

# **Corso Privacy Avanzato**

**Avv. Aurora Cavo (DPOffice Regione Toscana – Consorzio Metis)**

- Il **data flow**. Descrizione, funzione e rilevanza
- **L'individuazione dei ruoli data protection** e la regolarizzazione dei rispettivi rapporti sotto il profilo del trattamento dei dati personali (**DPA**)
- **L'informativa** sul trattamento dei dati personali. Contenuti obbligatori
- **Data breach**. Processo ed esempi
- **DPIA**. Processo ed esempi di trattamenti soggetti all'obbligo di valutazione d'impatto



# Accountability. Data Protection by design & by default



## ➤ Art. 24 GDPR

L'Ente deve «...essere in grado di dimostrare che il trattamento è effettuato conformemente al presente regolamento...»

Il principio di *accountability* è il presupposto di ciascun trattamento di dati personali, dettandone le regole di evidenza documentale e procedurale. E' altresì l'approccio pratico che mira allo sviluppo/adozione di strumenti che possono essere utilizzati per documentare i trattamenti e renderne conto all'Autorità Garante e agli interessati.



## **Accountability: doppia veste**

Principio che ispira  
l'adeguamento dell'Ente  
alla normativa data  
protection

Evidenza che dimostra la  
*compliance* dell'Ente alla  
normativa data protection

## ➤ **Scopo**

L'*accountability* mira all'utilizzo di strumenti per documentare le proprie attività sui dati personali e renderne conto all'Autorità Garante e agli interessati.

## ➤ **Data Protection Policy** regionale

1. **Accountability organizzativa:** come l'organizzazione si è modificata per adeguarsi al GDPR
2. **Accountability di processo:** come viene dato luogo, in termini di obiettivi, attività, ruoli e responsabilità alla messa in atto dei principi e delle indicazioni del GDPR
3. **Accountability tecnica/organizzativa:** quali sono le misure di sicurezza messe in atto per adeguarsi al GDPR



- ❑ E' principale sottoprocesso del processo di *accountability*, rappresentato da tutte quelle analisi e valutazioni da effettuare al momento dell'emissione di un atto che comporti un trattamento di dati personali.
- ❑ Nel caso in cui qualsiasi atto prefiguri il trattamento di dati personali, devono essere valutati i seguenti aspetti:
  - a. **Individuazione del trattamento sotteso al processo** che si va a ipotizzare o realizzare, modificare, integrare
  - b. **I soggetti coinvolti e le differenti figure dell'organizzazione GDPR**
  - c. Le relative **misure di sicurezza**.

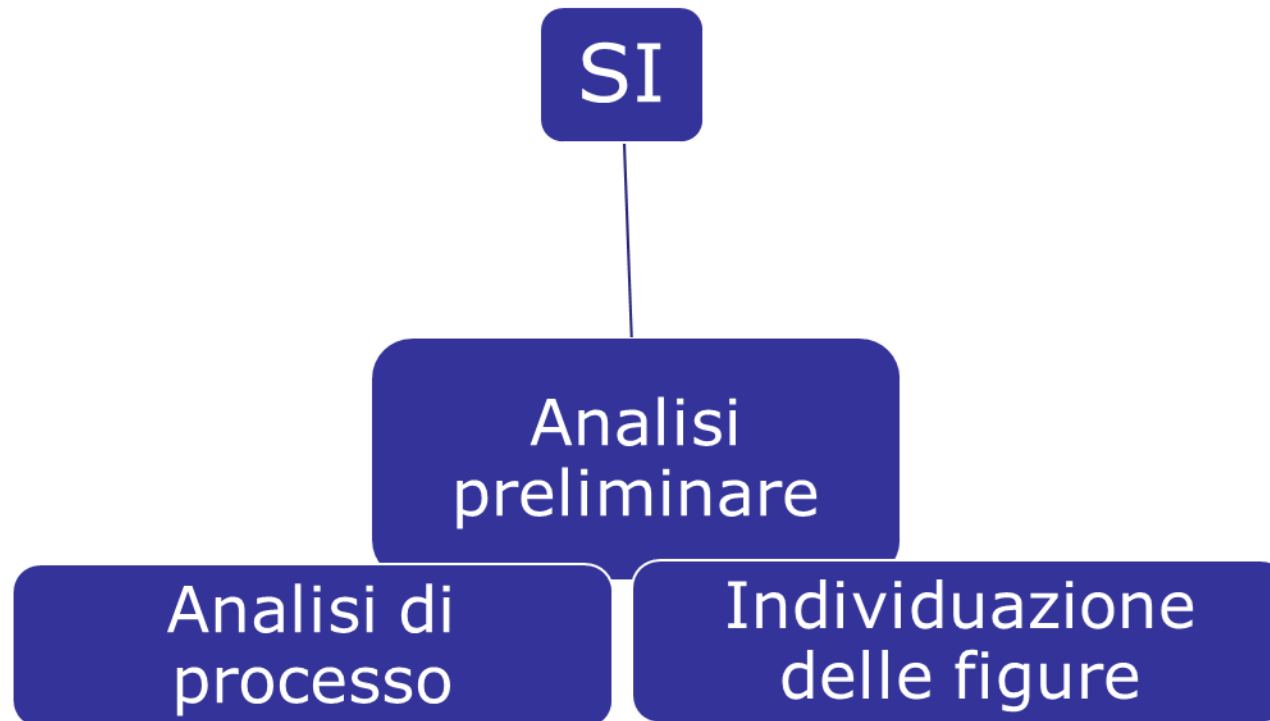
Tale processo deve essere vincolante nella produzione di un qualsivoglia atto.

Il processo è descritto nella DPP nel documento «*Linee guida per la Data Protection by design e by default*».

- Nel momento in cui si progetta un'iniziativa (delibere, decreti, bandi di gara o per l'erogazione di contributi, contratti, sviluppo di sistemi informativi...)



