UNIVERSITÀ POLITECNICA DELLE MARCHE

DII Dipartimento di Ingegneria dell'Informazione

unimc

# Centralità del Registro dei trattamenti nella gestione dei rischi GDPR

Flavia Cristiano

Responsabile protezione dati personali

Università degli Studi di Perugia

flavia.cristiano@unipg.it

Martedì 19 Settembre 2023

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

# Indice

- Di quali rischi parliamo nel Regolamento UE 2016/679 «GDPR»?
- Quali diritti e libertà fondamentali?
- Ruolo del Registro ex art.30 GDPR nella gestione dei rischi
- Modello base e dettagliato
- Caratterizzazione dell’attività di trattamento
- La valutazione del rischio GDPR
- Metodo di calcolo semplificato del rischio
- Scheda per la raccolta delle info dell’attività di trattamento

# Di quali rischi parliamo nel GDPR?

# Rischi GDPR

Le attività di trattamento di dati personali sono ritenute attività di per sé pericolose.

- Art. 15 comma 1 D.Lgs. 196/2003 (prev. D.Lgs.101/2018) : “Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell’articolo 2050 del codice civile”.
- Art. 2050 Codice civile, **Responsabilità per l'esercizio di attività pericolose**: “Chiunque cagiona danno ad altri nello svolgimento di un’attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno”.
- Artt. 24, 32 e 82 GDPR: il Titolare del trattamento è tenuto all’adozione di misure idonee ad evitare il danno, tenuto conto della natura …..e mezzi del trattamento. E’ esonerato dalla responsabilità se dimostra che l’evento dannoso non gli è in alcun modo imputabile
- I danni sono quelli derivanti alle persone fisiche (beni da proteggere), con particolare riguardo alle violazioni dei loro diritti e libertà fondamentali (rischi) che possono, volontariamente o meno, scaturire dal trattamento.

# Quali diritti e libertà fondamentali?

# Diritti e libertà fondamentali

- C75 GDPR: discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, discriminazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo
- Dignità, Libertà, Uguaglianza, Solidarietà, Cittadinanza e Giustizia: (Linee guida EDPB 4/2019, par. 11) la loro precisa formulazione è contenuta nella Carta dei diritti fondamentali dell'UE. È essenziale che il titolare del trattamento comprenda il significato dei principi di cui all'art. 5 GDPR e dei diritti, in quanto fondamento della protezione offerta dal GDPR.

Perché?

- Seconda Guerra Mondiale: razza, religione, orientamento sessuale, disabilità e altri dati personali sono stati utilizzati contro la popolazione.
- Council of Europe's Committee of Ministers: **Recommendation CM/Rec(2020)1 to member States on the human rights impacts of algorithmic systems**

# Ruolo del Registro ex art.30 GDPR nella gestione dei rischi

# Ruolo del Registro  ex art. 30 GDPR nella gestione dei rischi

- **Chindinica o Scienza del pericolo**:
  - La valutazione del rischio dipende dagli **obiettivi** per i quali essa viene svolta (secondo assioma), il rischio non può essere quantificato in modo assoluto, in quanto le misurazioni del rischio sono sempre relative al **contesto territoriale e temporale** in cui ogni individuo opera (primo assioma). La **conoscenza** riduce il rischio (quarto assioma)
  - Il rischio che minaccia un individuo è una funzione definita sull'**insieme della rete** che lo circonda (legge di reticolarità chindinica)
- **GDPR**:
  - Tenuto conto della natura, dell'ambito di applicazione, del contesto, delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà degli interessati, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, il titolare mette in atto misure adeguate per garantire un livello di sicurezza adeguato al rischio. Dette misure sono riesaminate e aggiornate qualora necessario.
  - Ogni titolare del trattamento (con alcune eccezioni) tiene un registro delle attività di trattamento, con contenuti minimi obbligatori descrittivi delle finalità, natura, ambito e contesto dei trattamenti

