Le priorità

- Nomina DPO
- Misure adeguate per evitare data breach
- Registro dei trattamenti

Novità introdotte dal D.Lgs 101/2018

- Informative per la gestione dati personali dei CV
- Comunicazione e diffusione dati ex art 6 lett e GDPR
- Controlli a distanza dei lavoratori
- Consenso dei minori
- Codici deontologici e autorizzazioni generali
- Regime semplificato per PMI
- Sanzioni penali