**Quello che sto progettando comporta il trattamento di dati personali?**





## □ **Analisi di processo**

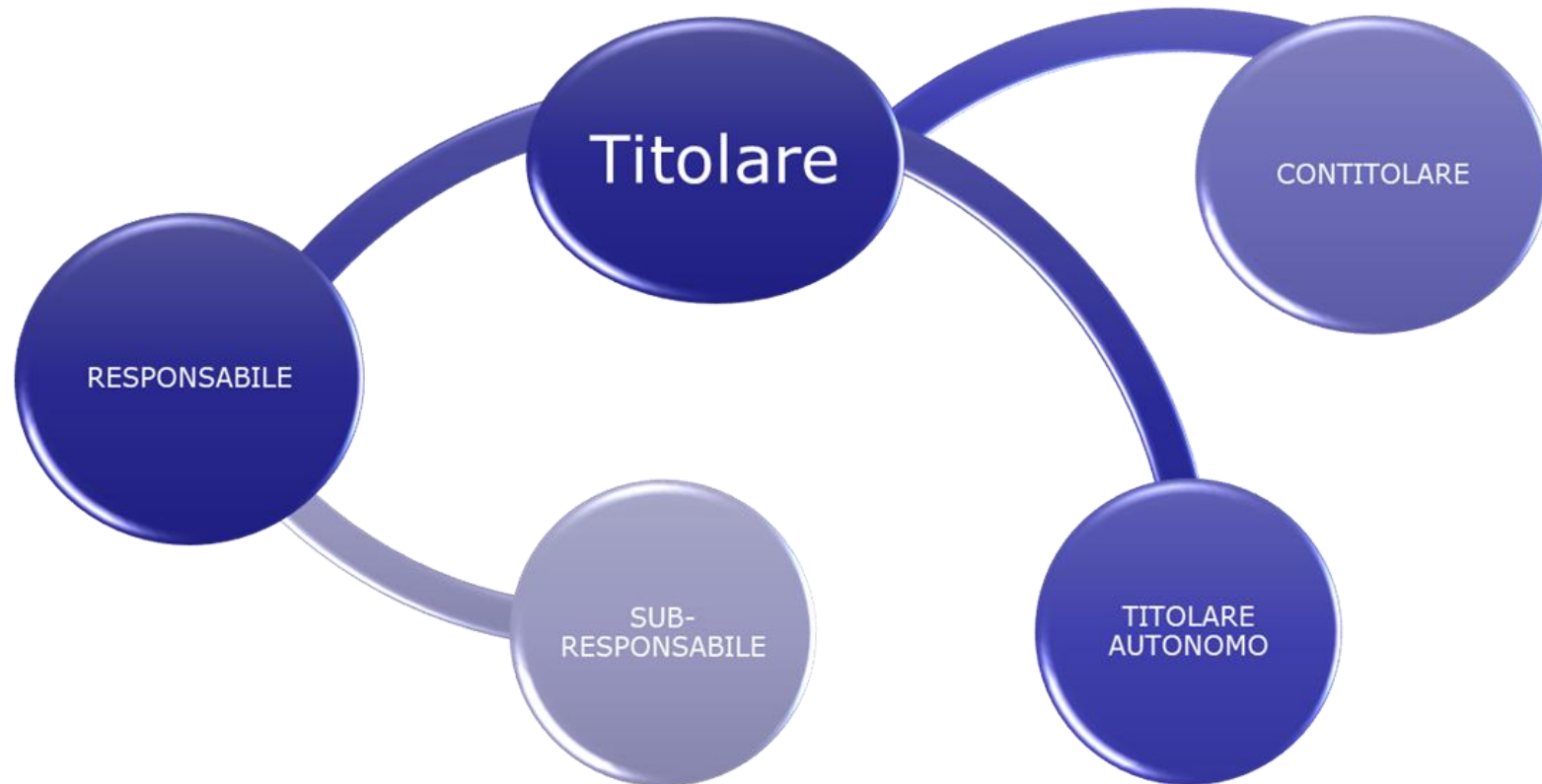
### **Rapporto trattamento / processo**

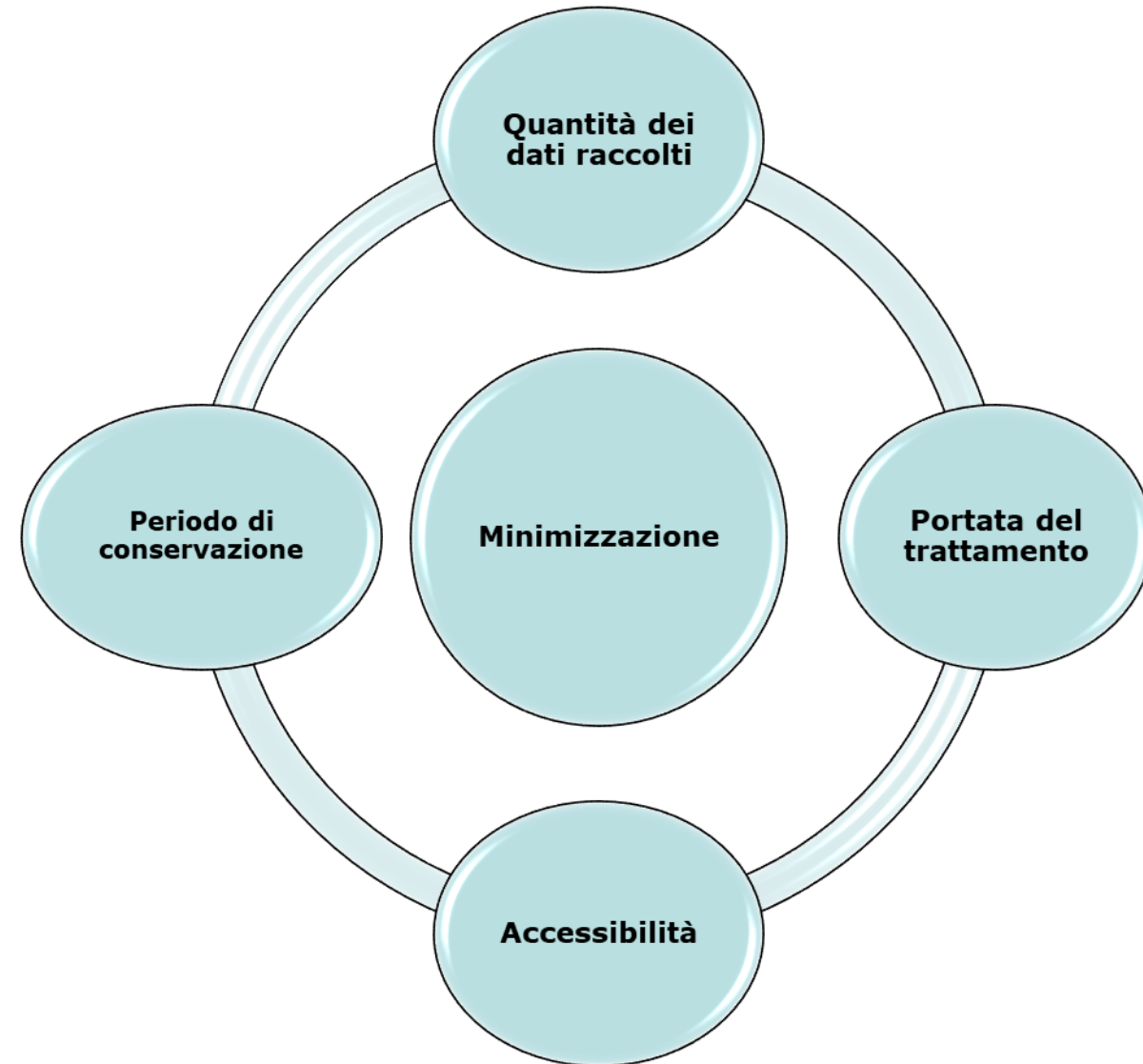
*Il trattamento è il segmento di un processo, attribuito da regole organizzative o dalle stesse norme alla competenza di uno specifico settore o direzione, in cui sono «coinvolti» dati personali.*

