Il Regolamento Generale sulla Protezione dei Dati personali

Gli elementi cardine della nuova disciplina

Workshop CCR INFN – Milano, 13 novembre 2017

Eleonora Bovo

Di cosa parliamo

Regolamento UE 2016/679 del Parlamento e del Consiglio relativo alla protezione delle persone fisiche con riguardo alla libera circolazione dei dati e che **abroga la direttiva 95/46/CE**

Pubblicato sulla G. U. Unione europea **il 4.5.2016**

Entrato in vigore il 24.5.2016

Si applica dal 25.5.2018

La nostra indagine

- **L'oggetto** della nuova disciplina
- **I soggetti** impegnati nel trattamento dati
- **Le attività** richieste per essere privacy-compliant
  - Il registro delle attività di trattamento
  - Privacy by design e by default
  - La Valutazione d'Impatto sulla Protezione dei Dati (DPIA)
  - Le misure tecniche ed organizzative per la sicurezza dei trattamenti
  - Il data breach

L'Oggetto

- Dati personali
- Categorie particolari di dati personali
- Dati relativi a condanne penali

Dati personali

Informazioni riguardanti una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata o identificabile mediante riferimenti come un nome, un numero di identificazione, un identificativo on line, uno o più elementi della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Categorie particolari di dati personali

- Informazioni che rivelino
  - **l'origine razziale o etnica**
  - **le opinioni politiche**
  - **le convinzioni religiose o filosofiche**
  - **l'appartenenza sindacale**
  - **dati genetici, biometrici, relativi alla salute o alla vita sessuale o all'orientamento sessuale**

- Dati relativi a
  - **condanne penali e reati**

Un nuovo approccio alla tutela dei dati personali

Il principio di Responsabilizzazione

Accountability

- Adozione di **comportamenti diretti a prevenire situazioni di rischio.**
- Dimostrazione della **concreta applicazione del Regolamento**

Gli ulteriori principi da osservare nel trattamento dei dati personali

- ✓ **Liceità, correttezza, trasparenza**
- ✓ **Limitazione della finalità:** i dati possono essere raccolti solo per finalità determinate, esplicite e legittime
- ✓ **Minimizzazione dei dati**: i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati

Gli ulteriori principi da osservare nel trattamento dei dati personali

- ✓ **Esattezza:** i dati devono essere esatti e se necessario aggiornati e devono essere adottate misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti
- ✓ **Limitazione della conservazione:** i dati devono essere conservati in una forma che consenta l'identificazione degli interessati solo per il periodo necessario a raggiungere le finalità per le quali sono trattati
- ✓ **Integrità e riservatezza**: i dati devono essere trattati in modo da garantirne un'adeguata sicurezza, compresa la protezione da trattamenti non autorizzati o illeciti o dalla perdita, distruzione o danno accidentali.

Attenzione al rispetto dei principi!

Il Legislatore europeo stabilisce per la violazione dei principi sanzioni pecuniarie di ammontare pari al doppio di quelle stabilite per la violazione delle norme che contengono obblighi.

I soggetti


Responsabile della protezione dei dati
Titolare del Trattamento
Soggetti autorizzati al trattamento
Responsabile del Trattamento

Il Titolare del Trattamento

Chi è

- Persona fisica o giuridica o **Autorità pubblica** che, **determina le finalità e i mezzi del trattamento dei dati personali**

Che cosa fa

- Tenuto conto della natura dei dati, dell'ambito di applicazione del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone, **pone in essere misure tecniche ed organizzative adeguate per garantire,** ed essere in grado di dimostrare, **che il trattamento è effettuato conformemente al Regolamento**

Il Responsabile del Trattamento

Chi è

- La persona fisica o giuridica o l'Autorità pubblica che tratta dati personali **per conto** del Titolare del trattamento.
- Soggetto esterno all'organizzazione del Titolare a cui quest'ultimo affida attività che comportano il trattamento di dati personali
- I trattamenti da parte di un Responsabile sono disciplinati mediante un contratto.

