GDPR

EU

General Data Protection Regulation

Nuove regole comunitarie in materia di protezione dei dati personali

SAPIENZA
UNIVERSITÀ DI ROMA

Ing. Francesco Ficarola
Cyber Security Technical Officer

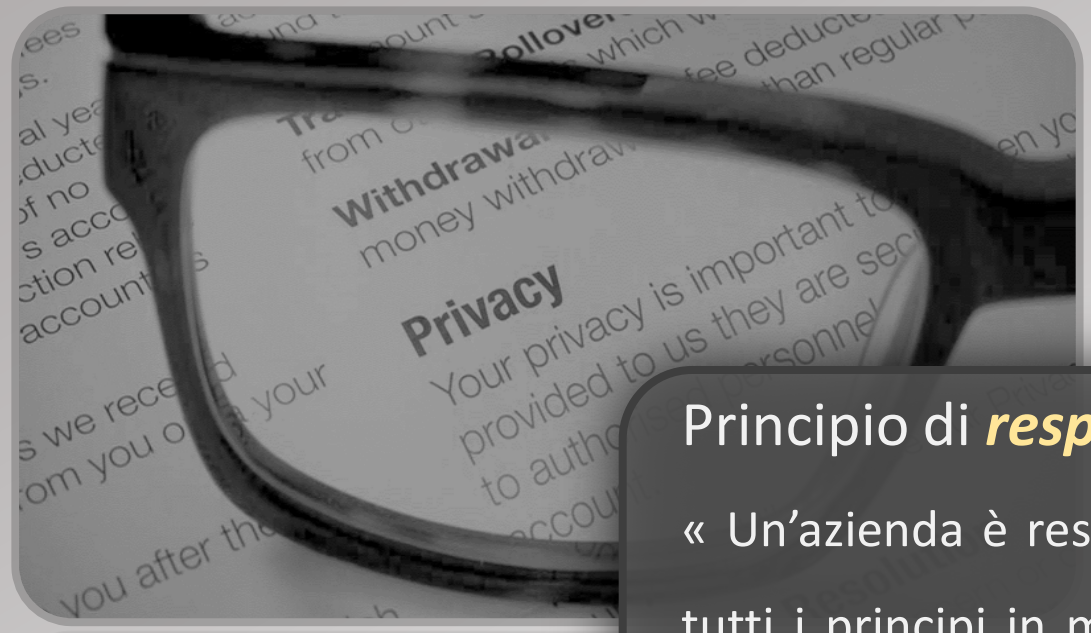
DI COSA SI TRATTA?

Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali.

- Regole più chiare su informativa e consenso
- Definizione limiti al trattamento automatizzato dei dati personali
- Introduzione nuovi diritti esercitabili dall'utente
- Norme rigorose per casi di data breach

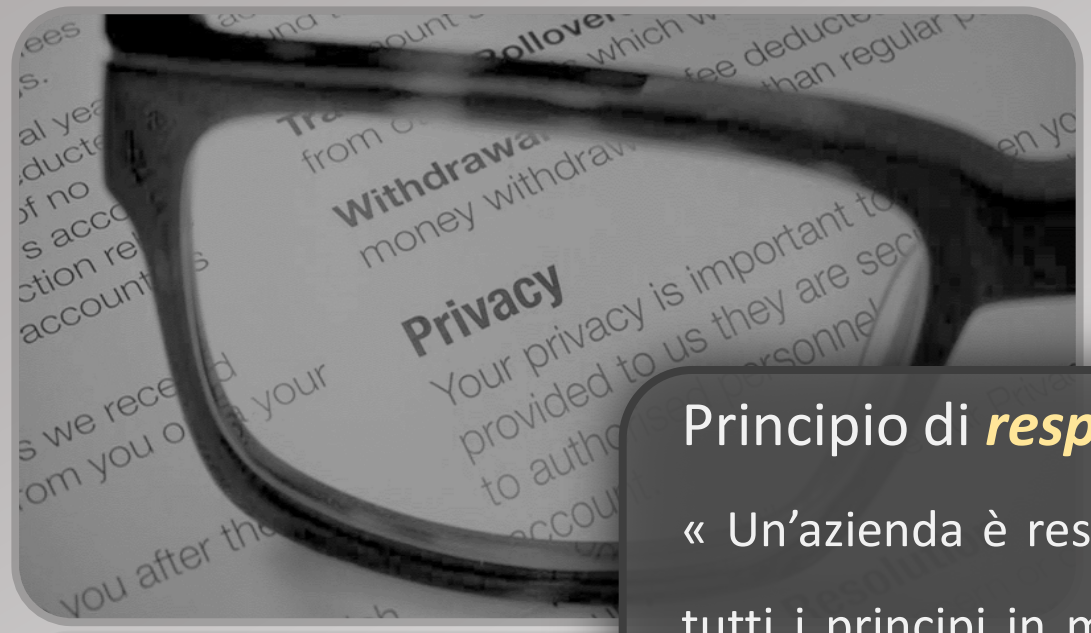
PRINCIPI DEL REGOLAMENTO

- Dati trattati in modo lecito e trasparente
- Finalità specifiche per il trattamento dei dati
- Minimizzazione dei dati
- Accuratezza dei dati (aggiornati ed esatti)
- Uso vietato dei dati per altri scopi
- Integrità e riservatezza dei dati



Principio di ***responsabilizzazione***

« Un'azienda è responsabile del rispetto di tutti i principi in materia di protezione dei dati, dimostrandone tale conformità »



Principio di ***responsabilizzazione***

« Un'azienda è responsabile del rispetto di tutti i principi in materia di protezione dei dati, dimostrandone tale conformità »

Codice di condotta

Meccanismo di certificazione

LIMITI DI CONSERVAZIONE DEI DATI

Dati conservati per il più breve tempo possibile

Stabilire limiti di tempo per cancellare o rivedere i dati

« In via eccezionale, i dati personali possono essere conservati per un periodo più lungo a fini di archiviazione nell'interesse pubblico o per ricerche scientifiche o storiche, a condizione che siano adottate misure tecniche e organizzative adeguate (ad esempio anonimizzazione, cifratura ecc.) »

INFORMARE GLI UTENTI

Informativa che descriva i seguenti punti:

- ❑ Chi è la tua azienda/organizzazione (dati di contatto)?
- ❑ Perché utilizzerai i loro dati personali (finalità)?
- ❑ Le categorie di dati personali interessate
- ❑ La giustificazione giuridica per il trattamento dei dati
- ❑ Tempo di conservazioni dei dati
- ❑ Chi altro potrebbe riceverli
- ❑ Eventuali trasferimenti a un destinatario al di fuori dell'UE
- ❑ Diritto di accesso ai dati personali
- ❑ Diritto di revocare il consenso in qualsiasi momento

INFORMARE GLI UTENTI

Informativa che descriva i seguenti punti:

- ❑ Chi è la tua azienda/organizzazione (dati di contatto)?
- ❑ Perché utilizzerai i loro dati personali (finalità)?
- ❑ Le categorie di dati personali interessate
- ❑ La giustificazione giuridica per il trattamento dei dati
- ❑ Tempo di conservazioni dei dati
- ❑ Chi altro potrebbe riceverli
- ❑ Eventuali trasferimenti a un destinatario al di fuori dell'UE
- ❑ Diritto di accesso ai dati personali
- ❑ Diritto di revocare il consenso in qualsiasi momento

MOTIVI DEL TRATTAMENTO

Trattamento dati personali solo nei casi seguenti:

- ✓ con il *consenso* delle persone interessate
- ✓ laddove esista un *obbligo contrattuale*
- ✓ per adempiere a *un obbligo giuridico*
- ✓ per l'esecuzione di un compito nell'*interesse pubblico*
- ✓ per proteggere gli *interessi vitali* di una persona
- ✓ per i *legittimi interessi* della tua organizzazione, ma solo dopo aver verificato che non vengano compromessi i diritti e le libertà fondamentali della persona di cui stai trattando i dati

LEGITTIMO INTERESSE

Trattamento dati personali solo nei casi seguenti:

- ✓ con il *consenso* delle persone interessate
- ✓ laddove esista un *obbligo contrattuale*
- ✓ per adempiere a *un obbligo giuridico*
- ✓ per l'esecuzione di un compito nell'*interesse pubblico*
- ✓ per proteggere gli *interessi vitali* di una persona
- ✓ per i *legittimi interessi* della tua organizzazione, ma solo dopo aver verificato che non vengano compromessi i diritti e le libertà fondamentali della persona di cui stai trattando i dati

Necessità di trattare dati personali per svolgere compiti legati alle attività aziendali.

DATI SENSIBILI

- Dati relativi a origine razziale o etnica
- Opinioni politiche
- Convinzioni religiose o filosofiche
- Appartenenza a un sindacato
- Dati genetici e dati biometrici
- Dati relativi alla salute
- Dati relativi alla vita sessuale di una persona

DATI SENSIBILI

- Dati relativi a origine razziale o etnica
- Opinioni politiche
- Convinzioni religiose o filosofiche
- Appartenenza a un sindacato
- Dati genetici e dati biometrici
- Dati relativi alla salute
- Dati relativi alla vita sessuale di una persona

Trattati dietro esplicito consenso

Ricerca scientifica o storica

Richiesto dalla legislazione alla azienda

Interessi vitali in gioco

Resi pubblici dalla persona

Difesa di un diritto in sede giudiziaria

Medicina preventiva o professionale

RUOLI PRINCIPALI NEL GDPR

Titolare del trattamento
(Data Controller)

Stabilisce le *finalità* e le *modalità* del trattamento dei dati personali.

Mette in atto misure tecniche e organizzative adeguate per garantire che il trattamento è effettuato conformemente al presente regolamento.

Insieme al responsabile del trattamento, designa il responsabile della protezione dati.

Responsabile del trattamento
(Data Processor)

Tratta i dati personali solo per conto del titolare del trattamento.

È privo di autonomia nel decidere come e per quali ragioni può trattare i dati degli interessati, né può ricorrere ad altro responsabile senza previa autorizzazione scritta.

Supporta il titolare per mettere in atto le misure tecniche e organizzative.

Responsabile della protezione dati
(Data Protection Officer)

Assiste il titolare del trattamento o il responsabile del trattamento in tutte le questioni relative alla protezione dei dati personali.

Il DPO può configurarsi in una persona fisica o giuridica e non può essere rimosso né penalizzato per l'adempimento de propri compiti.

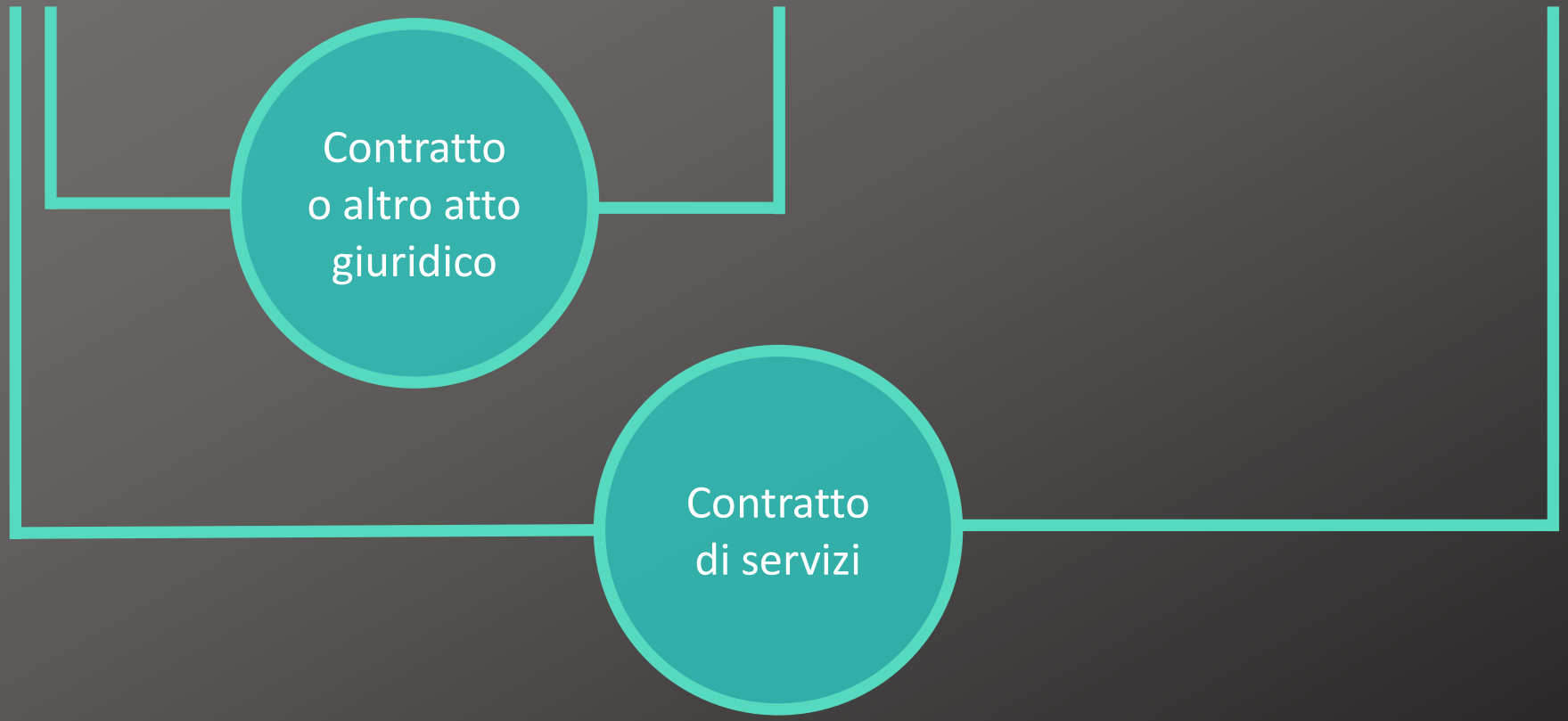
È tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.

RUOLI PRINCIPALI NEL GDPR

Titolare del trattamento
(Data Controller)

Responsabile del trattamento
(Data Processor)

Responsabile della protezione dati
(Data Protection Officer)



Protezione by Default

Protezione by Design

- Conservazione breve
- Solo dati necessari

MISURE TECNICHE ORGANIZZATIVE

- Pseudonimizzazione
- Cifratura

DATA BREACH

Si verifica una *violazione dei dati* quando i dati di cui la tua azienda/organizzazione è responsabile, subiscono un incidente di sicurezza con conseguente violazione della riservatezza, della disponibilità o dell'integrità.

DATA BREACH

In caso di data breach informare *l'autorità di vigilanza* senza indebito ritardo e al più tardi *entro 72 ore* dopo aver preso conoscenza della violazione

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

« Ogni volta che il trattamento può comportare un rischio elevato per i diritti e le libertà delle persone »

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

(Data Protection Impact Assessment)

SANZIONI

- Ammonimento
- Divieto di trattamento
- Sanzione *pecuniaria*

Fino a 20 milioni EUR

oppure

4% del fatturato annuo