Il processo deve essere descritto in termini di:

- a) Obiettivo → Finalità (base giuridica del trattamento)
- b) Categoria dei soggetti interessati
- c) Ruoli *data protection*
- d) Attività svolte da ciascun soggetto
- e) Dati trattati

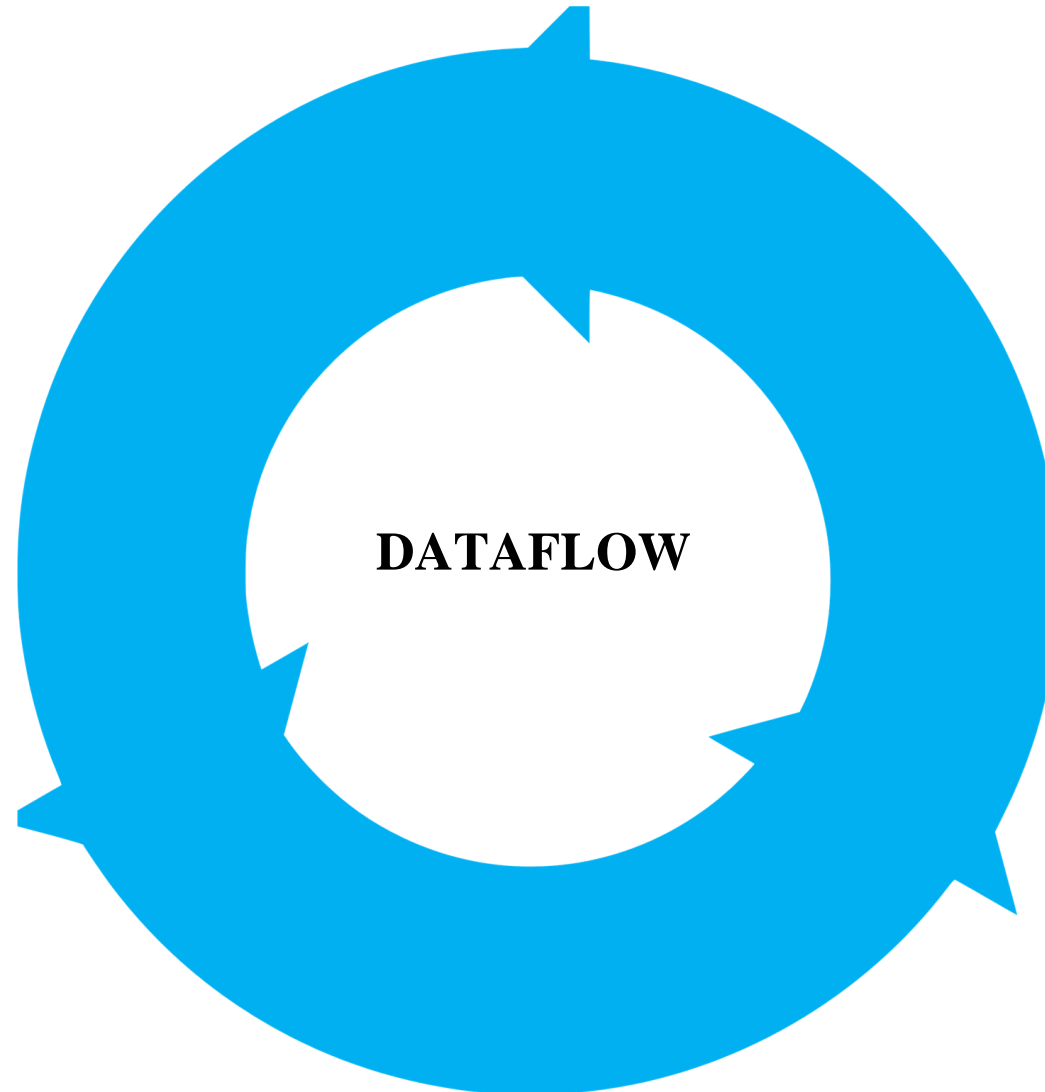
## □ Individuazione delle figure –infra-





**Tenere conto** del volume dei dati personali, delle tipologie, delle categorie e del livello di dettaglio dei dati personali richiesti per le finalità del trattamento.

- Valutazione sulla necessità di trattare i dati personali **per conseguire una determinata finalità** senza sottoporre a trattamento tutte le tipologie di dati personali.



### □ Art. 4, n. 2) GDPR

Alla definizione di «trattamento» sono riportate alcune operazioni. L'elenco, esemplificativo, è utile per ricostruire il *dataflow* di un trattamento.

«**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la **raccolta**, la registrazione, **l'organizzazione**, la strutturazione, la conservazione, l'adattamento o la modifica, **l'estrazione**, la consultazione, **l'uso**, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la **limitazione**, la cancellazione o la **distruzione**;

## Dataflow: definizione

### **Dataflow:**

Flusso dei dati, dalla raccolta alla gestione, fino all'archiviazione e cancellazione.

***In altre parole, il ciclo di vita del dato.***



❑ **Dataset**  Insieme di dati personali.

