La tutela della privacy nella Pubblica Amministrazione

Applicazione del Regolamento UE 679/2016

Anna Rita Marocchi

Evoluzione normativa

1995 Direttiva 95/46/UE
Protezione dati personali

L. 31/12/96 n. 675

D.Lgs. 196/2003
Codice Privacy

Regolamento UE 679/2016
Regolamento sulla protezione dei dati personali

Regolamento UE 679/2016
Le principali novità

- Uniformità in ambito UE
- Più attenzione alle tecnologie utilizzate
- Diritto all'oblio
- RPD, *Responsabile Protezione Dati*
- Principio di "*responsabilizzazione*"
- Privacy *by design* e *by default*
- Registro dei trattamenti
- Violazione dati - *Data breach*
- Nuovo sistema sanzionatorio

ancitel
La rete dei Comuni Italiani

Disposizioni Generale

Protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali (art. 1, c. 2)

Disposizioni generali

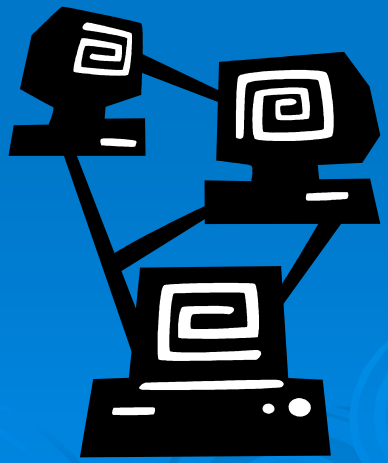
Si applica al trattamento interamente o parzialmente automatizzato dei dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi (art. 2)

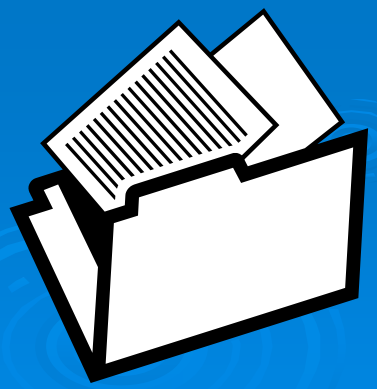
ancitel
La rete dei Comuni Italiani

E dunque le Risorse:

UMANE

STRUMENTALI





I princìpi del nuovo Regolamento – Artt. 5 e 9

- **I dati personali debbono essere:**
  - Trattati in modo lecito, corretto e trasparente
  - Raccolti per finalità determinate, esplicite e legittime
  - Adeguati, pertinenti e limitati a quanto necessario
  - Esatti e aggiornati: garantire tutte le misure ragionevoli per cancellare o rettificare i dati inesatti
  - Conservati in forma che consenta l'identificazione degli interessati per un tempo non superiore alla finalità per cui sono trattati
  - Trattati in maniera da garanatire un'adeguata sicurezza mediante misure tecniche e organizzative adeguate

I diritti degli interessati – Art. 12

Efficace protezione dei dati personali e disciplina dettagliata dei diritti degli interessati e degli obblighi di chi effettua il trattamento dei dati

- Cancellazione (oblìo) – Art. 17
- Limitazione del trattamento – Art. 18
- Accesso ed informazione – Art. 15
- Portabilità dei dati – Art. 20
- Rettifica e integrazione – Art.16
- Reclamo al Garante – Art. 77

