

# Il nuovo Regolamento Europeo sulla protezione dei dati personali

## Registro trattamenti - Sanzioni

Trento, 16 novembre 2017

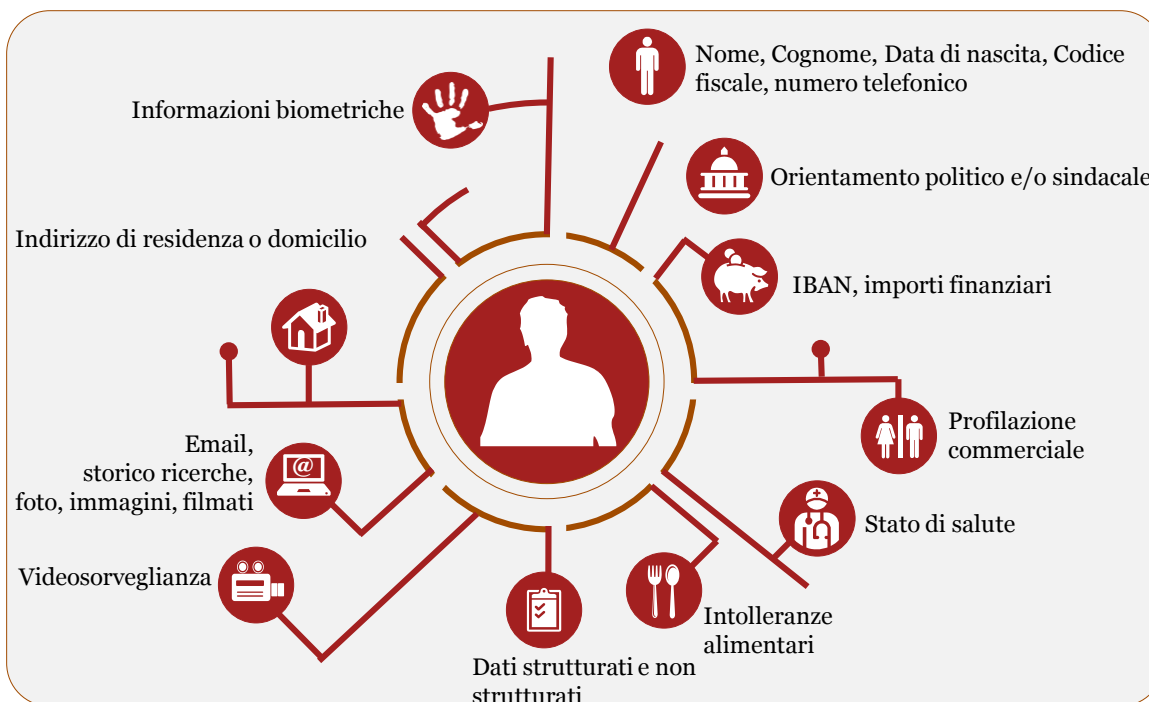
Avv. Stefano Cancarini

# I Dati Personali

## Cosa si intende per dato personale?

**"Dato Personale"**: qualsiasi informazione riguardante una persona fisica identificata o identificabile [...] con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

[Art.4 Definizioni – GDPR]



Esempi di trattamenti:

- Registrazione del dato per antiriciclaggio; ✓
- Invio di una comunicazione informativa al cliente in EU; ✓
- Reportistica sui dati finanziari del gruppo; ✗
- Pagamento dello stipendio di un dipendente; ✓
- Pagamento ad un fornitore persona giuridica; ✗
- Invio di una comunicazione informativa al cliente extra EU; ✓

# Il nuovo Regolamento sulla Privacy

## Il Regolamento Europeo sulla protezione dei dati personali (GDPR)

Il 14 aprile 2016 il Parlamento e il Consiglio Europeo hanno approvato in via definitiva il **Regolamento 679/2016** in materia di protezione dei dati personali (GDPR).



### Perché?

Un passo determinante per il superamento della frammentazione normativa che ha caratterizzato il panorama europeo e per l'adattamento alla evoluzione tecnologica.



### Quando?

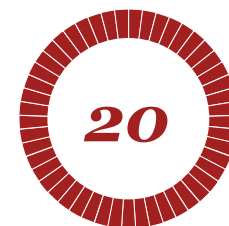
E' stato concesso un "grace period" di 2 anni dall'entrata in vigore sino al 25 maggio 2018 per implementare i cambiamenti necessari a garantire la conformità ai requisiti del nuovo Regolamento.