Il *dataset* può essere composto da:

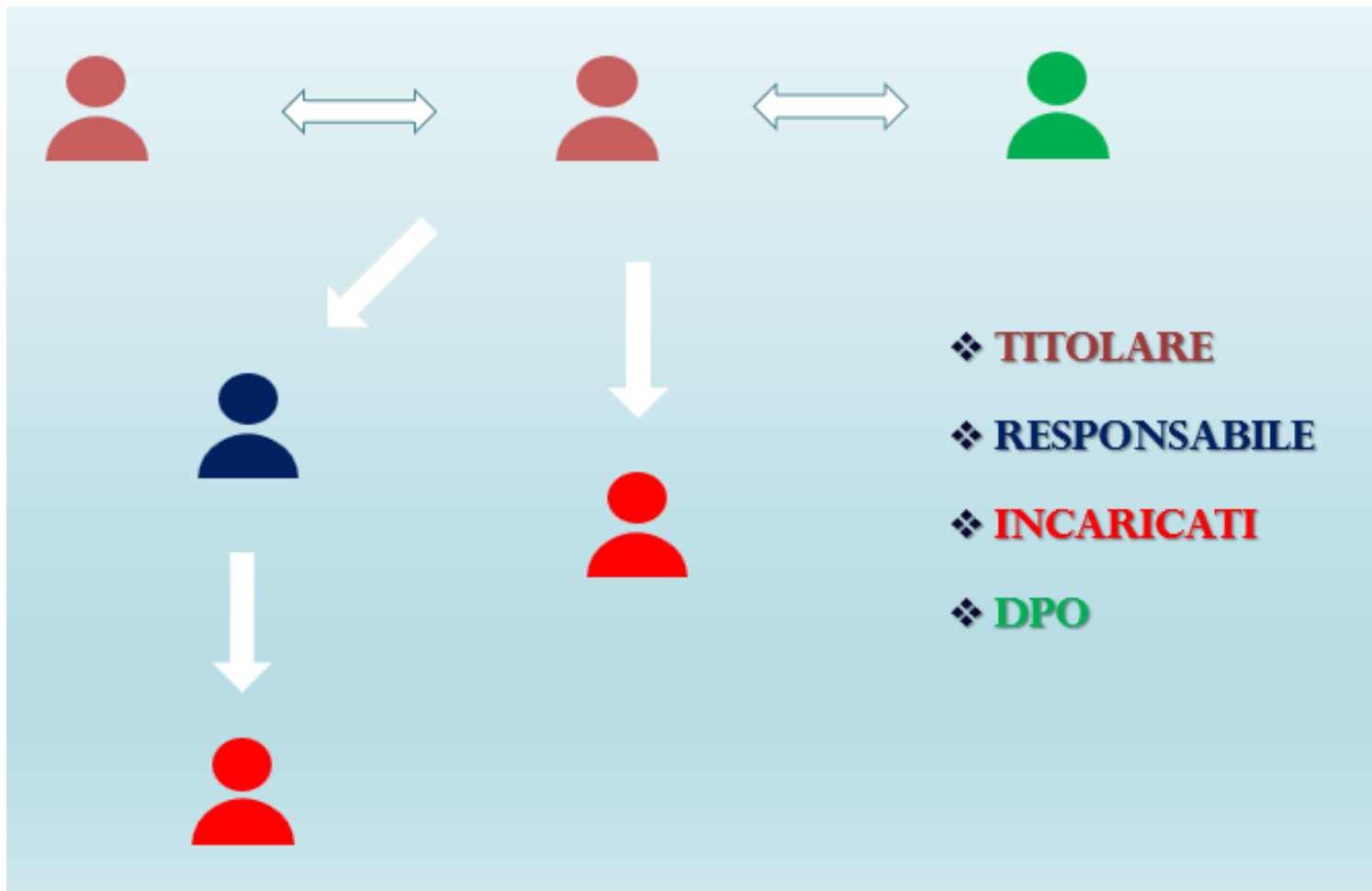
1. Elementi identificativi diretti (es. nome, cognome)
2. Elementi identificativi indiretti (frammenti di informazioni che possono essere usati da soli o in combinazione con altri elementi per re-identificare un individuo in un dataset – es. codice; data di nascita; età...)

❑ In diverse fasi del *dataflow*, il *dataset* può essere **distinto**.

Es. Raccolgo certe informazioni, ma ne comunico soltanto alcune a un altro soggetto; oppure, in una certa fase del trattamento, ne raccolgo e utilizzo ulteriori.

	A	B	C	D
1	First Name	Last Name	Date of birth	Age
2	Hank	McNeil	1-2-1993	25
3	Jessica	Williams	15-4-1956	62
4	Rick	Johnson	30-6-1966	52
5	John	Jenkins	17-4-1969	49
6	Joe	Vanderberg	4-11-1970	48
7	Mary	Dylan	12-12-1979	39
8	Leeroy	Johanson	12-7-1984	34

# L'individuazione dei ruoli data protection





# Linee guida EDPB 7/2020 sui concetti di titolare e responsabile del trattamento



## Titolare

- Stabilisce il motivo e le modalità del trattamento («mezzi essenziali»)
- Non è necessario che abbia accesso effettivo ai dati

## Contitolare

- Partecipa congiuntamente al Titolare nella definizione delle finalità e i mezzi di un'operazione di trattamento
- Il trattamento non sarebbe possibile senza la partecipazione del titolare e del/i contitolare/i: i trattamenti svolti da ciascuno sono indissolubilmente legati

## Responsabile

- E' un soggetto distinto rispetto al Titolare e tratta i dati per suo conto
- Deve limitarsi a trattare i dati in base alle istruzioni impartite dal Titolare

## Il titolare del trattamento. Key Words

- ❑ «**Autorità pubblica, servizio o altro organismo**»
- ❑ «**Determina**»: esercizio del potere decisionale su «Perché il trattamento ha luogo?» e «Chi ha deciso che il trattamento debba avvenire per una determinata finalità?»
- ❑ «**Singolarmente o insieme ad altri**» (contitolarità)
- ❑ «**Finalità e mezzi**»: decisione sul perché e sul come del trattamento.



## Il titolare del trattamento. Key Words

### Mezzi essenziali

- Sono determinati necessariamente dal titolare e strettamente legati alla finalità e portata del trattamento: **quali dati sono trattati? Per quanto tempo? Chi vi ha accesso? Quali sono le categorie di interessati?**

### Mezzi non essenziali

- Aspetti più pratici legati all'esecuzione del trattamento, quali la scelta di un particolare tipo di hardware o software e le misure di sicurezza specifiche in merito alle quali può altresì decidere il responsabile del trattamento. In ogni caso, il titolare deve comunque stabilire nel DPA l'istruzione di adottare le misure ex art. 32 GDPR e la garanzia da parte del responsabile di assistenza nell'adempimento degli obblighi di cui all'art. 32.