Che cosa fa

- Tratta i dati su istruzione documentata dal Titolare
- Garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza
- Adotta le misure di sicurezza nel proprio ambito operativo
- Ricorre ad un altro Responsabile solo su autorizzazione scritta del Titolare
- Assiste il Titolare per dar seguito alle richieste degli interessati per l'esercizio dei loro diritti

I soggetti autorizzati al trattamento

Chi sono

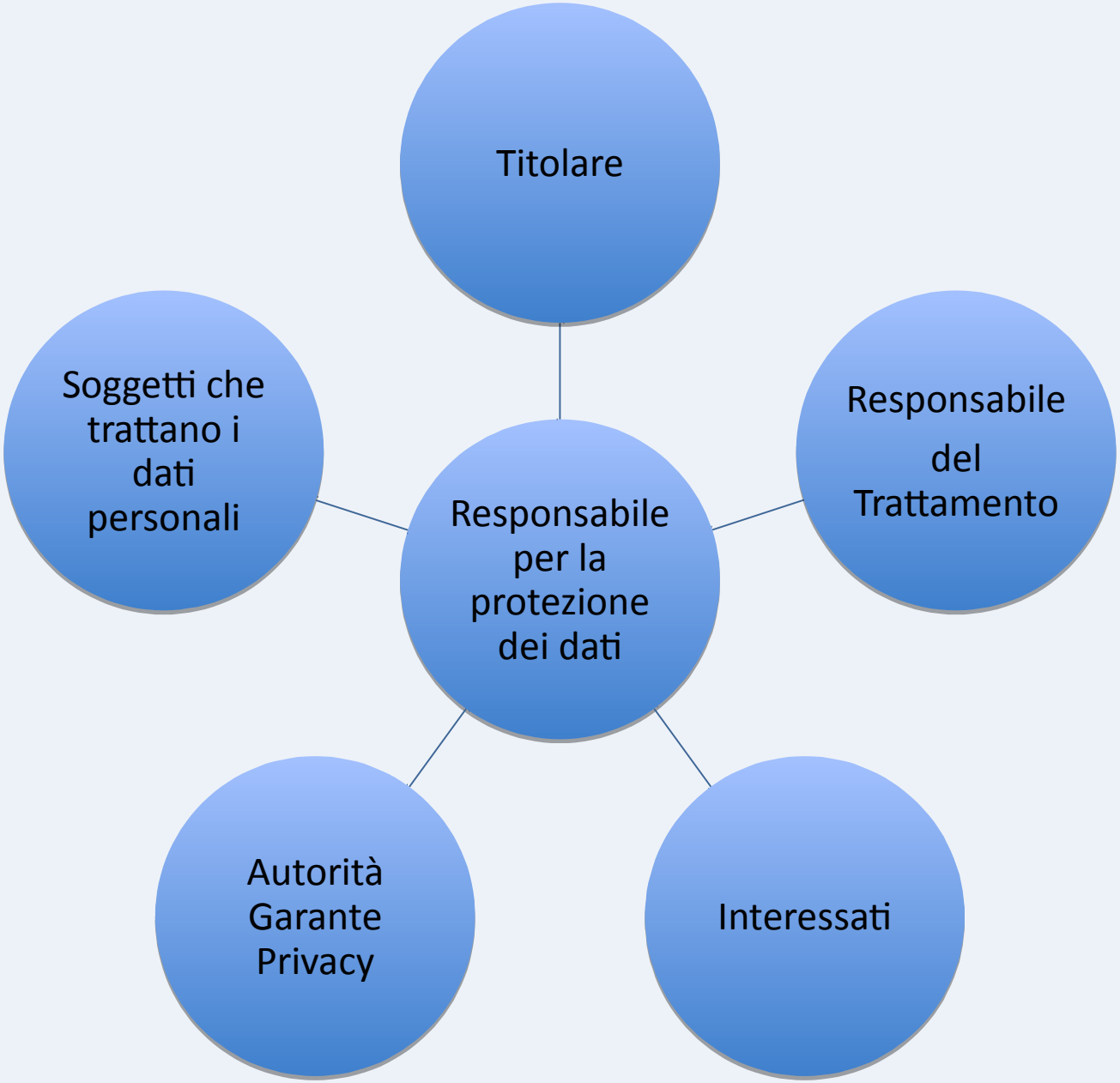
- coloro che operativamente trattano i dati personali secondo le istruzioni del Titolare (il Codice Privacy li definisce “Incaricati” del trattamento)