# Registro ex art. 30 GDPR: modello base e dettagliato

- Manuale RPD T4data, elaborato (per il settore pubblico) per il programma Training For Data, finanziato dall'UE, da cinque Garanti UE e due esperti del settore, inserisce nei compiti del RPD:
  - **Inventario iniziale ed essenziale** delle attività dell'organizzazione e del suo contesto operativo, inclusi legami con altre organizzazioni, comprendente tutte le attività potenzialmente concernenti dati personali;
  - **Inventario completo**, che segue quello iniziale, che dovrebbe portare alla creazione del Registro delle attività di trattamento;
  - **Registro base**, cui segue una raccolta **dettagliata** di informazioni, finalizzata a individuare accuratamente le **finalità** perseguite, la **natura**, il **contesto** e l'**ambito** del trattamento, senza i quali sarebbe inefficace la valutazione dei rischi GDPR.
- Art. 24, 25, 32, 39.2 e altri del GDPR (oltre ai vari considerando) riconducono e vincolano alla conoscenza di tali caratteristiche dell'attività di trattamento l'individuazione delle misure tecniche e organizzative idonee a garantire la sicurezza dei trattamenti e la dimostrabilità delle scelte operate.
- Anche la DPIA su una nuova tecnologia può essere riutilizzata SE, e solo se, non cambiano le caratteristiche dell'attività di trattamento per le quali è stata svolta

# Caratterizzazione dell'attività di trattamento

- **Natura**: **caratteristiche intrinseche** del trattamento in termini di operazioni di trattamento richieste (manuali e automatizzate), fasi di attuazione, flusso dei dati personali, attività/elementi nei quali si implementa, ruoli che accedono ai dati, caratteristiche tecnologiche rilevanti, coinvolgimento degli incaricati del trattamento nelle diverse operazioni, altro.
- **Contesto**: **circostanze del trattamento**, compreso l'ambiente tecnologico e organizzativo in cui viene eseguita l'attività (sistemi per il trattamento, tecnologie, processi), il mercato o il settore in cui opera, l'ambiente sociale in cui si attua, il contesto normativo, l'interazione con altre operazioni di trattamento, comunicazioni dei dati e trasferimenti internazionali che comporta, effetti collaterali sulla società, altro.
- **Ambito di applicazione**: **portata** e **estensione** del contesto (entità della quantità di dati e del numero di soggetti interessati, dei tipi e categorie di dati), ambito geografico, la durata del trattamento e della conservazione, la frequenza di raccolta e granularità, le relazioni tra le parti coinvolte e le aspettative degli interessati (Amministrativo contabile, Sanitario, Industriale,…), altro.
- **Finalità**: finalità **specifiche, esplicite e legittime** per il quale i dati personali vengono raccolti e utilizzati. Si aggiungono le finalità **strumentali e secondarie**, da non confondere con alcune delle misure che potrebbero essere adottate per raggiungere tali finalità

# La valutazione del rischio GDPR

# Valutazione del rischio GDPR

- **Beni da proteggere**: persona fisica, la sua salute e dignità, le sue libertà e diritti, come riconosciuti dalla Carta dei Diritti dell'Uomo e dalla nostra Costituzione
- **Rischio intrinseco**: discriminazioni, pregiudizi, impossibilità ad accedere ad un servizio o beneficio cui si ha diritto, limitazioni della libertà di circolazione o del diritto alla difesa, diritto alla salute, limitazione alla libertà di espressione e di voto,…
- **Rischi per la sicurezza**: distruzione, perdita, modifica, divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o **comunque trattati**
- **Fattori da considerare**: misure allo stato dell'arte e costi di attuazione, natura, ambito di applicazione, contesto e finalità del trattamento

# Metodo di calcolo semplificato del rischio

# Metodo di calcolo semplificato del rischio GDPR

## Quattro fasi (Manuale RPD)

a. **Definizione** del trattamento e del contesto in cui è effettuato (**Registro**)
b. Comprensione e valutazione dell'impatto sulle persone
c. Individuazione di eventuali minacce e valutazione della probabilità che queste possano verificarsi, con riguardo anche ai rischi per la persona
d. Valutazione del rischio complessivo, attraverso un calcolo basato sulla probabilità del verificarsi della minaccia e sulla misura dell'impatto che ne conseguirebbe, in base alle tre fasi precedenti.