## Il titolare del trattamento. Key Words

### **Titolarità legale esplicita**

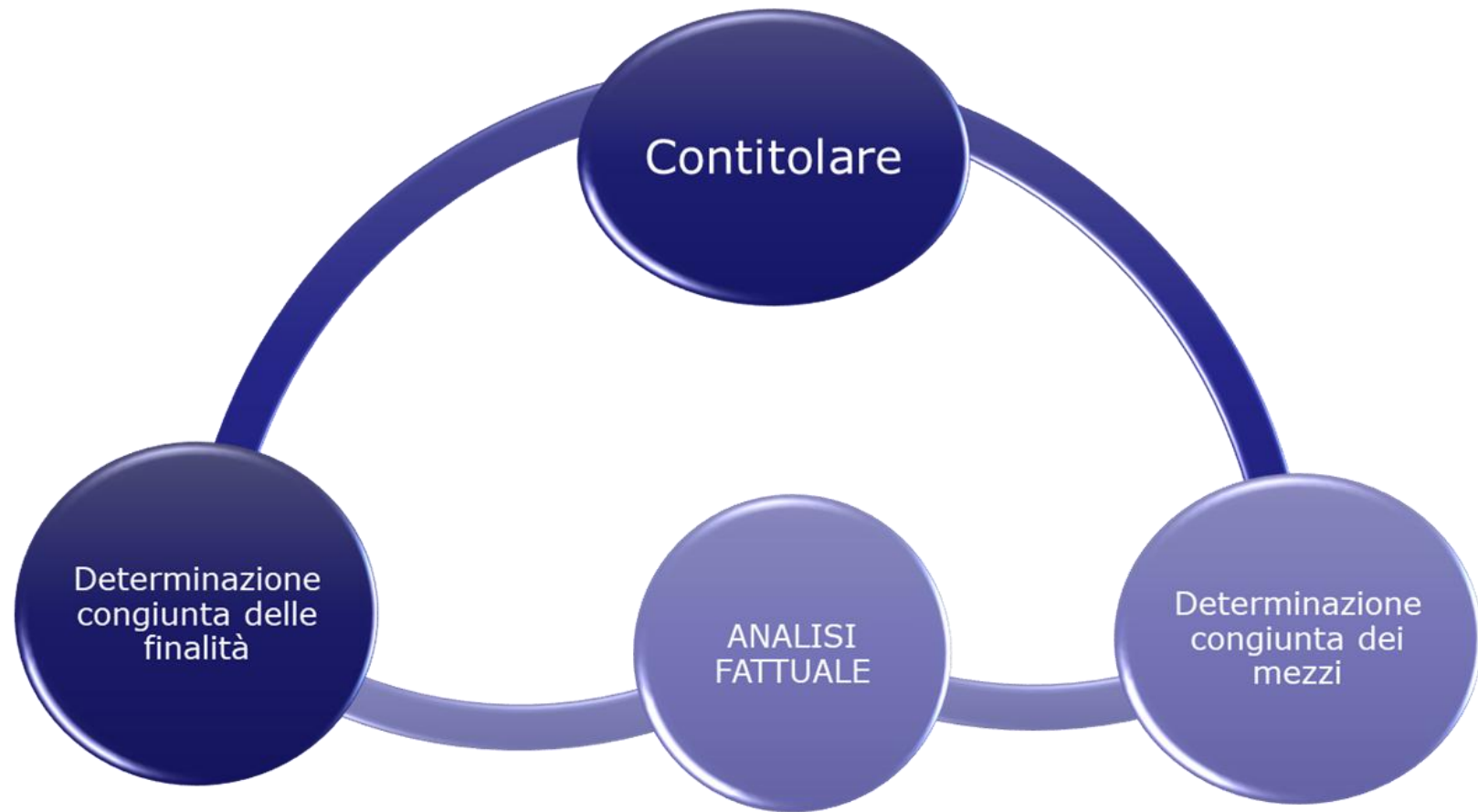
La titolarità del trattamento è definita specificamente dalla normativa

### **Titolarità legale implicita**

La normativa definisce un compito o impone l'obbligo di raccogliere e trattare determinati dati, e in linea di principio, il titolare del trattamento è il soggetto cui la legge demanda la realizzazione della funzione pubblica.



# Il contitolare del trattamento



## Situazioni in cui NON sussiste una contitolarità



- ❑ Scambio degli stessi dati o insiemi di dati tra due soggetti **in assenza** di finalità o mezzi di trattamento determinati congiuntamente
- ❑ Più soggetti utilizzino una banca dati condivisa o un'infrastruttura comune, qualora ciascuna di esse **determini autonomamente** le proprie finalità
- ❑ Vari soggetti trattano successivamente gli stessi dati personali in una catena di operazioni: ciascuno di essi ha una **finalità indipendente e impiega mezzi indipendenti** relativamente al segmento della catena di rispettiva competenza.

## Responsabile del trattamento

-L'EDPB rammenta che **non tutti i fornitori di servizi che trattano dati personali nel corso della prestazione sono responsabili del trattamento.**

❑ Il ruolo di responsabile scaturisce dalle **attività concrete in un contesto specifico**. Uno stesso soggetto **può agire contemporaneamente** come titolare per determinate operazioni di trattamento, e **come responsabile** per altre.

❑ La **natura del servizio** determinerà se l'attività di trattamento abbia per oggetto il trattamento di dati personali per conto del titolare.



**Resta necessaria un'analisi caso per caso**

## Responsabile del trattamento

-Un responsabile del trattamento può offrire un servizio secondo caratteristiche predeterminate, ma il titolare deve prendere la decisione finale di approvare attivamente le modalità di esecuzione del trattamento almeno per quanto concerne i **mezzi essenziali**.

Un responsabile del trattamento dispone infatti di un margine di manovra per quanto riguarda i mezzi non essenziali.

**Esempio: Fornitura di servizi IT.** Il fornitore ha proposto un servizio standardizzato. Il Titolare deve comunque assicurarsi che l'accordo in vigore sia conforme all'articolo 28, paragrafo 3, del GDPR, e che i dati personali di cui è titolare siano trattati esclusivamente per le proprie finalità. Deve inoltre assicurarsi che le sue istruzioni specifiche, concernenti per esempio i periodi di archiviazione, la cancellazione dei dati ecc. siano rispettate dal fornitore, indipendentemente da quanto previsto in via generale dal servizio standardizzato.



# Scelta del Responsabile del trattamento

Il Titolare è **responsabile** della valutazione dell'adeguatezza delle garanzie presentate dal responsabile e dovrebbe essere in grado di dimostrare di aver preso in seria considerazione tutti gli elementi di cui al GDPR.

