

# Regolamento UE 679/2016

**Sistema informativo per il GDPR**  
protezione delle persone fisiche...  
...con riguardo al trattamento dei dati  
personali

PRIVACY

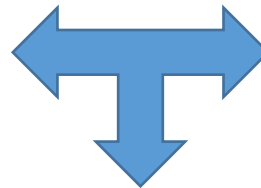


# EU-GDPR 2016\679

## Considerando 1

La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è uno dei diritti fondamentali.

Art.8 comma 1 carta dei diritti fondamentali dell'EU

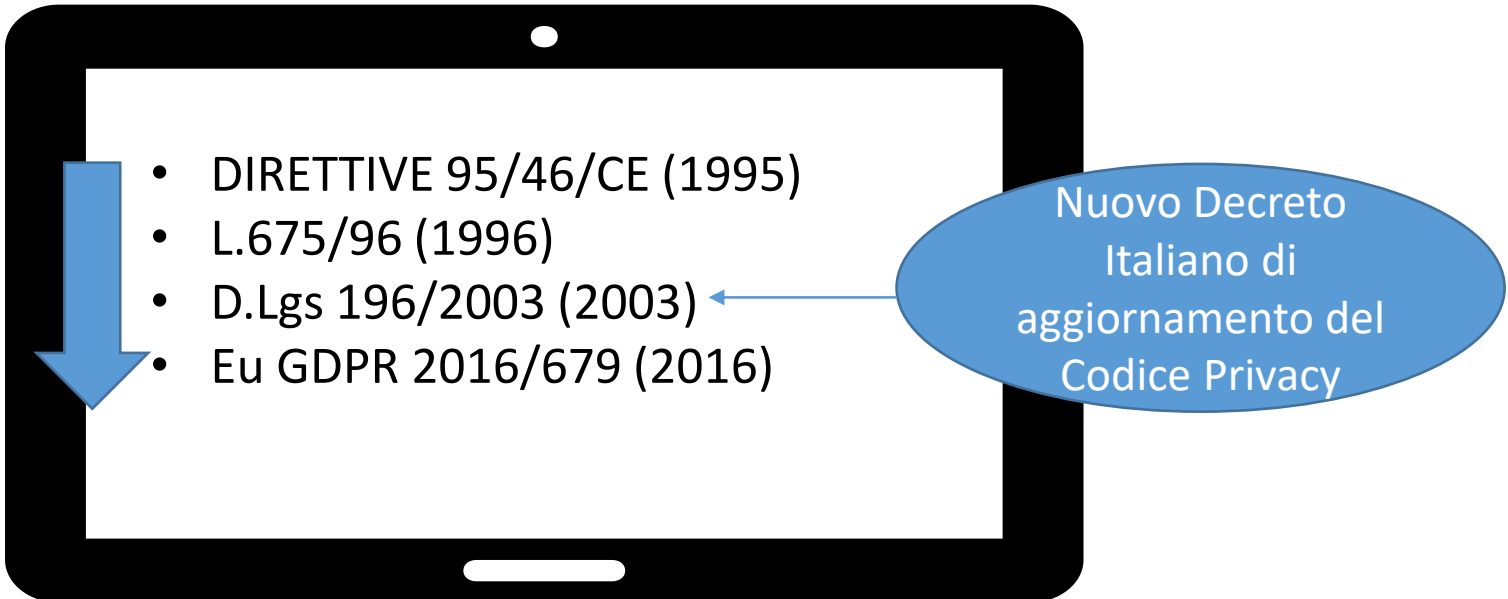


Art.16 comma 1 del TFUE\*

Stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano



# REGOLAMENTO EUROPEO EU-GDPR 2016/679

- 
- DIRETTIVE 95/46/CE (1995)
  - L.675/96 (1996)
  - D.Lgs 196/2003 (2003)
  - Eu GDPR 2016/679 (2016)

Nuovo Decreto  
Italiano di  
aggiornamento del  
Codice Privacy



# DIRITTO AL RISARCIMENTO E ALLE SANZIONI



## LA VIOLAZIONE DEGLI ARTT.

Sanzioni Penali  
introdotte dal nuovo  
Decreto di modifica del  
D.Lgs 196/2003

8,11,25,26,27,28,29,30,  
31,32,33,34,35,36,37,  
38,39,42,43

5,6,7,9, da 12 a 22, da  
44 a 49

Viene punita con:  
sanzione amministrativa  
pecuniaria fino a  
10.000.000 di euro o  
fino al 2% del fatturato  
mondiale annuo