Che cosa fanno

- Raccolgono i dati o comunque li trattano in ragione della finalità che caratterizza il loro lavoro (gestione del personale, gestione gare, sorveglianza sanitaria, gestione del contenzioso ecc. ...)

Una nuova figura: il Responsabile della Protezione dei Dati (R.P.D. o D.P.O.)

- È chiamato a facilitare l'osservanza delle disposizioni del Regolamento
- Funge da interfaccia tra i soggetti coinvolti nelle attività di trattamento dati


Titolare
Soggetti che trattano i dati personali
Responsabile del Trattamento
Responsabile per la protezione dei dati
Autorità Garante Privacy
Interessati

Compiti del Responsabile per la Protezione dei dati

- ✓ Informare e fornire consulenza al Titolare del Trattamento ed ai dipendenti circa gli obblighi che derivano dal Regolamento
- ✓ Sorvegliare l'osservanza del Regolamento e delle politiche del Titolare in materia di protezione dati
- ✓ Fornire pareri in merito alla Valutazione di Impatto sulla Protezione dei dati
- ✓ Cooperare con il Garante per il quale costituisce punto di contatto presso il Titolare

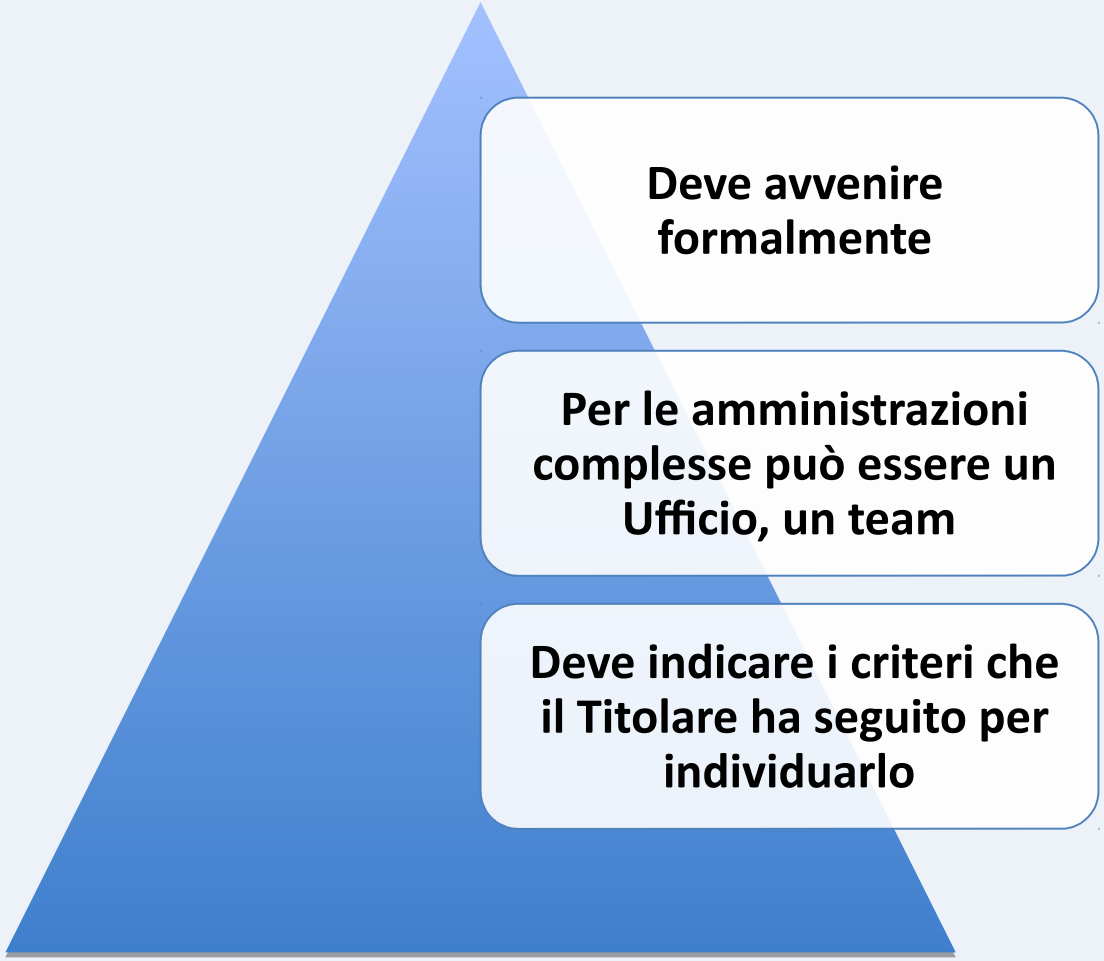
Requisiti del Responsabile della Protezione dei Dati