➤ Spesso ciò richiederà uno scambio di documentazione pertinente (es. registro delle attività di trattamento, policy, certificazioni ISO..). Il Titolare dovrebbe tenere conto:

1. **delle conoscenze specialistiche** (ad esempio, le competenze tecniche in materia di misure di sicurezza e di violazione dei dati)
2. **dell'affidabilità**
3. **delle risorse e della reputazione del responsabile sul mercato.**

➤ A intervalli adeguati, dovrebbe **verificare** le garanzie offerte dal responsabile, anche mediante attività di audit, e ispezioni, se del caso.



# Data Protection Agreement

## **MODELLI di DPA regionali**

Con decreto n. 387 del 12 gennaio 2023 sono stati approvati i seguenti modelli di:

- dpa Titolare - Responsabile
- dpa tra Titolari autonomi
- dpa tra Contitolari

-accesso alle banche dati regionali da parte di altre pubbliche amministrazioni per finalità delle stesse.

**Clausole Contrattuali Titolare – Responsabile**

# Data Protection Agreement

Il DPA TT-RT costituisce la formulazione, aggiornata ai sensi del Reg. UE 2016/679, di un facsimile di accordo da stipulare fra **Titolare e Responsabile** nell'ambito di contratti o convenzioni. Tale regolazione del rapporto può essere inserita all'interno dell'articolato dei contratti o convenzioni o essere oggetto di un atto separato sottoscritto dalle parti. Nel caso si configuri un rapporto con un terzo soggetto in qualità di sub Responsabile, andranno inserite le relative parti. L'accordo può essere semplificato in considerazione della quantità, qualità e tipologia dei dati oggetto dei trattamenti che il Titolare demanda all'elaborazione da parte del Responsabile.

**Clausole Contrattuali Titolare – Responsabile**

# Data Protection Agreement

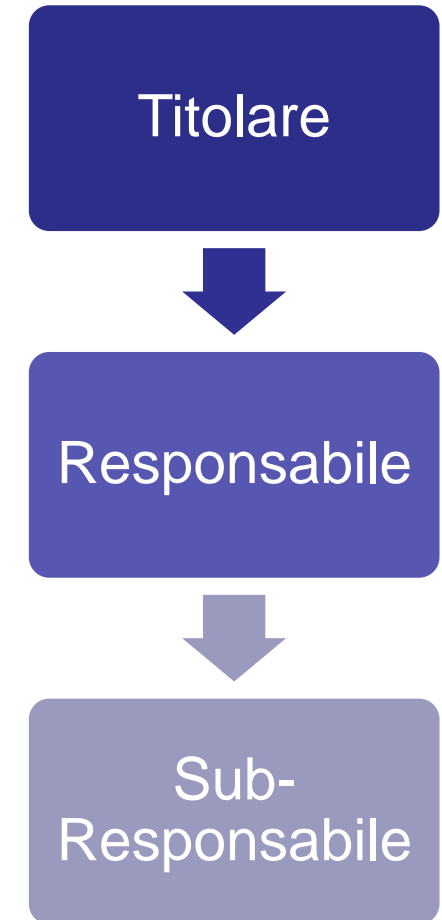
- Definizione di **obblighi vincolanti** per il responsabile e per il titolare nella forma di un contratto scritto, sottoscritto da entrambe le parti o integrato in un contratto più ampio, come un accordo sul livello dei servizi, contenente tutti gli elementi di cui all'art. 28, par. 3
- Un rapporto titolare-responsabile del trattamento potrebbe sussistere **anche in assenza** di un accordo di trattamento per iscritto e ciò implicherebbe una violazione dell'art. 28, par. 3, anche per il problema della mancata individuazione di una base giuridica su cui qualsivoglia trattamento dovrebbe basarsi (es. comunicazione dei dati tra titolare e presunto responsabile)

**Clausole Contrattuali Titolare – Responsabile**

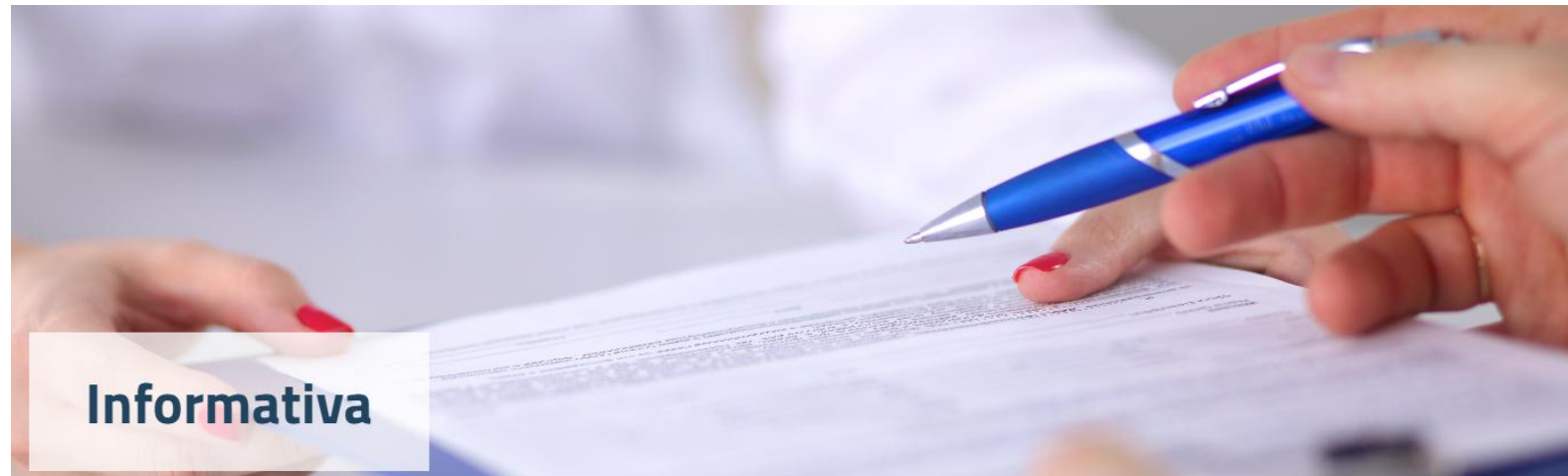
## Sub-responsabile del trattamento

Autorizzazione scritta, **specificata** (un determinato sub per una determinata attività e in un momento specifico) o **generale**, del titolare. In entrambi i casi, prima che qualsivoglia trattamento di dati personali sia affidato al sub-responsabile, il responsabile deve ottenere l'autorizzazione scritta del titolare dello stesso. La differenza principale è sul significato attribuito al **silenziio del titolare**: se generale, la mancata obiezione da parte del titolare entro un termine stabilito può essere considerato un **assenso**.