**DPIA obbligatoria** per le attività di trattamento ad **alto rischio intrinseco** (WP248 Gruppo WP29, DocWeb 9058979 ottobre 2018 Garante privacy)

# Metodo di calcolo semplificato del rischio GDPR

## Comprensione e valutazione

- **Cosa preservare**: riservatezza, integrità e disponibilità delle informazioni (RID)
- **Scopo**: mitigare i rischi di accesso, utilizzo, alterazione del contenuto informativo o cancellazione, indisponibilità (o utilizzo prolungato) non autorizzati, non necessari né voluti durante **tutta la vita del dato**, tenendo conto dei disagi o effetti indesiderati (impatti) sull'interessato e di tutte le finalità del trattamento, incluse quelle legali secondarie, p.e. esercizio del diritto di difesa (*p.e. tutela Whistleblower*)
- **Contesto:** finalità perseguite, modalità di trattamento utilizzate, rispetto dei princìpi art. 5 GDPR, realtà organizzativa e suo modello (centralizzato o distribuito), livello di formazione del personale addetto al trattamento

# Metodo di calcolo semplificato del rischio GDPR

## Individuazione minacce e valutazione probabilità

- **Misura qualitativa dell'impatto** (si valuta su ciascuna RID e si prende il Max):
  - Basso (1): Piccoli inconvenienti superabili senza difficoltà
  - Medio (2): Inconvenienti significativi, superabili con alcune difficoltà
  - Alto (3): Conseguenze significative che si dovrebbero poter superare ma con gravi difficoltà
  - Critico (4): Conseguenze significative o irreversibili, non superabili
- **Aree nelle quali valutare le minacce (**5 domande ciascuna, risposta S/N, probabilità= numero Si**):**
  a) Risorse di rete e tecnologiche,
  b) Processi o procedure connessi al trattamento,
  c) Soggetti e persone coinvolti nel trattamento,
  d) Settore di attività e scala del trattamento (quantità dei dati trattati, dei trattamenti applicati e dei tempi di conservazione)

# Metodo di calcolo semplificato del rischio GDPR

## Valutazione qualitativa rischio complessivo

| | LIVELLO DI IMPATTO | | | |
|---|---|---|---|---|
| **probabilità minacce** | | **Basso** | **Medio** | **Alto - Critico** |
| | **Bassa** | | | |
| | **Media** | | | |
| | **Alta** | | | |

Nei **progetti di maggior complessità**, derivante dalla numerosità e tipologia dei dati personali trattati, dalla tipologia e finalità dei trattamenti, dalle tecnologie utilizzate o dal numero di partner partecipanti al progetto, è consigliato https://www.enisa.europa.eu/news/enisa-news/securing-personal-data-a-risky-business. Se risultato giallo o rosso procedere alla DPIA

# Scheda per la raccolta delle info dell’attività di trattamento

# Ssssscheda per la raccolta delle info dell’attività di trattamento

- Supporto per intervista guidata, da adattare alla realtà aziendale
- Specifica per unità organizzativa (*il livello di dettaglio è una scelta del vertice aziendale*)
- Strumento del RPD per inventario e registro

Consente:

  - Standardizzazione modus operandi
  - Sensibilizzazione e formazione utente
  - Semplificazione dell’aggregazione attività per il Registro, tramite campi chiave

e….Si può sempre migliorare!


# Grazie dell’attenzione