- Conoscenze specialistiche (normativa e prassi in materia di protezione dati)
- Capacità di assolvere ai propri compiti (quindi anche familiarità con competenze tecnologiche)

Garanzie di autonomia e indipendenza del Responsabile Protezione Dati

- Non può ricevere istruzioni per lo svolgimento dei compiti
- Non possono essere previste penalizzazioni o rimozioni a causa delle funzioni svolte
- Non può svolgere compiti o funzioni in conflitto di interessi

La designazione del Responsabile per la Protezione Dati



Le attività richieste dal Regolamento

Il Registro delle attività di Trattamento

- È un obbligo per il Titolare del trattamento
- Costituisce il documento di base sul quale costruire l'intero assetto tecnico-organizzativo per la protezione dei dati personali

Il Registro delle attività di Trattamento

Deve consentire:

- La dimostrazione della conformità del trattamento al Regolamento europeo
- La cooperazione con il Garante Privacy
- Il monitoraggio da parte del Garante Privacy

Il Registro delle attività di Trattamento

Il Contenuto:

- ✓ **I dati di contatto del Titolare e del Responsabile della Protezione dati**
- ✓ **Le finalità del trattamento: è bene indicare la base giuridica del trattamento in relazione al fatto che come PA trattiamo dati senza il consenso degli interessati**
- ✓ **Le categorie dei dati e degli interessati**

Il Registro delle attività di Trattamento

Il Contenuto:

- ✓ **Soggetti o categorie di destinatari ed eventuali trasferimenti di dati**
- ✓ **Termini di cancellazione dei dati e misure di sicurezza adottate**
- ✓ **Eventuali informazioni ulteriori (luogo in cui risiedono i dati, eventuali certificazioni acquisite, DPIA …)**

Il Registro delle attività di Trattamento

Tenuta e gestione

- **Forma scritta, (anche in formato elettronico)**
- **Istituzione entro il 25 maggio 2018**
- **Aggiornamento al variare di uno degli elementi che ne costituiscono il contenuto**

Uno schema per il Registro delle attività di trattamento

Finalità (base giuridica)	Categorie interessati	Categorie dati	Destinatari comunicazione	Trasferimento	Termini Cancellazione	Misure di sicurezza	Contenuti ulteriori
Gestione del personale	**Dipendenti Collaboratori …**	**Dati personali Dati sanitari dati giudiziari**	**Enti previdenziali ….**	**….**	***Individuazione di un termine***	***Individuazione delle misure***	
Protocollo							
Radioprotezione							
Contenzioso							

La protezione dei dati

Privacy by design

- **Il Titolare mette in atto misure tecniche ed organizzative adeguate, quali la pseudonimizzazione, dirette a proteggere in modo efficace i principi di protezione dei dati, quali la minimizzazione, e ad integrare nel trattamento le garanzie necessarie a soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati.**

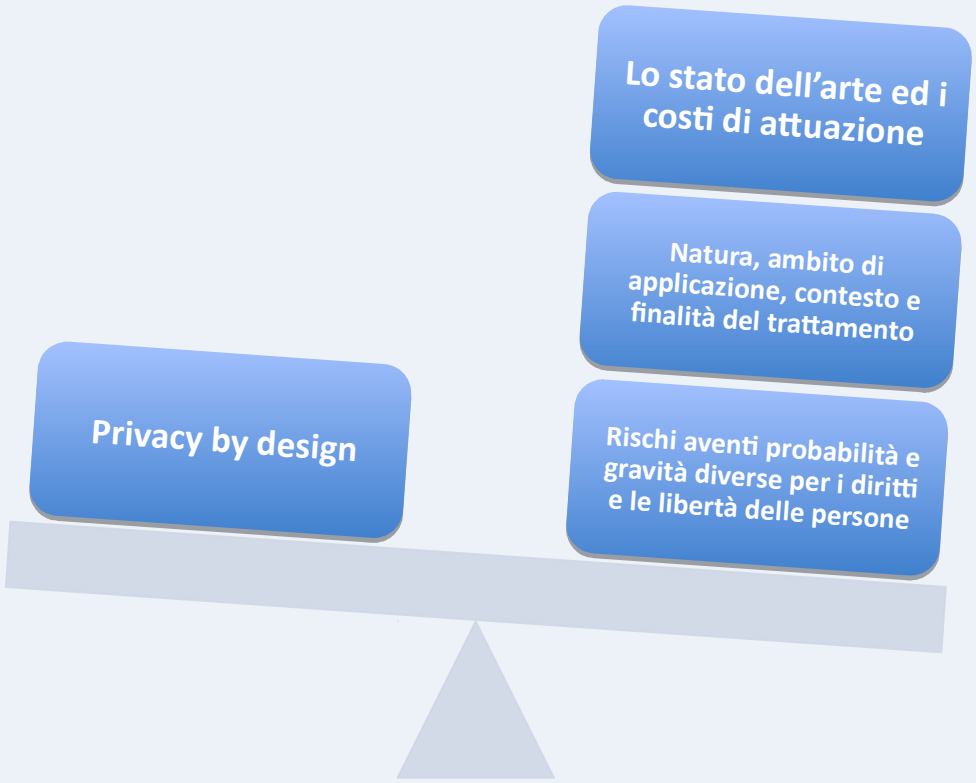
Privacy by default

- **Il Titolare mette in atto misure adeguate per garantire che siano trattati per impostazione predefinita solo i dati personali necessari per ogni specifica finalità del trattamento.**

Privacy by design

Sia al momento di determinare i mezzi del trattamento

Sia all'atto del trattamento



Privacy by default

Adozione di misure adeguate per garantire che siano trattati per impostazione predefinita solo i dati personali necessari per ogni specifica finalità del trattamento

Vale per:

La quantità dei dati raccolti;

La portata del trattamento;

Il periodo di conservazione;

L'accessibilità

Per impostazione predefinita non possono essere resi accessibili dati personali a un numero indefinito di persone senza l'intervento di una persona fisica

La Valutazione d'Impatto sulla Protezione dei Dati (DPIA)

- **Costituisce uno strumento di valutazione del rischio**

- **È necessaria**:
  - Per i trattamenti che presentano **rischi elevati** per i diritti e le libertà delle persone
    - Rischio elevato: principio di carattere generale, può derivare dall'uso di nuove tecnologie, considerati la natura, l'oggetto ed il contesto del trattamento