Viene punita con:  
sanzione amministrativa  
pecuniaria fino a  
20.000.000 di euro o  
fino al 4% del fatturato  
mondiale annuo



# DIRITTO AL RISARCIMENTO E ALLE SANZIONI

Artt. 82 e 83

Chiunque subisca un danno «Materiale» o «Immateriale» cagionato da una violazione del Regolamento ha diritto di ottenere il risarcimento del danno dal Titolare o dal responsabile

- Un Titolare risponde per il danno cagionato di un trattamento non conforme al Regolamento
- Un Responsabile risponde al danno solo se non ha adempiuto ai suoi obblighi
- Il Titolare risponde sempre
- Le azioni Legali sono promosse dall'interessato davanti all'autorità Giurisdizionale competente



# DIRITTO AL RISARCIMENTO E ALLE SANZIONI

**EFFETTIVE, PROPORZIONATE E DISSUASIVE**

Prima di infliggere una sanzione si tiene conto di:

- 1.** Natura, gravità e durata della violazione
- 2.** Carattere doloso o colposo
- 3.** Misure adottate dal proprietario per attenuare il danno
- 4.** Responsabilità del titolare tenuto conto delle misure adottate
- 5.** Precedenti violazioni
- 6.** Cooperazione con le autorità
- 7.** Categoria di dati personali interessate
- 8.** Modo in cui l'autorità è venuta a conoscenza
- 9.** Provvedimenti in precedenza emessi nei confronti del titolare
- 10.** Adesioni a codice di condotta o ai meccanismi di certificazione approvati ai sensi dell'art.42
- 11.** Altre attenuanti o aggravanti (benefici economici o perdite)



# CAPO 2

## PRINCIPI DEL TRATTAMENTO

|   |            |
|---|------------|
| ■ | MARCO      |
| ■ | ROSSI      |
| ■ | 17/08/1971 |
| ■ | NAPOLI     |

**PRINCIPI  
GENERALI DEL  
TRATTAMENTO**

**ART.5 (1)- I DATI PERSONALI OGGETTO  
DI TRATTAMENTO SONO...**

Principio di liceità,  
correttezza e  
trasparenza...  
Trattati in modo lecito,  
corretto e trasparente  
nei confronti  
dell'interessato

Principio di  
minimizzazione dei  
dati...  
Adeguati, pertinenti e  
limitati a quanto  
necessario rispetto alle  
finalità per le quali  
sono trattati





**PRINCIPI  
GENERALI DEL  
TRATTAMENTO**

**ART.5 (1)- I DATI PERSONALI OGGETTO  
DI TRATTAMENTO SONO...**

Principio di esattezza e  
aggiornamento...  
Esatti e, se necessario  
aggiornati; devono essere  
adottate tutte le misure  
ragionevoli per cancellare o  
rettificare  
**TEMPESTIVAMENTE** i dati  
inesatti rispetto alle finalità  
per le quali sono trattati

Principio di  
limitazione delle  
finalità...  
Raccolti per finalità  
determinate, esplicite  
e legittime, e  
successivamente  
trattati in modo che  
non sia incompatibile  
con tali finalità



**PRINCIPI  
GENERALI DEL  
TRATTAMENTO**

**ART.5 (1)- I DATI PERSONALI OGGETTO DI TRATTAMENTO SONO...**

Principio di integrità e riservatezza...  
Trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, o dalla distruzione o dal danno accidentale

Principi di limitazione della conservazione...  
Adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattate

I dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per i quali sono trattati (salvo trattamenti archiviazione di pubblico interesse o per finalità di ricerca scientifica o per finalità statistiche)



# PRINCIPI GENERALI DEL TRATTAMENTO

Art.5 comma 2

## Responsabilizzazione

Il titolare del trattamento è competente per il rispetto del paragrafo 1 (*principi*) e in grado di provarlo