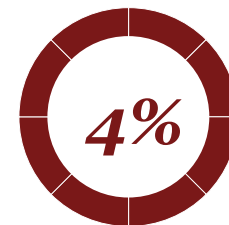
### Chi?

La riforma coinvolge tutti i soggetti stabiliti in Stati UE o che offrono beni o servizi a soggetti ivi localizzati.

## Sanzioni



Milioni di Euro



Fatturato mondiale  
annuo

# Il GDPR in pillole

## Perimetro

La riforma coinvolge tutti gli Stati UE (sostituendo le singole legislazioni nazionali) e chiunque tratti dati di cittadini europei (a prescindere dalla localizzazione sede legale del titolare del trattamento)

## Responsabilità

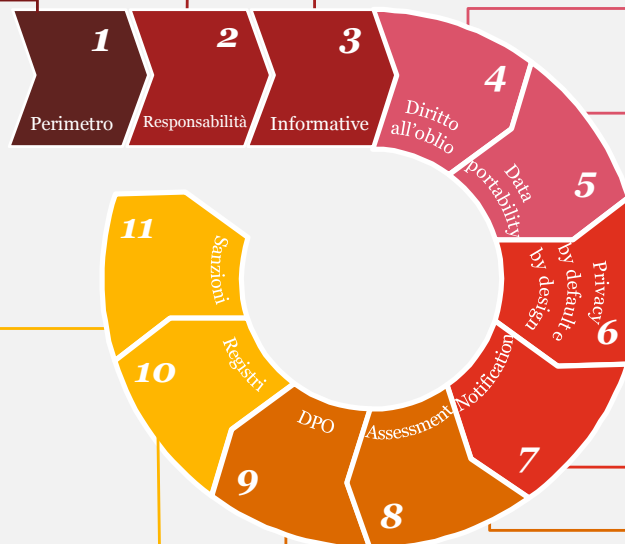
Viene disciplinato in modo più dettagliato il ruolo di responsabile del trattamento, il contenuto del contratto di nomina e le relative responsabilità, anche dirette nei confronti degli interessati

## Informative chiare

Viene rafforzato l'obbligo di fornire informative semplici e chiare al fine di rafforzare il controllo degli interessati rispetto al trattamento dei propri dati personali

## Diritto all'oblio

La riforma introduce il diritto dell'interessato di ottenere dal titolare del trattamento la cancellazione dei dati personali al ricorrere di determinate specifiche ipotesi



## Data portability

Viene introdotto il diritto alla portabilità del dato che permette all'interessato di ricevere i propri dati su un formato strutturato e leggibile e/o di farli trasmettere da un titolare all'altro

## Privacy by design & by default

Il titolare deve implementare misure idonee a proteggere i dati sin dal momento di determinazione dei mezzi di trattamento (privacy by design) e garantire solo il trattamento dei dati necessari al perseguimento di specifiche finalità per cui sono raccolti (privacy by default)

## Data breach notification

Viene previsto che determinate violazioni di dati debbano essere segnalate sia al Garante che agli interessati senza ritardo e, in alcuni casi, entro 72 ore dalla violazione.

## Sanzioni

La riforma ha incrementato in modo molto significativo le sanzioni derivanti dall'inosservanza delle disposizioni in tema di privacy, sino ad un massimo di € 20.000.000 o al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore

## Registri del trattamento

Il regolamento introduce l'obbligo per il titolare e il responsabile del trattamento di conservare, anche in formato elettronico, un registro dei trattamenti effettuati, contenente alcuni specifici dettagli

## Data Protection Officer

Viene introdotta, per talune tipologie di titolari, la figura del Data Protection Officer (DPO), che ha i compiti di sorvegliare l'osservanza delle disposizioni privacy, fornire consulenza e pareri e fungere da contatto con il Garante o gli interessati

## Privacy Impact Assessment

Viene introdotto l'obbligo per ciascun titolare di svolgere, e di conseguenza documentare, una autovalutazione del rischio derivante dai trattamenti effettuati e, sulla base degli esiti delle analisi, di effettuare una consultazione preventiva con l'Autorità garante

# Il Registro delle attività di trattamento

DESCRIZIONE DEL TRATTAMENTO												
ID Trattamento	ID Sub. Trattamento	Finalità del Trattamento	Descrizione del Trattamento (Sub. Trattamento ove applicabile)	Ruolo di [=] (Titolare / Responsabile)	Indicazione del Titolare (ove [=] fosse anche Responsabile)	Categorie di interessati	Categorie di interessati minorenni	Categorie di dati personali				Termine ultimo per la cancellazione del dato
								Comuni	Finanziari / Patrimoniali (cons. 78)	Sensibili (art. 9)	Giudiziari (art. 10)	