L'analisi dei rischi

- Deve essere svolta nell'ambito della Valutazione d'impatto sulla Protezione dei Dati (DPIA)
- È propedeutica alla valutazione delle misure da adottare
- Non è una misura nuova (era già prevista nell'ambito del Documento Programmatico sulla Sicurezza)

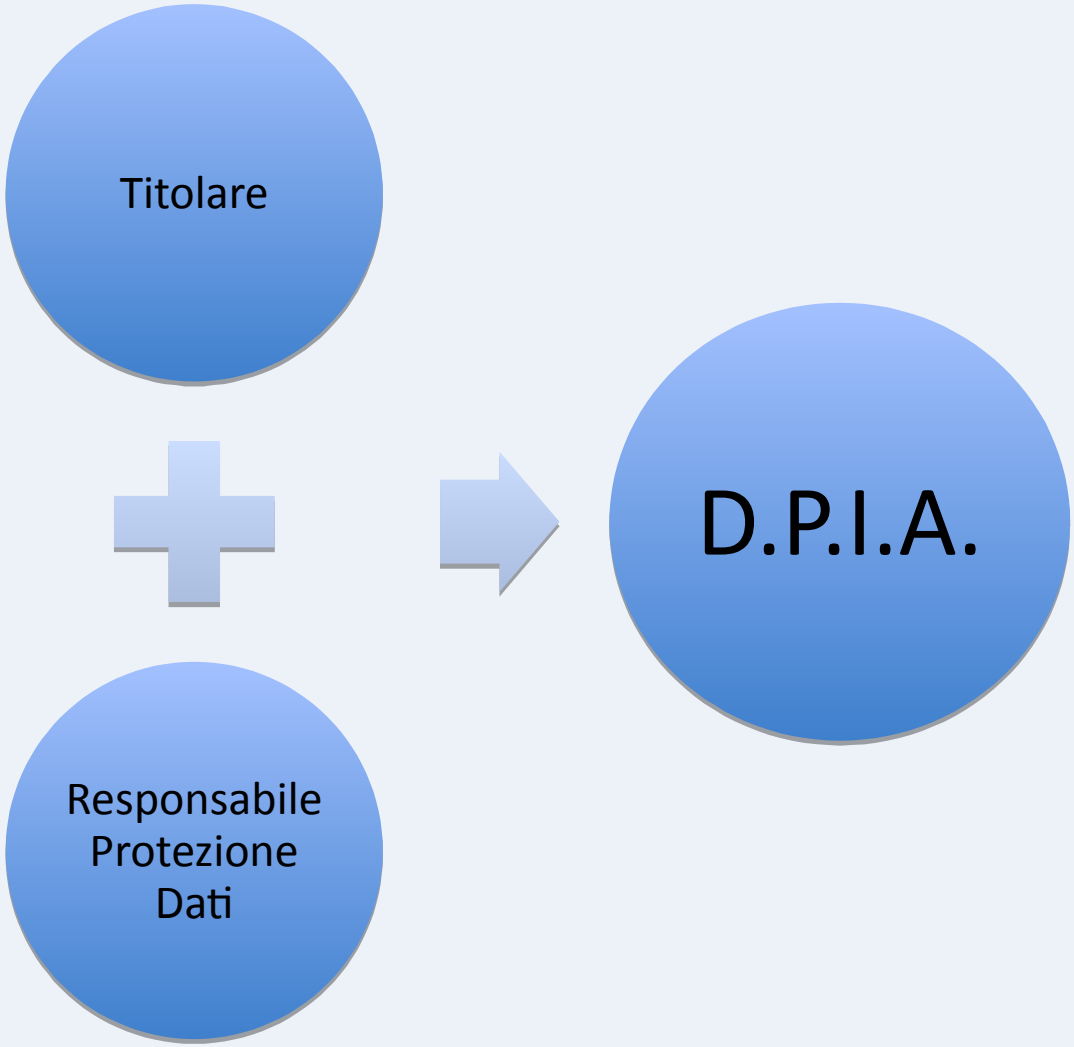
La Valutazione d'Impatto sulla Protezione dei Dati (DPIA)

Costituisce attività basilare per gestire il rischio relativo al trattamento ed individuare le misure di sicurezza adeguate al trattamento effettuato in concreto.

