

# **REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI(RGPD)**

Regolamento (UE) 2016/679 del  
Parlamento Europeo e del Consiglio  
del 27 aprile 2016

Nuova normativa:  
principali novità

Ambito di  
applicazione e  
definizioni

Principi  
fondamentali del  
RGPD e diritti  
degli interessati

Obblighi dei  
titolari e  
responsabili  
del trattamento

Metodologia

Conclusioni

# Nuova normativa: principali novità

## Nueva normativa

### RGPD

**Regolamento (UE) 2016/679** del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (**Regolamento Generale sulla Protezione dei Dati**)

### Progetto di legge organica

Publicato nell **BOE il 24 novembre 2017**: a sua approvazione è prevista per marzo 2018.

Rispetta sempre il Regolamento Generale sulla Protezione dei Dati e chiarisce il contenuto.

Sostituirà l'attuale legge organica sulla protezione dei dati.

### Abrogato

La precedente direttiva europea 95/46 / CE è abrogata.

La legge organica 15/99 sulla protezione dei dati è abrogata.

Il regio decreto 1720/2007 è abrogato.

Non è necessario trasporre (sarà lo stesso in tutti i paesi dell'UE).



**Obbligatorio dal 25  
maggio 2018**

# Cambiamenti concettuali

## LOPD



## RGPD

Consenso tacito

3 livelli: base, medio, alto

Registrazione pubblica dei file in AEPD

Regolamento esterno: misure di sicurezza RD 1720/2007

Diritti: Arco

Consenso espreso

2 livelli: speciale e non speciale

Registro interno delle attività

Autoregolamentazione: proprie misure di sicurezza


6 Diritti: ARCO + oblio + portabilità

# Ambito di applicazione e definizioni

## Ambito di applicazione del RGPD

**Trattamenti (automatizzati o no)** dei dati personali delle persone fisiche, indipendentemente dalla loro nazionalità o dal loro luogo di residenza.

- **Titolare situato nell'UE**, indipendentemente dal fatto che il trattamento avvenga nell'UE o meno.
- **Interesati residenti nell'UE** che offrono beni o servizi a tali soggetti interessati non UE, anche gratuitamente.



**Non** si applica  
alle persone  
giuridiche.



**Non** si applica  
nella sfera  
personale o  
domestica  
(social  
network).

### **Dati di contatto e singoli imprenditori.**

- Si presume siano protetti da interessi legittimi (6.1.f RGPD).
- Il RGPD è applicato a loro.

## Definizioni del RGPD

### Dato personale

Informazione riguardante una persona fisica identificata o identificabile (“interessato”)

### Trattamento

Operazione o insieme di operazioni compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali

### Archivio

Insieme strutturato di dati personali accessibili secondo criteri determinati

### Titolare del trattamento

Persona fisica o giuridica, autorità pubblica, il servizio o altro organismo che, singolarmente o insieme al altri, determina la finalità e i mezzi del trattamento.

### Responsabile del trattamento

Persona fisica o giuridica, autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento



# Principi fondamentali del RGPD e diritti degli interessati

## Principi fondamentali del RGPD


- Liceità, correttezza e trasparenza.
- Limitazione della finalità.
- Minimizzazione dei dati.
- Esattezza.
- Limitazione della conservazione.
- Integrità e riservatezza.
- Responsabilizzazione - “Accountability”.

## Diritti degli Interessati

- 
- Diritto di **accesso** (art. 15 RGPD).

- 
- Diritti a **rettifica e cancellazione** (art. 16 y 17 RGPD).
    - “Diritto all’**oblio**”: Internet.

- 
- Diritto di **limitazione di trattamento** (art. 18 RGPD).

- 
- Diritto alla **portabilità dei dati** (art. 20 RGPD).
    - Telecomunicazioni, etc.

- 
- Diritto di **opposizione** (art. 21 RGPD).

# Obblighi dei titolari e responsabili del trattamento

## Obblighi del titolare e del responsabile

Registrazione delle attività di trattamento.

Misure di sicurezza e analisi dei rischi.

Violazioni della sicurezza.

Valutazione dell'impatto sulla protezione dei dati (EIPD).

Responsabile della Protezione dei Dati

Codici di condotta e certificazione.

Trasferimenti internazionali di dati

Violazioni e sanzioni.