- ❑ Il responsabile conserva nei confronti del titolare **l'intera responsabilità** dell'adempimento degli obblighi dell'altro responsabile.
- ❑ Previsione **degli stessi obblighi** di cui all'art. 28, par. 3.



# L' informativa sul trattamento dei dati personali



# L' informativa sul trattamento dei dati personali. Art. 13 GDPR



1. In caso di raccolta **presso l'interessato** di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, **nel momento in cui i dati personali sono ottenuti**, le seguenti informazioni:

- a) **l'identità e i dati di contatto del titolare del trattamento** e, ove applicabile, del suo rappresentante;
- b) **i dati di contatto del responsabile della protezione dei dati**, ove applicabile;
- c) **le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento**;
- d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- e) **gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali**;
- f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili.



# L' informativa sul trattamento dei dati personali. Art. 13 GDPR



2. **In aggiunta** alle informazioni di cui al paragrafo 1, **nel momento in cui i dati personali sono ottenuti**, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

a) **il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;**

b) **l'esistenza del diritto dell'interessato** di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), **l'esistenza del diritto di revocare il consenso** in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

d) **il diritto di proporre reclamo a un'autorità di controllo;**

e) **se la comunicazione di dati personali è un obbligo legale** o contrattuale oppure un requisito necessario per la conclusione di un contratto, **e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;**

f) **l'esistenza di un processo decisionale automatizzato**, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.





# L' informativa sul trattamento dei dati personali. Legenda



- ☒ Forma chiara, concisa e intelligibile
- ☒ Finalità e base giuridica del trattamento
- ☒ Identità Titolare e dati di contatto; recapiti DPO
- ☒ Trasferimento dati paesi extra-UE
- ☒ Periodo di conservazione
- ☒ Diritti degli interessati, tra cui reclamo all'Autorità
- ☒ Categorie di destinatari
- ☒ Natura del conferimento dei dati e conseguenze della mancata comunicazione

## **Informativa e «*secondary use*» dei dati Art. 13, par. 3, GDPR**

Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.

## E quando i dati non sono stati ottenuti presso l'interessato? Art. 14, GDPR

In questo caso, l'informativa deve essere fornita all'interessato:

- 1) entro un termine ragionevole e comunque **non oltre un mese** dalla raccolta dei dati in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
- 2) se i dati personali sono destinati alla comunicazione con l'interessato, **al più tardi al momento della prima comunicazione** all'interessato;
- 3) nel caso in cui sia prevista la comunicazione ad altro destinatario, **non oltre la prima comunicazione** dei dati personali.

L'informativa deve contenere **tutti i requisiti di cui all'art. 13, e in aggiunta:**

- 1) l'indicazione delle categorie dei dati personali oggetto del trattamento;
- 2) l'indicazione della fonte da cui hanno origine i dati personali.

## E quando i dati non sono stati ottenuti presso l'interessato?

### Art. 14, par. 5, GDPR – **ECCEZIONI**

- a) l'interessato dispone già delle informazioni;
- b) informare l'interessato risulta impossibile o implicherebbe uno sforzo sproporzionato (es. trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni);
- c) la registrazione o la comunicazione sono espressamente previsti per legge; oppure
- d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge.

## Ordinanza ingiunzione nei confronti di Istituto per Ciechi Ardizzone Gioeni - 16 settembre 2021

### Reclamo di un interessato

- Informativa videosorveglianza carente di base giuridica del trattamento, dati di contatto del DPO, menzione del diritto degli interessati di proporre reclamo a un'autorità di controllo
- Informativa generale agli ospiti della struttura: consenso e legittimo interesse (per categorie particolari di dati) come basi giuridiche di un soggetto pubblico
- Informativa non trasparente, non intelligibile e non facilmente accessibile in ragione dello stato di vulnerabilità degli interessati

Sanzione: € 5.000



## Ordinanza ingiunzione nei confronti di Azienda Sanitaria Locale Frosinone - 13 gennaio 2022

### Conclusione:

**Illiceità del trattamento** di dati personali effettuato dalla ASL di Frosinone in violazione del principio di trasparenza (art. 5 par. 1 lett. a) del Regolamento) e del diritto degli interessati di ricevere, al momento della raccolta dei dati, tutte le informazioni di cui all'art. 13 del Regolamento in una forma concisa, chiara e intellegibile, ai sensi dell'art. 12 del Regolamento.

Sanzione: € 7.500





*“la 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 trasmessi, conservati o comunque trattati”*

Tipi di violazioni di dati personali:

- ❑ “violazione della **riservatezza**”, in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
- ❑ “violazione dell’**integrità**”, in caso di modifica non autorizzata o accidentale dei dati personali;
- ❑ “violazione della **disponibilità**”, in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.





## Linee guida 1/2021 EDPB

- Riflettono le esperienze comuni degli Stati Membri e delle autorità di controllo da quando è entrato in vigore il GDPR. Il suo scopo è quello di aiutare i titolari del trattamento a decidere come gestire le violazioni dei dati e quali fattori considerare durante la valutazione del rischio.
- **Importanza di riconoscere** un data breach
- La **documentazione interna** di una violazione è un obbligo indipendente dai rischi connessi alla violazione, e deve essere eseguita in ogni singolo caso.



# Linee guida 1/2021 EDPB. Il caso. Dati personali altamente confidenziali inviati per errore via posta elettronica



L'ufficio di collocamento di un'amministrazione pubblica ha inviato un messaggio di posta elettronica - relativo ai prossimi corsi di formazione - alle persone registrate nel suo sistema come persone in cerca di lavoro. Per errore, è stato inviato un documento contenente tutti i dati personali di queste persone in cerca di lavoro (nome, indirizzo e-mail, indirizzo postale, numero di previdenza sociale), allegato a questa e-mail. Il numero di persone interessate è di oltre 60000. Successivamente, l'ufficio ha contattato tutti i destinatari chiedendo loro di cancellare il messaggio precedente e di non utilizzare le informazioni in esso contenute.



## Comunicazione agli interessati

- ❑ Il Titolare o un suo Delegato, avvalendosi del supporto del CISO e del DPO, deve valutare la necessità di procedere anche alla comunicazione dell'incidente agli interessati. **Quando?**

*«Quando la violazione dei dati personali 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.»*

Ciò potrebbe avvenire quando non è stato possibile mettere in atto misure di sicurezza adeguate in grado di porre rimedio alla violazione e/o di attenuarne i possibili effetti negativi scongiurando il rischio elevato per i diritti e le libertà degli interessati.