Occorre documentare le azioni intraprese

Accountability



# LICEITÀ DEL TRATTAMENTO

## **Comma 6 art.1**

**Il trattamento è lecito solo se è  
nella misura in cui ricorre almeno  
una delle seguenti condizioni**



# LICEITÀ DEL TRATTAMENTO

- ✓ **CONSENSO** Per una o più specifiche finalità
- ✓ **CONTRATTO** Necessità di esecuzione di un contratto di cui interessato è parte o di misure precontrattuali
- ✓ **OBBLIGO LEGALE** Necessità di adempire ad un obbligo legale
- ✓ **SALVAGUARDIA INTERESSI VITALI** Necessità di salvaguardia dell'interessato o di un'altra persona fisica
- ✓ **COMPITO DI INTERESSI PUBBLICI CONNESSO ALL'ESERCIZIO DI PUBBLICI SERVIZI**  
Necessità di esecuzione di un compito di interesse pubblico o connesso agli esercizi di pubblici poteri
- ✓ **LEGGITTIMO INTERESSE DEL TITOLARE** Necessita per il perseguimento del legittimo interesse del titolare se non prevalgono interessi, diritti e libertà fondamentali dell'interessato specie se minore



## LICEITA' DEL TRATTAMENTO

### ***LEGITTIMO INTERESSE DEL TITOLARE***

Il legittimo interesse del titolare del trattamento può costituire la base giuridica del trattamento dei dati, nel qual caso non occorre il consenso dell'interessato, purché, però, non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato tenuto conto delle ragionevoli aspettative dello stesso in base alla relazione col titolare del trattamento

Può essere considerato legittimo interesse trattare dati personali per finalità di Marketing diretto.

Va motivato:  
Documentazione processo decisionale  
+  
Valutazione dei rischi



# CONDIZIONI PER IL CONSENSO



## ART. 7



Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.



Il titolare deve essere in grado di dimostrare che l'interessato ha effettivamente prestato il proprio consenso in modo conforme a quanto stabilito dal Regolamento

La richiesta del consenso deve essere comprensibile, facilmente accessibile, redatta in forma e con termini semplici e chiari e deve essere presentata all'interessato «in modo chiaramente distinguibile dalle altre materie»

Consenso libero  
Il consenso deve essere liberamente prestato

**CONDIZIONI PER IL CONSENSO**

L'interessato ha il diritto di revocare il consenso di qualsiasi momento. La revoca non pregiudica la liceità del trattamento basata sul consenso prima della revoca

Esclusione di ogni forma di consenso tacito (il silenzio non equivale al consenso) oppure ottenuto proponendo all'interessato una serie di opzioni già preselezionate

Consenso esplicito per trattare dati sensibili





# TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI

Art. 9 , Considerando 51

Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Decreto  
ITALIA



Ex Dati Sensibili



## TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI

Il regolamento vieta il trattamento dei dati particolari, salvo quando ricorrono specifiche condizioni:

- 1) Consenso espresso per finalità specifiche
- 2) Necessità di osservare obblighi in materia di diritto di lavoro, sicurezza sociale, protezione sociale
- 3) Trattamento effettuato da organismo non a scopo di lucro con finalità politiche, religiose, filosofiche, sindacali
- 4) Dati resi manifestamente pubblici dall'interessato
- 5) Necessità di accertare, esercitare o difendere un diritto in sede giudiziaria
- 6) Interesse pubblico sulla base dell'ordinamento europeo o interno
- 7) Trattamenti sanitari
- 8) Ricerca scientifica, storica e statistica



# TRATTAMENTI DI DATI PERSONALI RELATIVI A CONDANNE PENALI O REATI

## Art. 10

Deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

- Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

Decreto  
ITALIA





# CAPO 3 DIRITTI DELL'INTERESSATO



# INFORMAZIONI, COMUNICAZIONI E MODALITÀ TRASPARENTI PER L'ESERCIZIO DEI DIRITTI DELL'INTERESSATO

## Articolo 12 (Cons. 58, 60, 64)

Comma 1: Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni ... e le comunicazioni ... relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.



## INFORMAZIONI, COMUNICAZIONI E MODALITÀ TRASPARENTI PER L'ESERCIZIO DEI DIRITTI DELL'INTERESSATO

### Comma 3:

Articolo 12 (Cons. 58, 60, 64)

Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta .... senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.



### **Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato**

1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:
  - a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
  - b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
  - c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;



## INFORMAZIONE E ACCESSO AI DATI PERSONALI

### Articolo 13 (Cons. 60, 62)

- d) qualora il trattamento rientra ..., i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione ..., il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.





# INFORMAZIONE E ACCESSO AI DATI PERSONALI

## Articolo 13 (Cons. 60, 62)

2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

a) Il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;



## INFORMAZIONE E ACCESSO AI DATI PERSONALI

### Articolo 13 (Cons. 60, 62)

- c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- d) il diritto di proporre reclamo a un'autorità di controllo;
- e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;



## INFORMAZIONE E ACCESSO AI DATI PERSONALI

### Articolo 13 (Cons. 60, 62)

f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.



## RETTIFICA E CANCELLAZIONE

Articolo 15 (Cons. 63, 64)  
Diritto di accesso dell'interessato

Articolo 16 (Cons. 65)  
Diritto di rettifica

Articolo 17 (Cons. 65, 66)  
Diritto alla cancellazione  
(«diritto all'oblio»)

Se il trattamento non  
è più necessario



Articolo 18 (Cons. 67)  
Diritto di limitazione di trattamento



## RETTIFICA E CANCELLAZIONE

### Articolo 19 (Cons. 31)

#### **Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento**

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate ..., salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.



## RETTIFICA E CANCELLAZIONE

### Articolo 20 (Cons. 68)

#### **Diritto alla portabilità dei dati**

1. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:
  - a) il trattamento si basi sul consenso o su un contratto; e
  - b) il trattamento sia effettuato con mezzi automatizzati.
2. Nell'esercitare i propri diritti relativamente alla portabilità dei ..., l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare ...all'altro...





# CAPO 4

## TITOLARE DEL TRATTAMENTO E RESPONSABILE DEL TRATTAMENTO



# RESPONSABILITÀ DEL TITOLARE

Art. 24 RESPONSABILITÀ DEL TITOLARE

FORMAZIONE E CONSAPEVOLEZZA

Tenendo conto di:  
Contesto  
Finalità  
Rischi per i diritti e  
libertà dei soggetti

Mette in atto  
misure tecniche ed  
organizzative

Per  
Dimostrare  
Garantire

Trattamento  
conforme al reg.  
679/2016 UE





# PRIVACY BY DESIGN E BY DEFAULT

Art. 25 DALLA PROGETTAZIONE ALLA PROTEZIONE



# PRIVACY BY DESIGN E BY DEFAULT

Art. 25 DALLA PROGETTAZIONE ALLA PROTEZIONE

## Privacy by design:

Previsione di misure a protezione dei dati **già al momento della progettazione** di un prodotto o di un software



## Privacy by default:

Il responsabile del trattamento mette in atto opportune misure per garantire che siano trattati, **di default**, solo **i dati personali necessari** per ogni specifica finalità del trattamento; ciò vale per la quantità dei dati raccolti, l'estensione del trattamento, il periodo di conservazione e la loro accessibilità.



# PRIVACY BY DESIGN E BY DEFAULT

## Art. 25 DALLA PROGETTAZIONE ALLA PROTEZIONE

1. Tenendo conto dello **stato dell'arte** e dei **costi** di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei **rischi** aventi **probabilità** e **gravità** diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso **il titolare del trattamento mette in atto misure tecniche e organizzative adeguate**, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i **diritti degli interessati**.



# PRIVACY BY DESIGN E BY DEFAULT

## Art. 25 DALLA PROGETTAZIONE ALLA PROTEZIONE

2. **Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate** per garantire che siano trattati, **per impostazione predefinita**, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.



# RESPONSABILE DEL TRATTAMENTO

## Art. 28 RESPONSABILE DEL TRATTAMENTO

Il titolare "ricorre unicamente" a responsabili che presentino **garanzie** per mettere in atto:

**Misure Tecniche**  
**Misure Organizzative**



Trattamento soddisfa i requisiti del Regolamento

Certificazione



# CONTITOLARI DEL TRATTAMENTO

## Art. 26 CONTITOLARI DEL TRATTAMENTO

Due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento.

→ Essi sono **Contitolari** del trattamento



# CONTITOLARI DEL TRATTAMENTO

## Art. 26 CONTITOLARI DEL TRATTAMENTO

Determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità.

L'accordo riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati.

La sintesi degli accordi è messa a disposizione degli interessati.

Indipendentemente da quanto disposto negli accordi, l'interessato può esercitare i propri diritti nei confronti e contro ciascun titolare del trattamento.



TITOLARE DEL TRATTAMENTO

RESPONSABILE DEL TRATTAMENTO

INCARICATI DEL TRATTAMENTO?

Non ci sono più gli incaricati, ma diventano addetti.  
Il GDPR richiama il termine “chiunque” che tratta i dati.  
L’addetto deve avere la formazione per trattare i dati.  
Anche i responsabili (esterni) dovranno essere idonei a trattare i dati ed autorizzati a farlo.

Chiunque agisce sotto l’autorità del titolare del trattamento deve essere istruito da esso sulle modalità di trattamento.

Decreto  
ITALIA





# INCARICATI DEL TRATTAMENTO

## Articolo 29

Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento (Cons. 81)

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare 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.



# REGISTRO DEL TITOLARE O DEL RESPONSABILE

## Art. 30 REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO

Cosa sono i registri del trattamento?



Adempimento formale, sostitutivo della  
notifica prevista dal Codice Privacy

Quali sono i registri del trattamento?



Registro del Titolare o suo rappresentante

Registro del Responsabile o suo rappresentante



# REGISTRO DEL TITOLARE DEL TRATTAMENTO

- a. Nome e i dati del titolare del trattamento, se del caso del contitolare, del rappresentante del titolare del trattamento
- b. Finalità
- c. Descrizione della categoria di interessati e delle categorie di dati personali
- d. Categorie di destinatari a cui verranno comunicati i dati (compresi paesi terzi o organizzazioni internazionali)
- e. Ove applicabile il trasferimento di dati personali verso un paese terzo
- f. Termini per la cancellazione
- g. Descrizione generale delle misure di sicurezza tecniche ed organizzative



# REGISTRO DEL RESPONSABILE DEL TRATTAMENTO

- a. Nome e i dati di contatto del responsabile (i) del trattamento, per ogni titolare del trattamento per cui il responsabile agisce
- b. Categorie di trattamenti effettuati per conto di ogni titolare
- c. I trasferimenti di dati personali verso un paese terzo, o un'organizzazione internazionale, compresa l'identificazione del paese terzo, e per i trasferimenti di cui al comma 2 dell'art. 49, la documentazione delle garanzie
- d. Descrizione generale delle misure di sicurezza tecniche ed organizzative



# REGISTRO DEL TITOLARE O DEL RESPONSABILE DEL TRATTAMENTO

## Obbligatorietà del registro dei trattamenti

Dipende dalla numerosità dei dipendenti dell'organizzazione:

$\geq 250$

- Sempre

$< 250$

- Rischio per diritti e libertà dell'interessato
- Trattamento non occasionale di dati sensibili o giudiziari



# VALUTAZIONE DEI RISCHI E SICUREZZA DEI DATI PERSONALI

Art. 32 – Sicurezza del trattamento (Considerando 83 )



# VALUTAZIONE DEI RISCHI E SICUREZZA DEI DATI PERSONALI

Art. 32 – Sicurezza del trattamento (Considerando 83 )

## Comma 1

Tenendo conto dello **stato dell'arte** e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del **rischio di varia probabilità e gravità** per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto **misure tecniche e organizzative adeguate** per garantire un **livello di sicurezza adeguato al rischio...**



# VALUTAZIONE DEL RISCHIO E SICUREZZA DEI DATI PERSONALI

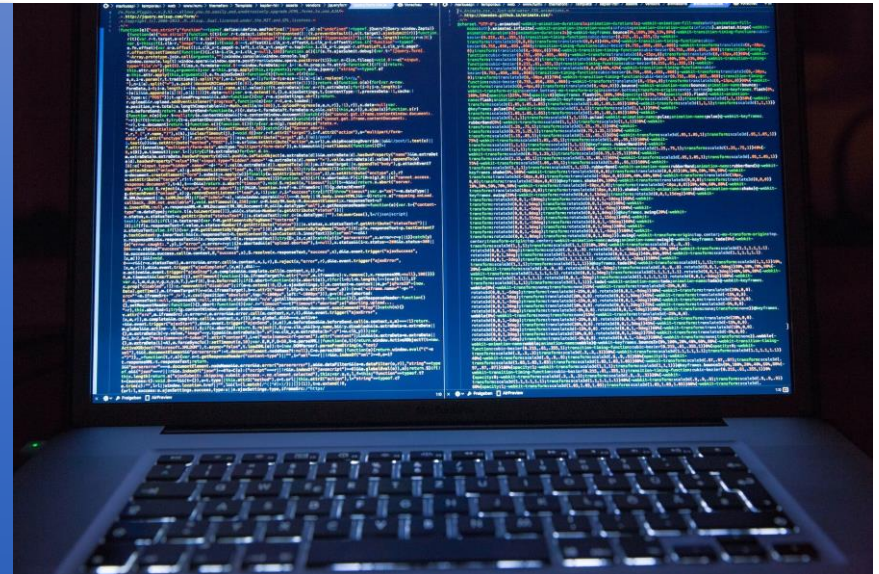
Art. 32 – Sicurezza del trattamento (Considerando 83 )





# VIOLAZIONE DI DATI PERSONALI (DATA BREACHES)

La distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso, in modo accidentale o illecito, ai dati personali trasmessi, memorizzati o comunque elaborati.



(artt. 33 e 34 considerando 85 e 86)



Potrebbe non essere colpa del titolare, ma deve dimostrarlo



# VIOLAZIONE DI DATI PERSONALI (DATA BREACHES)

## Notifica della violazione

In caso di una violazione dei dati personali, il Titolare deve mettere in atto:

- ✓ Non appena viene a conoscenza di un'avvenuta violazione, deve notificare senza ingiustificato ritardo all'Autorità di Controllo
- ✓ Se possibile entro 72 ore dal fatto



**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**



# VIOLAZIONE DI DATI PERSONALI (DATA BREACHES)

## Notifica della violazione

Qualora la notifica non sia effettuata entro le previste- 72 ore, deve essere accompagnata dai motivi del ritardo.

Il Titolare deve documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio e mettere su richiesta a disposizione del garante la relativa documentazione.



**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**



# VIOLAZIONE DI DATI PERSONALI (DATA BREACHES)

## Comunicazione di una violazione all'interessato

- **Segnalazione al diretto interessato (senza ritardo ingiustificato)**

Quando la violazione dei dati personali è suscettibile di presentare un **rischio elevato per i diritti e le libertà** delle persone fisiche, il Titolare deve comunicare la violazione anche all' interessato, senza ingiustificato ritardo, descrivendola con un linguaggio semplice e chiaro.

*(salve circostanze al verificarsi delle quali la comunicazione è esclusa\*)*



# Come può essere utile il CRM per il GDPR?

- ✓ Il CRM gestisce quasi tutti gli attori dell'organizzazione (dipendenti e collaboratori interni, persone che rappresentano i clienti, contatti/leads, ecc.)
- ✓ È possibile classificare il «contatto» in base al rapporto che ha con l'organizzazione (cliente con rapporto contrattuale, contatto commerciale, ecc.)
- ✓ Può gestire in modo selettivo l'invio di comunicazioni a tutti i contatti, comprendendo anche l'informativa al trattamento dei dati personali
- ✓ Può memorizzare consensi, richieste di cancellazione da newsletter, richieste di limitazioni del trattamento, cancellazioni di dati, rettifiche...



# Come può essere utile il CRM per il GDPR?

Il CRM, tramite sviluppo di apposite funzioni/moduli può gestire diverse attività necessarie per ottemperare al GDPR:

- Redazione ed aggiornamento del **registro dei trattamenti**
- **Gestione documentale** relativa alla privacy con distribuzione controllata ai soggetti interessati: informative, procedure, istruzioni, nomine incaricati/autorizzati al trattamento, nomine responsabili esterni al trattamento, modulistica per la raccolta di consensi,....
- Gestione delle anagrafiche dei **responsabili esterni al trattamento** con relativi documenti contrattuali, istruzioni, verifiche, ecc.



# Come può essere utile il CRM per il GDPR?

- Registrazione e gestione di **data breach** o degli incidenti di sicurezza delle informazioni
- Gestione della **valutazione dei rischi privacy**: identificazione dei rischi, delle minacce, delle vulnerabilità, analisi e ponderazione dei rischi, gestione delle azioni di trattamento dei rischi
- Gestione delle politiche di **conservazione e cancellazione dei data** (*data retention*)



# Come può essere utile il CRM per il GDPR?

In generale un uso disciplinato del CRM permette di raccogliere i dati personali dei clienti effettivi e potenziali in un unico database, evitando la proliferazione di soluzioni personalizzate tramite liste, stampe, file Excel che provocano una duplicazione dei dati dei clienti con il rischio del proliferare di errori e di non riuscire a tenere sotto controllo le modifiche e le cancellazioni dei dati che costituiscono un diritto dell'interessato







Ing. Fabrizio Di Crosta  
CONSULENZA DIREZIONALE DI IMPRESA



Grazie per l'attenzione