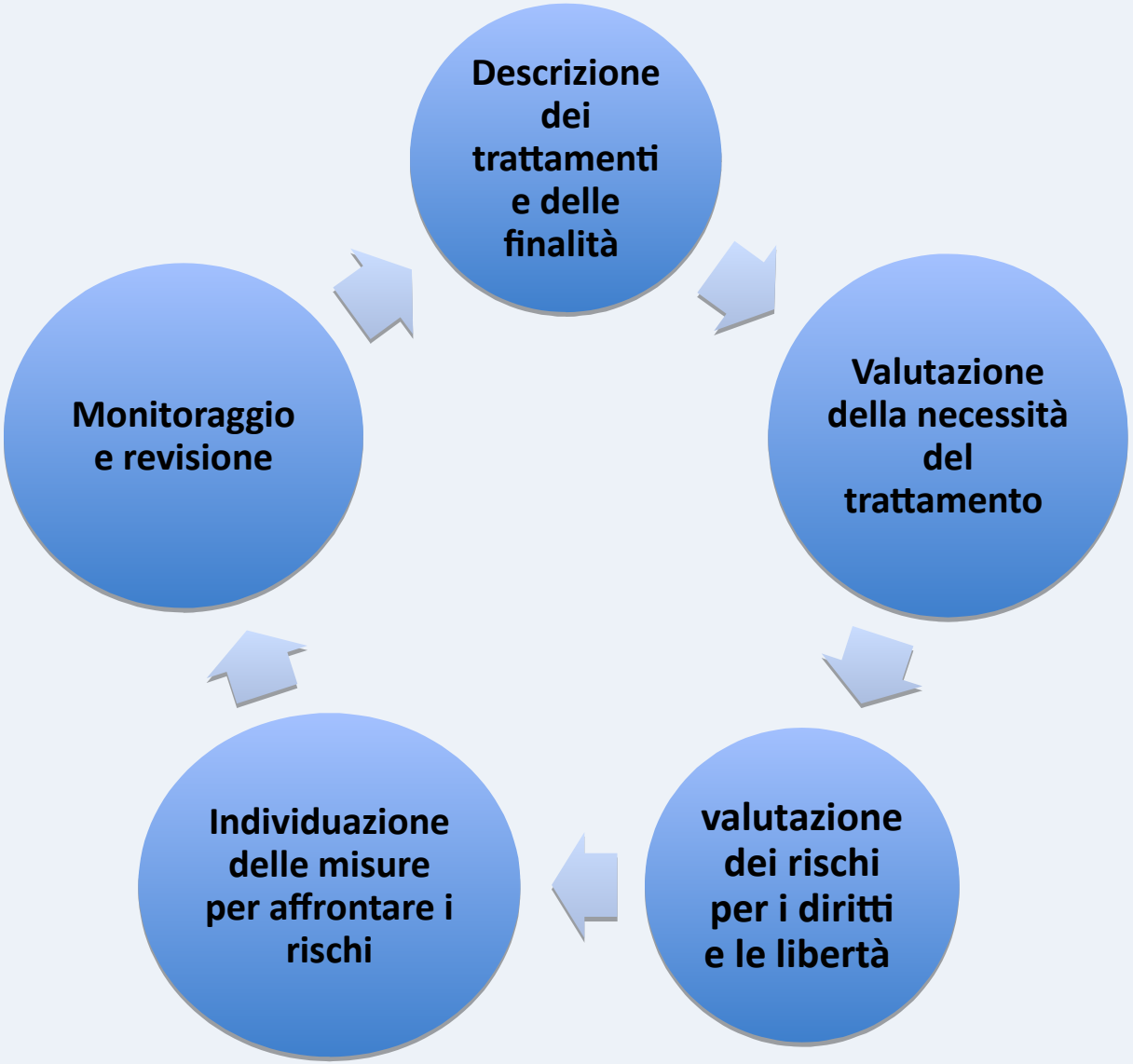
DPIA: Quando è obbligatoria

- ✓ In caso di valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, sulla quale si fondano decisioni che hanno effetti giuridici
- ✓ **In caso di trattamento su larga scala di categorie particolari di dati personali (dati sanitari, genetici, opinioni politiche, sindacali, vita e orientamento sessuale …)**
- ✓ Sorveglianza sistematica di zona accessibile al pubblico

DPIA: chi la conduce



DPIA: come si fa



La sicurezza dei trattamenti

I dati personali devono essere trattati in modo da garantirne un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali

Le indicazioni del Garante

- Sicurezza tramite trasparenza nei trattamenti dei dati personali
- Documentazione dei trattamenti come elemento di sicurezza
  - Importanza della documentazione tecnica dei trattamenti con strumenti elettronici
  - Documentazione dei sistemi informativi:
    - Viste e diagrammi
    - *Deployment view*
    - Attori interni ed esterni

Le misure di sicurezza indicate nel Regolamento

Pseudonimizzazione

- "Trattamento dei dati personali in modo tale che i dati non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni siano trattate separatamente e soggette a misure tecniche e organizzative intese a garantire intesi a garantire che tali dati non siano attribuiti a una persona identificata o identificabile"

Cifratura

- "Tecnica di protezione crittografica dei dati rilevante per minimizzare i rischi incombenti soprattutto in caso di accessi abusivi o perdita di dati"

Le misure di sicurezza indicate nel Regolamento

Consistenza	• Capacità di assicurare su base permanente, integrità disponibilità e resilienza dei sistemi e dei servizi di trattamento
Disaster recovery	• Capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico
Valutazione delle misure	• Procedura per testare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

Le misure di sicurezza indicate nel Regolamento