- ❑ Comunicazione pubblica: sito Web, Media (stampa, tv..) o altre forme di comunicazione atte a garantire che tutti gli interessati possano essere raggiunti.



# La procedura di notifica al Garante

- ❑ **Chi?** Titolare o Delegato del Titolare del trattamento (Dirigente/Direttori)
- ❑ **Dove?** Procedura telematica sul sito del Garante Privacy a partire dal 1° luglio 2021. Collegamento alla pagina web e download del file pdf per prendere visione dei dati forniti durante la compilazione del modulo; sottoscrizione del file pdf con firma digitale; caricamento del file sulla pagina web indicata previo inserimento di un Identificativo e di un Codice Upload nell'email contenente le istruzioni.

- ❑ **Cosa?**

[https://servizi.gpdp.it/databreach/resource/1629905132000/DB\\_Istruzioni](https://servizi.gpdp.it/databreach/resource/1629905132000/DB_Istruzioni)



# Data Protection Impact Assessment



- ❑ **Cosa è?** Processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, e a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento.
- ❑ **Quando è obbligatoria?** Secondo l'art. 35, quando il trattamento «*può presentare un **rischio elevato** per i diritti e le libertà delle persone fisiche*»
- ❑ **Quali eccezioni?** Due. La DPIA non è necessaria:
  - se non ricade nell'elenco di trattamenti soggetti a DPIA redatto dall'Autorità
  - se l'Autorità si è già espressa su una valutazione d'impatto su quel tipo di trattamento.



## □ **DPIA: perchè?**

E' uno strumento rilevante in termini di *accountability*, come procedura che permette di valutare e dimostrare la conformità con le norme in materia di data protection.



- ❑ La **valutazione d'impatto sulla protezione dei dati** è richiesta in particolare nei casi seguenti:
  - a) una **valutazione sistematica e globale di aspetti personali** relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
  - b) **il trattamento, su larga scala, di categorie particolari** di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
  - c) **la sorveglianza sistematica su larga scala** di una zona accessibile al pubblico.



Casi espressamente indicati dal GDPR



# «Rischio elevato»: quando? I criteri del WP29



Criteri	Esempi
Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, l'ubicazione	Creazione di profili comportamentali basati sull'utilizzo del proprio sito Web o sulla navigazione sullo stesso
Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente sull'interessato	Utilizzo di algoritmi, senza l'intervento umano, ai fini della valutazione istruttoria dei requisiti di ammissibilità all'erogazione di contributi, o ai fini di assunzione
Monitoraggio sistematico	Sorveglianza sistematica su larga scala nel contesto di spazi pubblici o di una zona accessibile al pubblico (videosorveglianza)
Dati sensibili o dati aventi carattere altamente personale	Non solo dati ex art. 9 GDPR, ma anche documenti personali riservati (come messaggi di posta elettronica)
Trattamento di dati su larga scala	Uno dei criteri indicati dalla Data Protection Policy regionale ai fini dell'individuazione della presenza di un trattamento su larga scala è quello numerico, da 100.000 interessati. A ogni modo, il WP29 raccomanda di tenere conto di alcuni fattori, tra cui il numero di interessati.
Creazione di corrispondenze o combinazione di insiemi di dati	Trattamento di dati personali raccolti per una finalità secondo una modalità diversa e una finalità ulteriore e/o da titolari diversi, oltre le ragionevoli aspettative dell'interessato (Big Data)
Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative	Combinazione di impronta digitale e riconoscimento facciale per miglior controllo degli accessi fisici; Internet of Things
Un trattamento che in sé impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto	Screening dei clienti di una banca attraverso i dati registrati in una centrale rischi al fine di stabilire se ammetterli o meno a un finanziamento.

# Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati del Garante Privacy nazionale



1. Trattamenti valutativi o di *scoring* su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad *“aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato”*.
2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono *“effetti giuridici”* oppure che incidono *“in modo analogo significativamente”* sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. *screening* dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).
3. Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi *web*, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di *budget*, di *upgrade* tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.

# Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati del Garante Privacy nazionale



4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).
5. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).
6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
7. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi *wearable*; tracciamenti di prossimità come ad es. il *wi-fi tracking*) ogniqualevolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 .
8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.
9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. *mobile payment*).

# Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati del Garante Privacy nazionale



**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**

10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

- L'attivazione di un nuovo trattamento o una sua modifica comporta l'avvio del processo «*Data Protection by Design*», nell'ambito del quale è prevista la decisione riguardante l'opportunità/obbligatorietà di effettuare una DPIA.
- La decisione deve essere presa dal Titolare in considerazione degli obblighi di legge e dell'opportunità di effettuarla in base alla delicatezza dei dati trattati.



- ❑ La formulazione della DPIA è competenza del dirigente/della direzione che emette l'atto o che pone in essere la progettualità.
- ❑ I DPS, con il supporto del DPO o di assistenza esterna (contratti di servizio, ecc.. ), hanno il compito di coadiuvare il delegato del Titolare nell'esecuzione della DPIA.
- ❑ Il DPO può, se richiesto dal delegato del Titolare, formulare il proprio parere sulla DPIA.



# Il software «PIA»: esempio di metodologia



- ❑ A livello regionale lo strumento attualmente adottato per l'effettuazione di DPIA è il software «PIA» messo a punto dall'Authority francese (CNIL).
- ❑ Il primo step previsto dal software è specificare il trattamento oggetto di DPIA e i soggetti responsabili della conduzione:
  - Titolo della DPIA
    1. Autore
    2. Revisore
    3. Validatore
    4. Data
    5. Stato

Versione 1.6.3

**pia** | Valutazione d'impatto sulla protezione dei dati

PANNELLO DI CONTROLLO

Lista Ordina

PIA

Nome della PIA

Autore  
Cognome, nome

Revisore  
Cognome, nome

Validatore  
Cognome, nome

05/11/2018

Stato  
Inizializzazione

0%

Avvia



## La consultazione preventiva

- ❑ Qualora persista un rischio residuo elevato, pur in presenza delle misure di sicurezza adottate, è necessario ricorrere al Garante.
- ❑ Il Titolare del trattamento:
  1. contatta il Garante richiedendo la consultazione preventiva
  2. invia tutte le informazioni relative al procedimento di consultazione
  3. riceve il parere dell'Autorità e condivide l'esito con il DPO che supporta il Titolare in ordine alle decisioni conseguenti all'esito.
- In casi di particolare rilevanza, come **trattamenti di dati personali con possibile impatto sulla protezione sociale e sulla sanità pubblica** può comunque essere prevista la necessità di una consultazione preventiva con il Garante.



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI