Aspetti di privacy e GDPR

6 novembre 2018

Simona Stoklin – Massimiliano Zanchiello

Dipartimento Trasformazione Digitale

GDPR

- **Il 25 maggio 2018** è divenuto applicabile il GDPR (Regolamento generale sulla Protezione dei Dati n. 2016/679)

- No necessità di norme di recepimento

- Nuovi adempimenti -> intensa attività di adeguamento

GDPR – principali novità

- **Accountability** (Art. 5): i titolari devono assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali

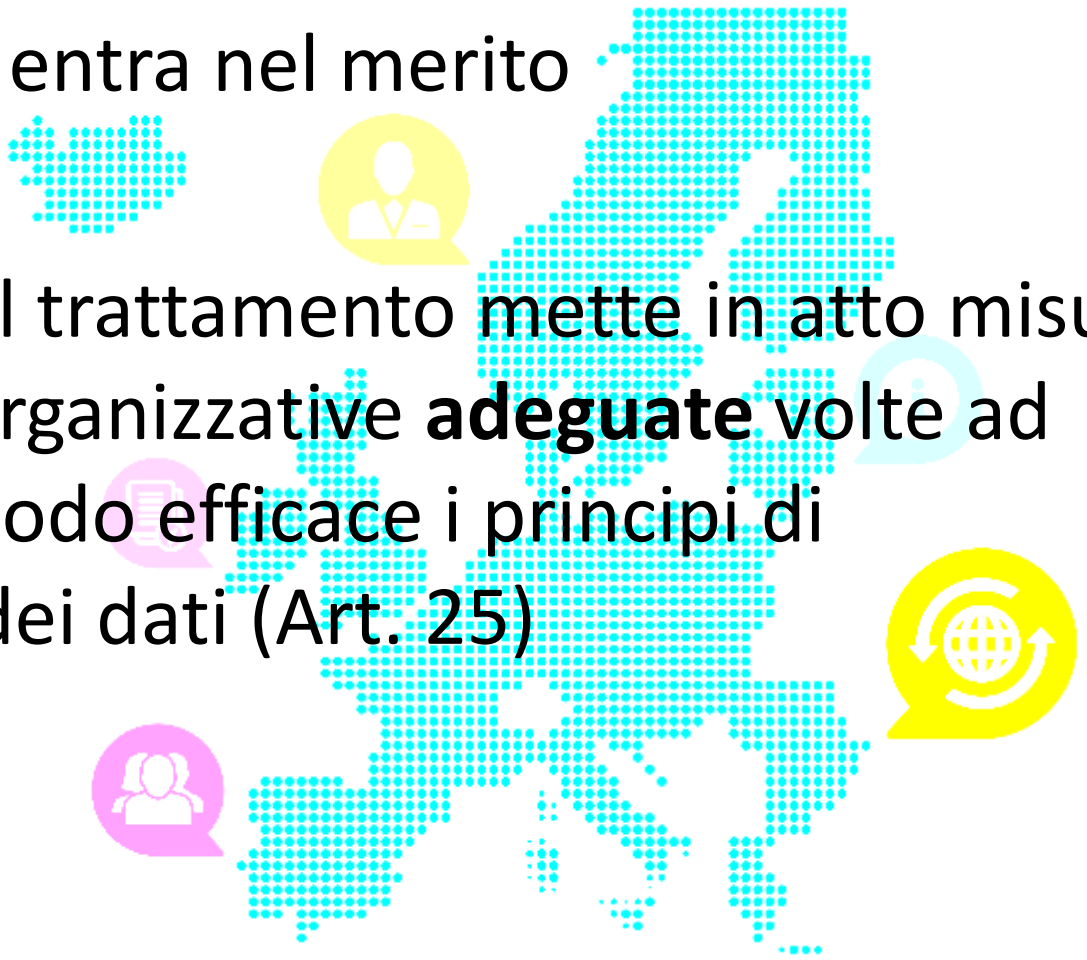
- **Figura del DPO**

- **Data Breach**

GDPR - Quali misure minime?

- Il GDPR non entra nel merito

- Il titolare del trattamento mette in atto misure tecniche e organizzative **adeguate** volte ad attuare in modo efficace i principi di protezione dei dati (Art. 25)



Da dove cominciare?

Il Garante per la protezione dei dati personali suggeriva alle PA di avviare, con assoluta priorità:

1. **Designazione del Responsabile della protezione dei dati – RPD (artt. 37-39)**
2. **Istituzione del Registro delle attività di trattamento (art. 30 e cons. 171)**
3. **Notifica delle violazioni dei dati personali (cd. data breach, art. 33 e 34)**

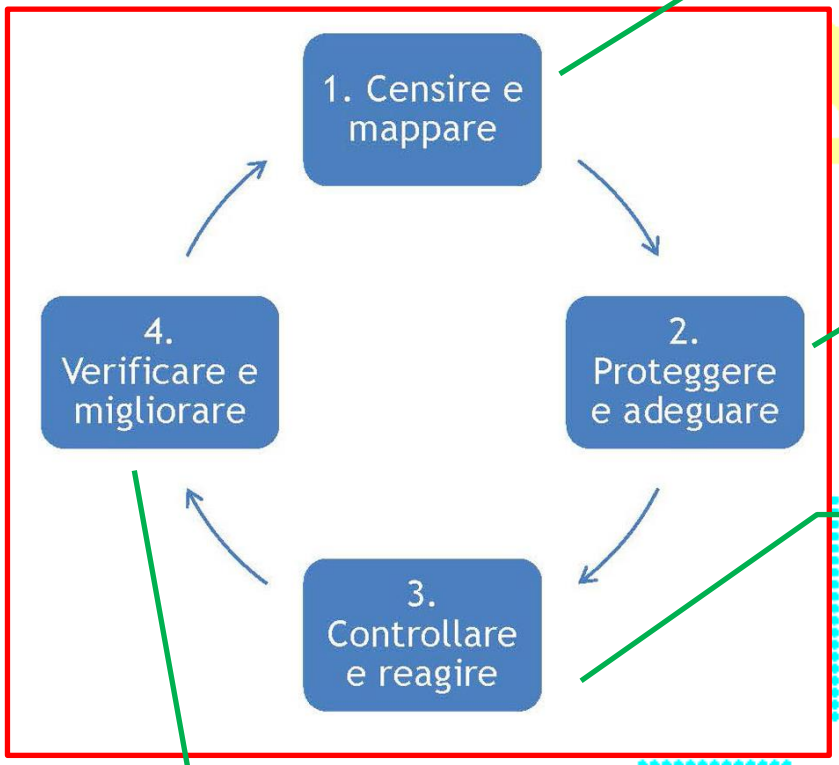
Importante per adeguamento al GDPR

- Committment dall'alto
- Collaborazione di tutti gli uffici del Dipartimento che trattano dati sensibili (es. ufficio personale, segreterie, ecc.)

Attività da fare

- Rivedere policy e procedure
- Rivedere i contratti di fornitura e fare le **nomine ai responsabili esterni dei trattamenti**
- Rivedere le **informative** agli interessati
- Modificare le applicazioni e le procedure per: rispettare i criteri di minimizzazione e conservazione limitata nel tempo, i diritti dell'interessato (accesso, oblio, portabilità)
- Ristrutturare la gestione del consenso (raccolta e uso appropriato dello stesso)
- **Creare i registri delle attività di trattamento**
- Preparare le procedure per la **notifica delle violazioni dei dati personali** al Garante e agli interessati
- Adottare misure di sicurezza aggiuntive rispetto alla situazione precedente al GDPR

Flusso GDPR



Realizzazione dei documenti:
- Asset Inventory
- Registro dei Trattamenti

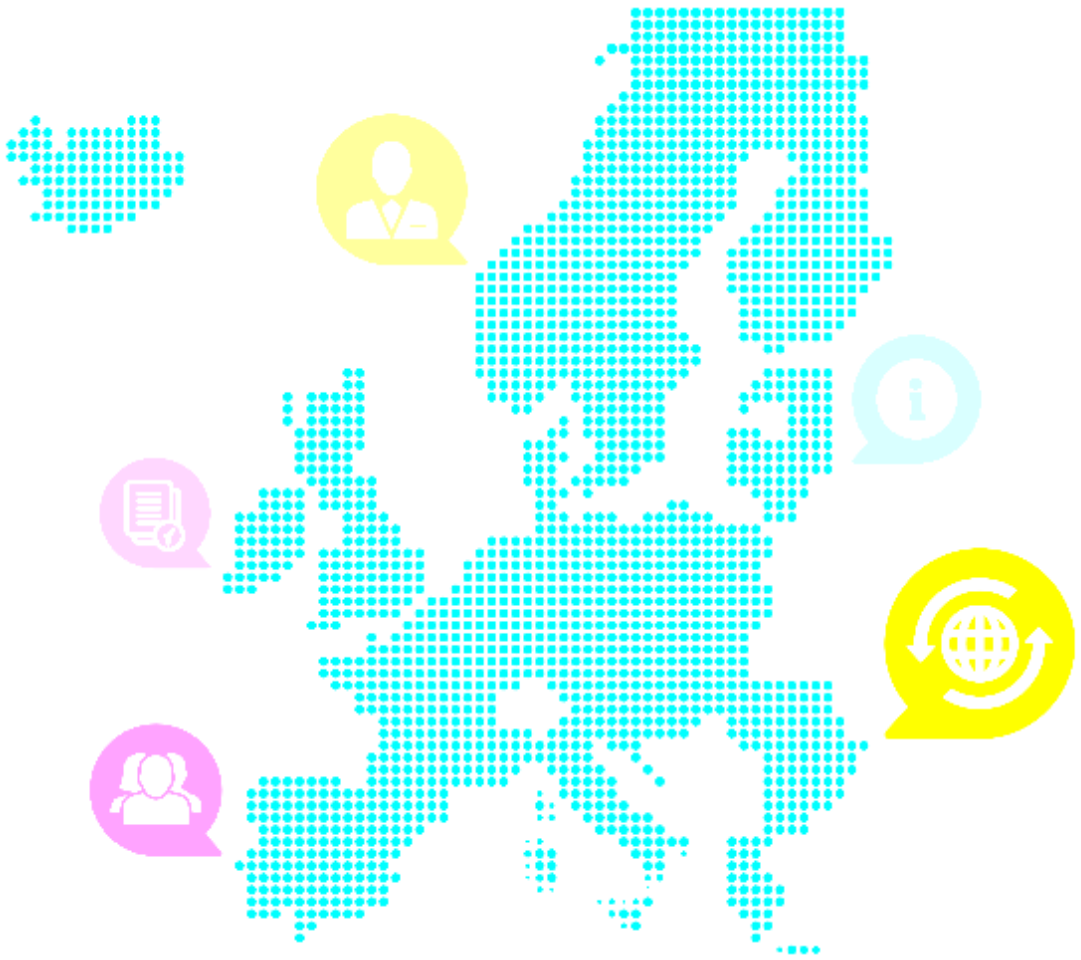
Nomina delle figure:
- Responsabili Esterni
- Amministratori di Sistema
- Incaricati

- Organizzare l'eventuale risposta al Data Breach

- Realizzazione del Registro delle Violazioni

Le parti in gioco

- **Interessato**
- **Titolare**
- **Responsabile**
- **Addetto**



Interessato

- Persona fisica al quale si riferiscono i dati personali. Quindi, se un trattamento riguarda, ad esempio, l'indirizzo, il codice fiscale, ecc. di Mario Rossi, questa persona è l'"interessato" (articolo 4)

Titolare

- Persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico o privato, l'associazione, ecc., che adotta le decisioni sugli scopi e sulle modalità del trattamento (articolo 4)

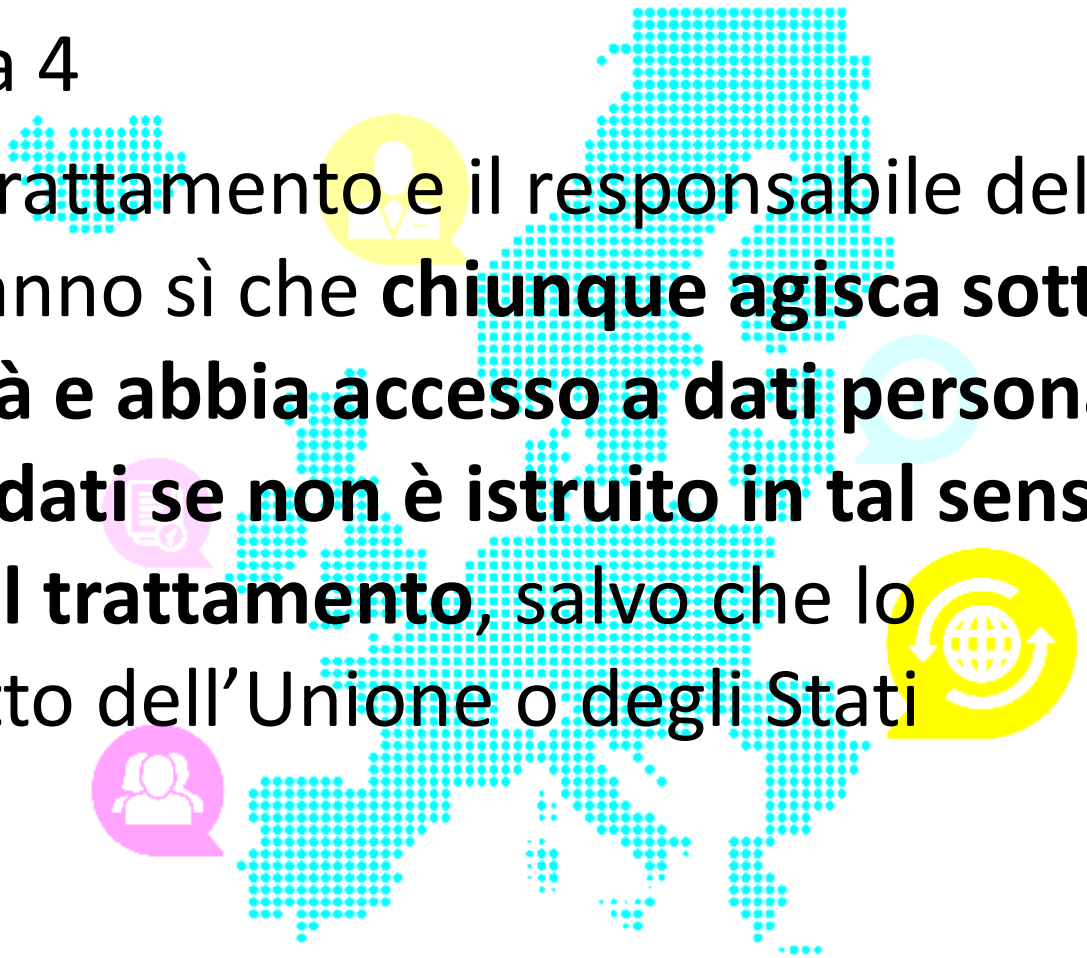
Responsabile

- Persona fisica o giuridica al quale il titolare affida, anche all'esterno della sua struttura organizzativa, specifici e definiti compiti di gestione e controllo per suo conto del trattamento dei dati (articolo 4).
- Il Regolamento ha introdotto la possibilità che un responsabile possa, a sua volta e secondo determinate condizioni, designare un altro soggetto c.d. *"sub-responsabile"* (articolo 28).

Addetto

Art. 32 comma 4

Il titolare del trattamento e il responsabile del trattamento fanno sì che **chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento**, salvo che lo richieda il diritto dell'Unione o degli Stati membri.



Trattamenti

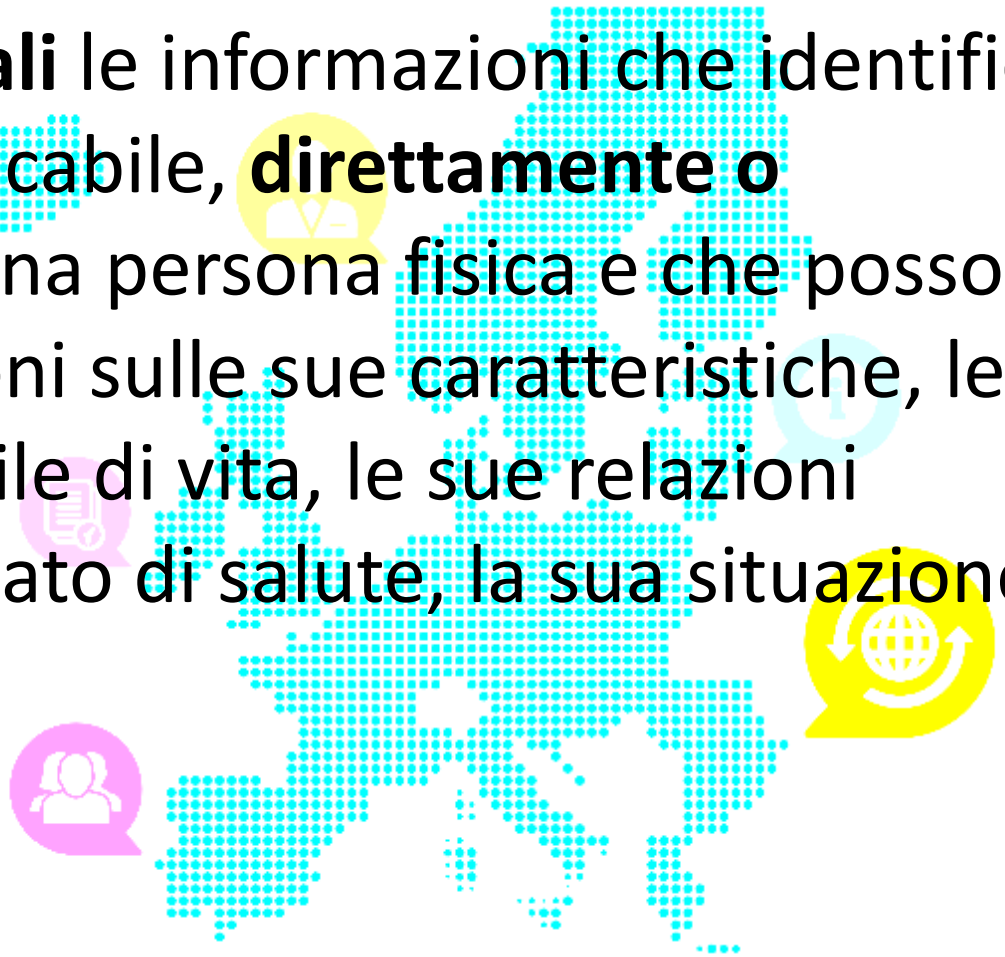
Art. 4 GDPR comma 2

Definizione di «**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;

Dati personali

Sono **dati personali** le informazioni che identificano o rendono identificabile, **direttamente o indirettamente**, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc..



Dati personali 1/3

Dati che permettono l'identificazione diretta - come i dati anagrafici (nome e cognome), le immagini, ecc. - e i **dati che permettono l'identificazione indiretta**, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa);

Dati personali 2/3

Dati rientranti in particolari categorie: si tratta dei dati c.d. *"sensibili"*, cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il GDPR (articolo 9) ha incluso nella nozione anche i **dati genetici, i dati biometrici** e quelli relativi all'**orientamento sessuale**;

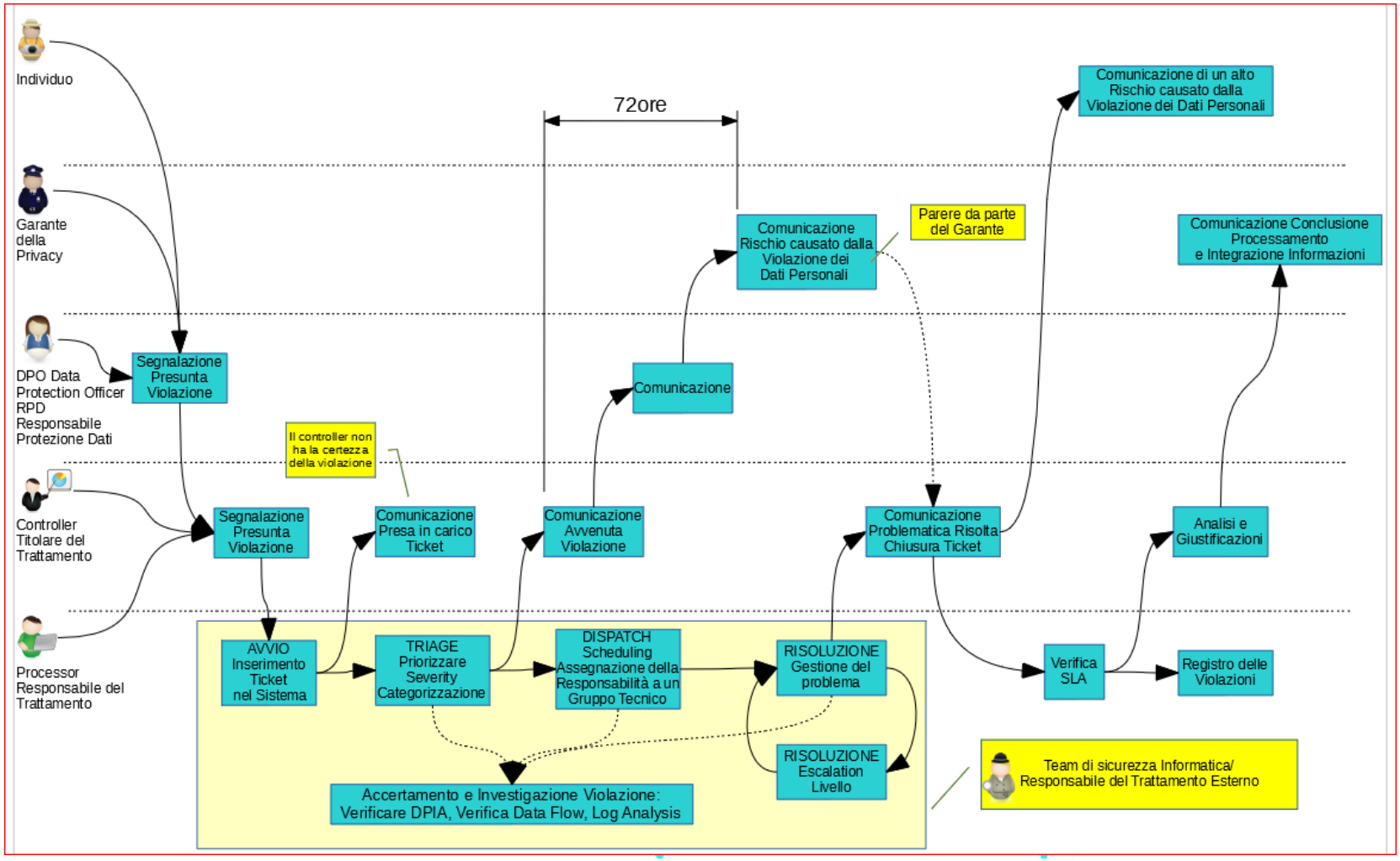
Dati personali 3/3

i **dati relativi a condanne penali e reati**: si tratta dei dati c.d. *"giudiziari"*, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad es. i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il GDPR (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Data breach

- Processo centralizzato per Roma Capitale?
- E' una tematica molto importante che rientra nelle attività prioritarie indicate dal Garante; nella definizione del processo di data breach vi sono impatti organizzativi che necessitano di autorizzazione da parte delle direzioni per la creazione di un gruppo di lavoro ad hoc opportunamente formato

Risposta al Data Breach



Risposta adeguata
alla normativa GDPR

- Monitoraggio attento e continuo delle attività;
- Predisporre le modalità e formati delle comunicazioni;
- Assegnare le responsabilità