Attenzione:

Chiunque abbia accesso al trattamento dei dati personali può trattarli soltanto se è stato istruito in tal senso dal Titolare del trattamento

La minimizzazione dei rischi

- ✓ Sicurezza come percorso, non come obiettivo tecnico assoluto
- ✓ Adeguatezza delle misure rispetto ai rischi incombenti sui dati
- ✓ Richiamo alla ragionevolezza delle misure sulla base di considerazioni di carattere tecnico ed economico
- ✓ Gestione del rischio residuo
- ✓ Minimizzazione dei dati. Meno dati = meno rischi

Insomma …

Abbiamo qualcosina da fare da qui a maggio!

Un piccolo accenno al *data breach*

- Che cos'è:

  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 raccolti, conservati o comunque trattati

- Con l'entrata in vigore del Regolamento determinerà obblighi di condotta per la generalità dei Titolari

Obblighi del Titolare in caso di data breach

Il Titolare del trattamento notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, salvo che sia improbabile che la violazione presenti rischi per i diritti e la libertà delle persone

Quando la violazione presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare comunica la violazione all'interessato senza ingiustificato ritardo

Il Titolare documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le conseguenze e i provvedimenti per porvi rimedio.

(Necessari per eventuali verifiche del Garante)

Cosa notificare al Garante

- ✓ La natura delle violazioni dei dati personali, comprese le categorie e il numero approssimativo degli interessati coinvolti, nonché le categorie e il numero approssimativo di registrazione dei dati in questione
- ✓ I dati identificativi e di contatto del Responsabile della Protezione dei Dati
- ✓ La descrizione delle probabili conseguenze della violazione di dati personali
- ✓ La descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se possibile attenuarne i possibili effetti negativi.

Grazie!