SOGGETTI COINVOLTI NEL TRATTAMENTO																			
Responsabile interno del trattamento	Funzione di riferimento	Funzione di supporto	Responsabili esterni del trattamento					Sub-responsabile	Presupposto di trasferimento in paesi extra UE			Destinatari dei dati in qualità di titolari autonomi (es. Banca d'Italia, Amministrazione Finanziaria, UIF)			Presupposto di trasferimento in paesi extra UE				
			UE		Extra UE				Consenso	Decisione di adeguatezza	BCR/CMC	UE		Extra UE			Consenso	Decisione di adeguatezza	BCR/CMC
			Nome	Finalità della comunicazione	Nome	Destinazione	Finalità della comunicazione					Nome	Finalità della comunicazione	Nome	Destinazione	Finalità della comunicazione			

LOCALIZZAZIONE DEI DATI E MISURE DI SICUREZZA ASSOCIATE												
Applicazioni	Data Base	Supporto utilizzato			Misure di sicurezza		Condizione di liceità del trattamento (art. 6)				Data Protection Impact Assessment (art. 35)	
		Cartaceo	Localizzazione Cartaceo	Informatico	Tecniche	Organizzative	Consenso	Esecuzione contratto	Obbligo di legge	Legittimo interesse		

# Sanzioni ai sensi del GDPR

## Sanzioni amministrative pecuniarie (articolo 83 GDPR)

Fino a **€ 20 milioni** o al **4%** del fatturato **mondiale** totale annuo dell'esercizio precedente, se superiore

In caso di violazione delle disposizioni in materia di, tra le altre:

- ✓ **principi generali** applicabili al trattamento;
- ✓ **condizioni di liceità del trattamento;**
- ✓ trattamento di **categorie particolari di dati;**
- ✓ **diritti dell'interessato;**
- ✓ **trasferimento** dei dati extra UE;
- ✓ norme nazionali in tema di rapporti di lavoro;
- ✓ inosservanza di un ordine da parte dell'autorità di controllo.

Fino a **€ 10 milioni** o al **2%** del fatturato **mondiale** totale annuo dell'esercizio precedente, se superiore

In caso di violazione delle disposizioni in materia di, tra le altre:

- ✓ trattamento dei dati di minori;
- ✓ *Privacy by Design / Privacy by Default;*
- ✓ mansioni e responsabilità del **responsabile del trattamento;**
- ✓ **registro** delle attività di trattamento;
- ✓ **misure di sicurezza** adeguate;
- ✓ notifica al Garante di una **violazione dei dati personali** e/o comunicazione della stessa agli interessati;
- ✓ **DPIA;**
- ✓ designazione del **DPO** e adempimenti connessi.

# Sanzioni ai sensi del GDPR

<b>Condizioni generali per infliggere sanzioni amministrative pecuniarie (art. 83, paragrafo 2, GDPR) Interpretazioni dell'Article 29 Data Protection Working Party</b>			
<b>a</b>	<b>Natura, gravità e durata</b> della violazione tenendo in considerazione la natura, oggetto, o finalità del trattamento, nonché il numero di interessati lesi dal danno e il livello del danno subito	<b>f</b>	Grado di <b>cooperazione con il Garante</b> al fine di porre rimedio alla violazione e attenuare i danni
<b>b</b>	Carattere <b>doloso o colposo</b> della violazione	<b>g</b>	<b>Categorie di dati personali</b> interessate dalla violazione
<b>c</b>	<b>Misure adottate</b> dal titolare <b>per attenuare il danno</b> subito dagli interessati	<b>h</b>	Maniera in cui l'autorità di controllo ha preso conoscenza della violazione e, in particolare, se è stata <b>notificata</b> dal titolare
<b>d</b>	Grado di responsabilità del titolare, tenuto conto delle <b>misure tecniche ed organizzative adottate</b> ai sensi degli articoli 25 e 32	<b>i</b>	Precedente disposizioni di <b>provvedimenti ex articolo 58, par. 2, GDPR</b> relativamente allo stesso oggetto e il loro rispetto da parte del titolare
<b>e</b>	<b>Precedenti violazioni pertinenti</b> commesse	<b>j</b>	Adesione ai <b>codici di condotta</b> o ai <b>meccanismi di certificazione</b>