# Sanzioni

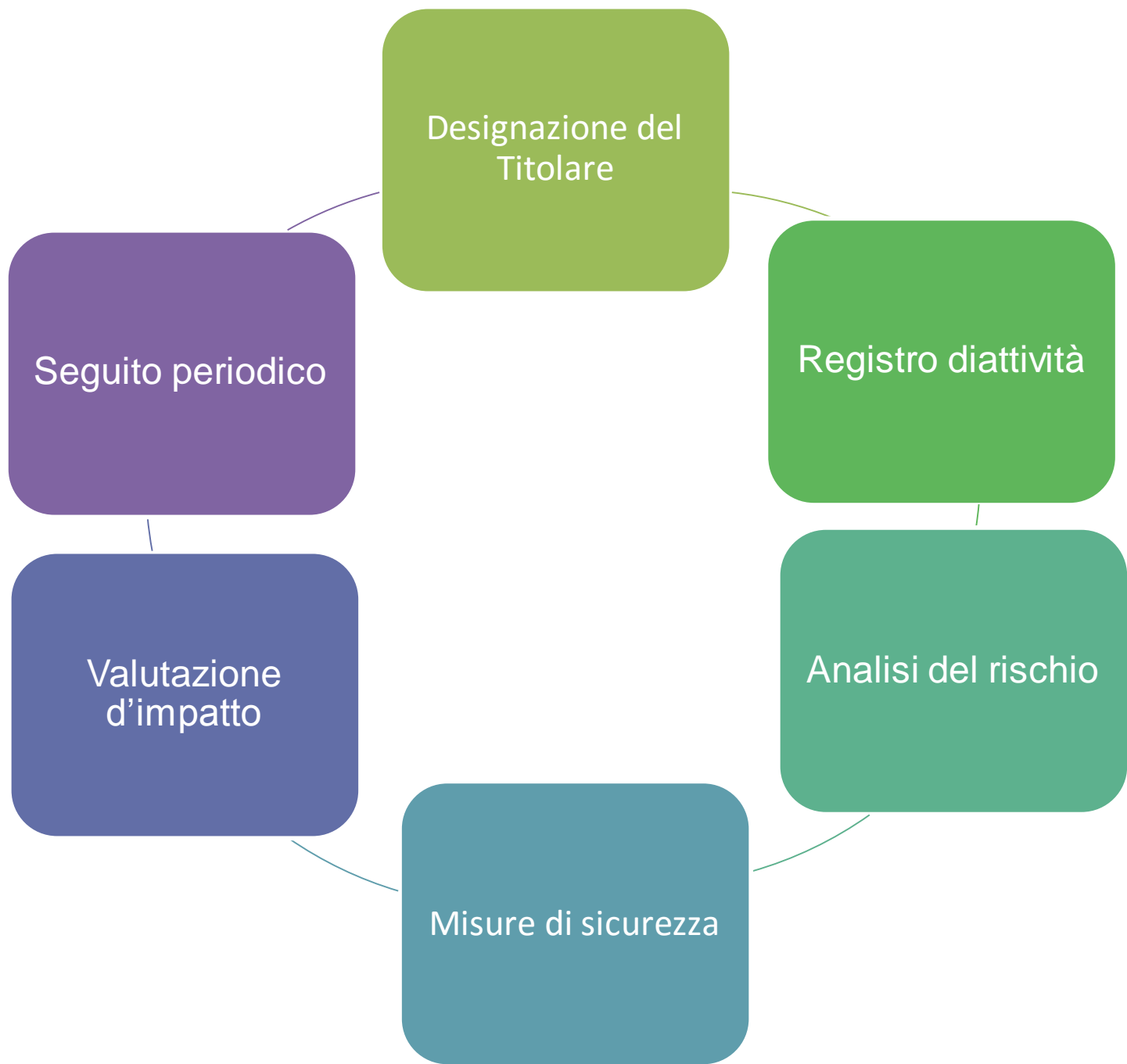
## Art. 45 LOPD

- 1.- Le violazioni minori saranno sanzionate con una multa da 900 a 40.000 euro.
- 2.- Le violazioni gravi saranno sanzionate con una multa da 40,001 a 300.000 euro.
- 3.- Le violazioni molto gravi saranno sanzionate con una multa da 300,001 a 600.000 euro

## Art. 83 RGPD

- 1.- Sanzioni amministrative fino a 10.000.000 EUR o, per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.
- 2.- Sanzioni amministrative fino a 20.000.000 EUR o, per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

# Metodologia.





# Metodo Mosler

## Concetto

- I rischi rilevati devono essere misurati e valutati al fine di trattarli correttamente.
- Esistono diversi metodi di valutazione del rischio, non tutti utili per valutare i rischi legati alla protezione dei dati.
- Il metodo Mosler è un metodo matematico riconosciuto a livello internazionale e utilizzato nell'analisi del rischio.

Conclusini.

# Conclusioni

Data chiave RGPD: 25 maggio 2018.

Responsabilità - “Accountability”.

Metodologia o procedura di adattamento.

Rivedi tutti i testi legali della Protezione dei Dati: consenso, diritto di informazione, pagine web.

Preparare le politiche di protezione dei dati adattate alla nostra organizzazione.


Le sanzioni possono raggiungere fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente.

# Domande frequenti


## GENERALE



- È necessario continuare a registrare i archivi nell'AGPD?



- L'attuale LOPD continuerà ad applicarsi in alcuna area?




- Qual è il primo passo per l'adeguamento del nuovo regolamento?



- Cosa succederebbe in caso di violazione della sicurezza?

## SUL LAVORO

- 
- Posso mantenere i dati di un ex-lavoratore? Se mi chiede di cancellarli, cosa dovrei fare e come?

- 
- Devo cancellare i candidati che ho nel mio database?


- 
- Posso contattare un candidato tramite un'email che trovo online?

- 
- Cosa succede se il curriculum proviene da un portale di lavoro o simili?

## GESTIONE



- Con un database di clienti e potenziali che uso per contattare in modo massiccio, posso continuare a usarlo "così com'è"?




- Come posso ottenere il consenso esplicito di quelli elencati nel mio database e non sono clienti?



- Per quanto riguarda il consenso tacito, esiste una regola di legge transitoria per mantenerla valida?



- Ho un avviso legale sul mio sito web, posso ancora usarlo?




- In un gruppo multinazionale, dovrebbe essere nominato un Responsabile per la Protezione dei Dati o uno per ogni paese?



## NUOVE FIGURE

---

- 
- Quali nuovi strumenti di controllo hanno i cittadini?

- 
- In cosa consiste il meccanismo dello “sportello unico”?

# Grazie per la tua attenzione

**Josep Ma Barcelona Pedret**  
Bufete Escura  
[jmbarcelona@escura.com](mailto:jmbarcelona@escura.com)