I diritti degli interessati – Art. 12

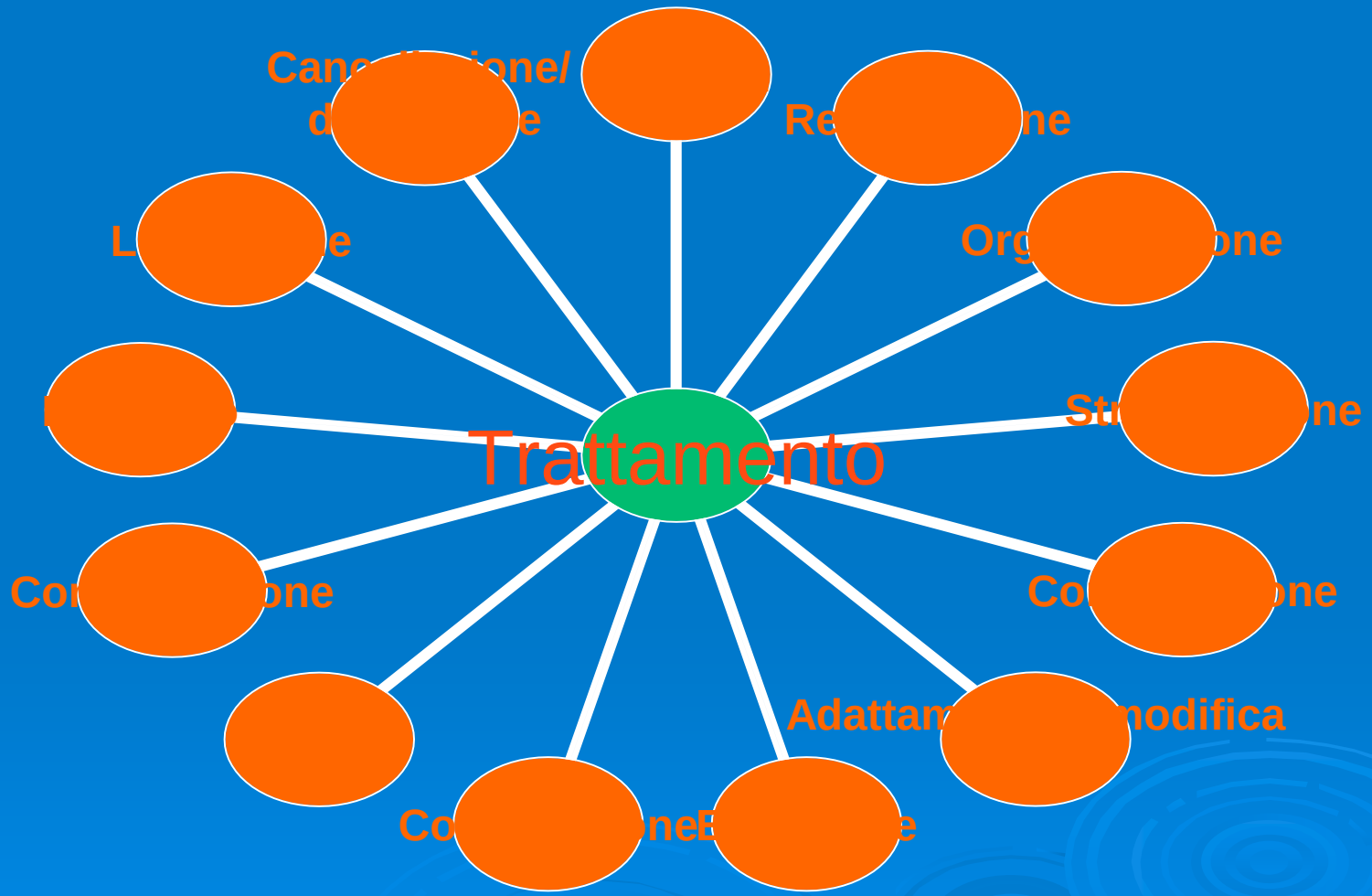
Il titolare del trattamento deve:

- Dare risposta in forma scritta entro 1 mese dal ricevimento della richiesta (fino a 3 mesi se complessa)
- Rispondere in modo chiaro, semplice, conciso

DEFINIZIONI – Art. 4

- Dato personale
- Trattamento
- Limitazione del trattamento
- Profilazione
- Pseudonimizzazione
- …
- Dati genetici (es. caratteristiche genetiche ereditarie)
- Dati biometrici (es. rilevazione immagine facciale)

DEFINIZIONI - Il Trattamento



LE PRIORITA' DEL NUOVO REGOLAMENTO

- Individuazione e nomina *RPD* - Art. 37
- Predisposizione del *registro dei trattamenti* – Art. 30
- *Violazione dati. Data breach* – Art. 33
- Formazione – Art. 29 e 39

Le figure della Privacy

TITOLARE
Art. 24

RESPONSABILE
Art. 28

Autorizzati ad accedere ai dati (incaricati)
Artt. 29, 32

RPD – DPO
Responsabile Protezione Dati
Art. 37

INTERESSATO (persona fisica, identificata o identificabile)
Art. 4

TITOLARE DEL TRATTAMENTO

Artt. 24, 25, 28, 30, 32 e 35)

- Responsabilità (accountability)
- Misure tecniche ed organizzative adeguate
- Privacy by design (protezione dei dati fin dalla progettazione) – art. 25, par. 1
- Privacy by default (protezione dei dati per impostazione predefinita) – Art. 25, par. 2
- Registro dei trattamenti – Art. 30
- Garanzia del livello di sicurezza – Art. 32
- Privacy impact assessment – PIA – Art. 35

RESPONSABILE PROTEZIONE DEI DATI – RPD - Art. 37

- Obbligatorio nella P.A.
- E’ designato in funzione della qualifica professionale e conoscenza specialistica della normativa e prassi in materia di protezione dei dati personali
- Può essere un dipendente del titolare o del responsabile del trattamento oppure un esterno con contratto di servizi
- I suoi dati sono pubblici e comunicati al Garante

I compiti del RPD – Art. 39

- Informare e fornire consulenza al titolare o al responsabile del trattamento in merito agli obblighi derivanti da tale Regolamento
- Sorvegliare l'osservanza del Regolamento e fornire un parere in merito alla valutazione sulla protezione dei dati (PIA – Privacy Impact Assessment)
- Cooperare con il Garante e fungere da punto di contatto per questioni connesse al trattamento

Il registro dei trattamenti - Art. 30

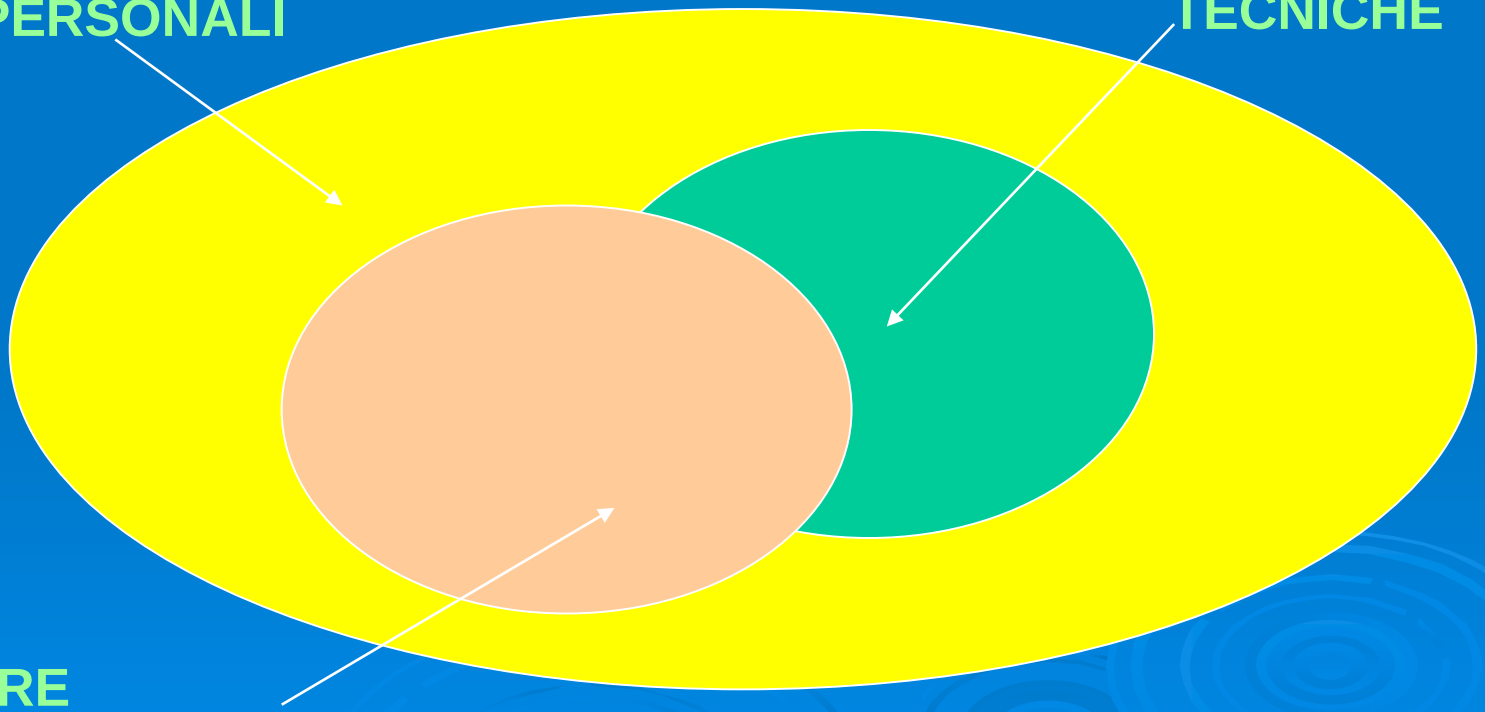
Ogni titolare deve predisporre un registro dei trattamenti in cui si descrive l'insieme delle attività di trattamento e una descrizione generale delle misure di sicurezza tecniche e organizzative

In particolare il registro evidenzia:

- **Le generalità del titolare, dei contitolari e responsabili**
- **Finalità del trattamento**
- **Categoria dei destinatari a cui i dati saranno comunicati**
- **I trasferimenti di dati verso paesi terzi o org.ni int.li**
- **Le modalità del trattamento**
- **I termini per la cancellazione**
- **Le misure di sicurezza tecniche e organizzative**

Sicurezza del trattamento – Art. 32

MISURE ADEGUATE A GARANTIRE LA SICUREZZA DEI DATI PERSONALI



Valutazione impatto protezione dati Art. 35

Il titolare effettua una valutazione dei rischi quando il trattamento (*considerati la natura, l'oggetto e il contesto e le finalità*) prevede l'uso di nuove tecnologie e può presentare un rischio elevato per i diritti e le libertà delle persone fisiche

La valutazione contiene:

- Descrizione sistematica dei trattamenti, finalità e interesse legittimo
- Valutazione della necessità e proporzionalità in relazione alle finalità
- Valutazione dei rischi per gli interessati
- Misure previste per affrontare i rischi (comprova di aver adottato tutte le misure adeguate alla protezione dei dati)

Violazione dei dati personali – *data breach* - Artt. 33 e 34

In caso di violazione dei dati personali il titolare del trattamento notifica la violazione al Garante SENZA INGIUSTIFICATO RITARDO entro 72 ore ove la violazione presenti un rischio per i diritti e le libertà delle persone fisiche

Principio di trasparenza – Comunicazione all'interessato

COSA FARE

Organizzazione:

- **Individuazione del modello organizzativo**
- **Individuazione e nomina del Responsabile Dati Personali**

Adempimenti:

- **Verifica e programmazione della sicurezza**
- **Predisposizione Piano di adeguamento e documentazione a supporto**
- **Predisposizione del Registro dei Trattamenti**
- **Piano di formazione**

Tutela dei diritti dell'interessato:

- **Informativa**
- **Accesso ai dati**
- **Data breach**

Adeguamento delle procedure:

- **Ordini di servizio**
- **Regolamento e Linee guida sui trattamenti**

Predisporre un processo di adeguamento adeguato

RPD

DOCUMENTAZIONE
- Monitoraggio e sorveglianza
- Cooperare con il Garante

TITOLARE

CONTITOLARE
RESPONSABILI

MISURE DI SICUREZZEA ADEGUATE
Parere Risk assessment

PIANO DI FORMAZIONE

GUIDE DI COMPORTAMENTO E REGOLAMENTO INTERNO

PIANO DI ADEGUAMENTO

ancitel
La rete dei Comuni Italiani

Anna Rita Marocchi

SANZIONI – Artt. 83 e 84

CRITERI PER LE SANZIONI AMMINISTRATIVE

- Effettive, proporzionate e dissuasive
- Natura, gravita e durata della violazione
- Carattere doloso o colposo della violazione
- Misure adottate dal titolare/responsabile del trattamento
- Precedenti violazioni
- Adesione ai codici di condotta
- Eventuali fattori aggravanti

SANZIONI SEVERE = in base alle violazioni

Dal 2% al 4% del fatturato globale

Da 10 mln di euro fino a 20 mln di euro

Grazie per l'attenzione

Per info: marocchi@ancitel.it
Tel. 06 76291311 – cell. 331 9009743