www.pwc.com

Il nuovo Regolamento Europeo sulla protezione dei dati personali

Registro trattamenti - Sanzioni

Trento, 16 novembre 2017

Avv. Stefano Cancarini

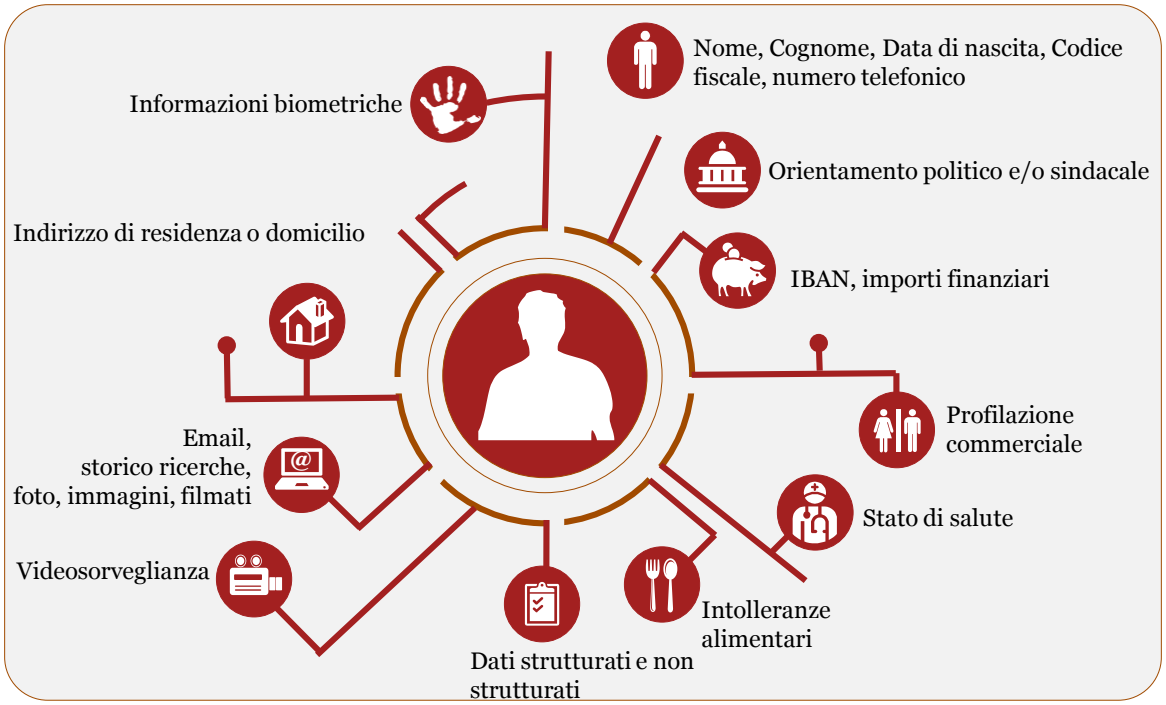
pwc

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

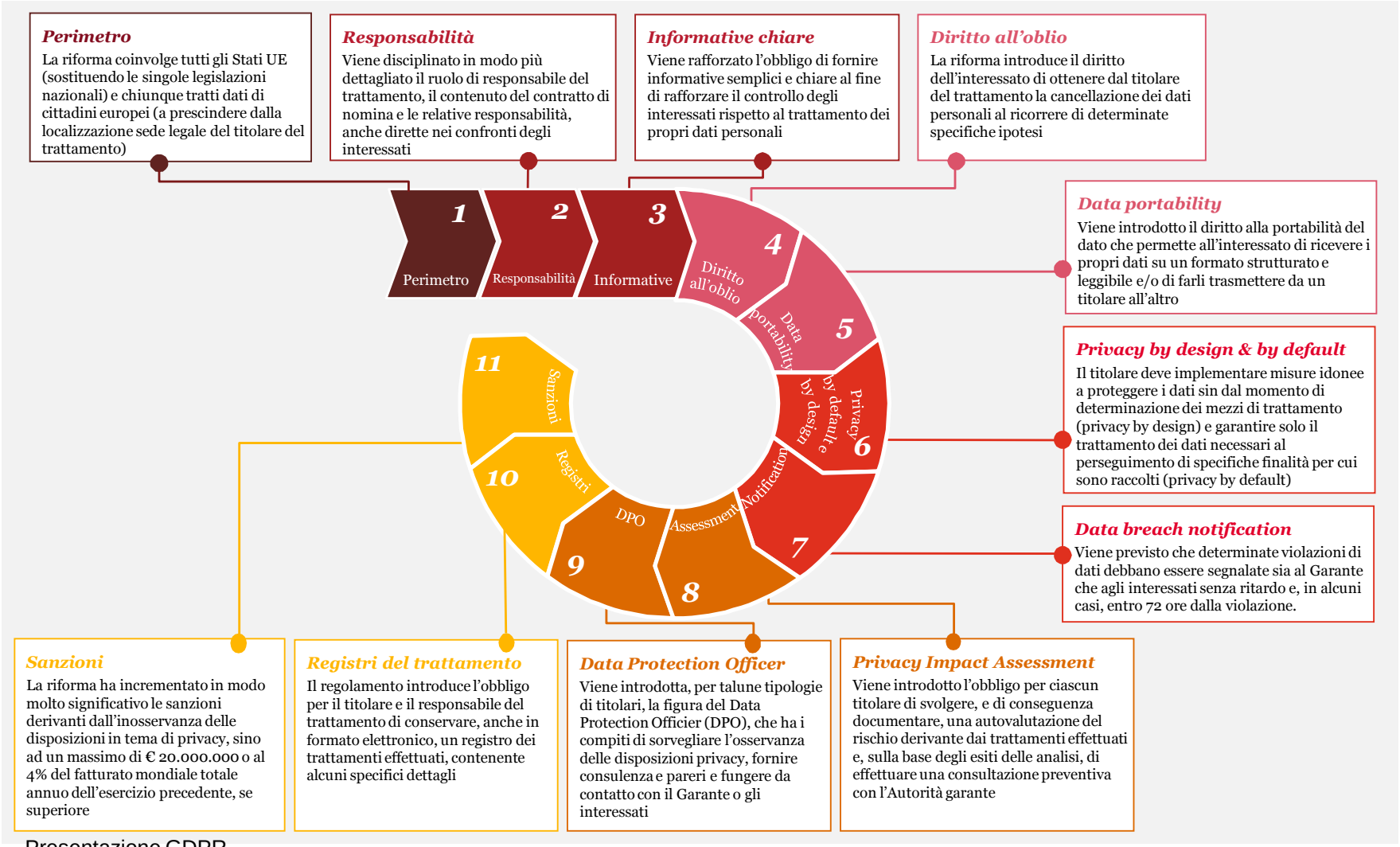
20

Milioni di Euro

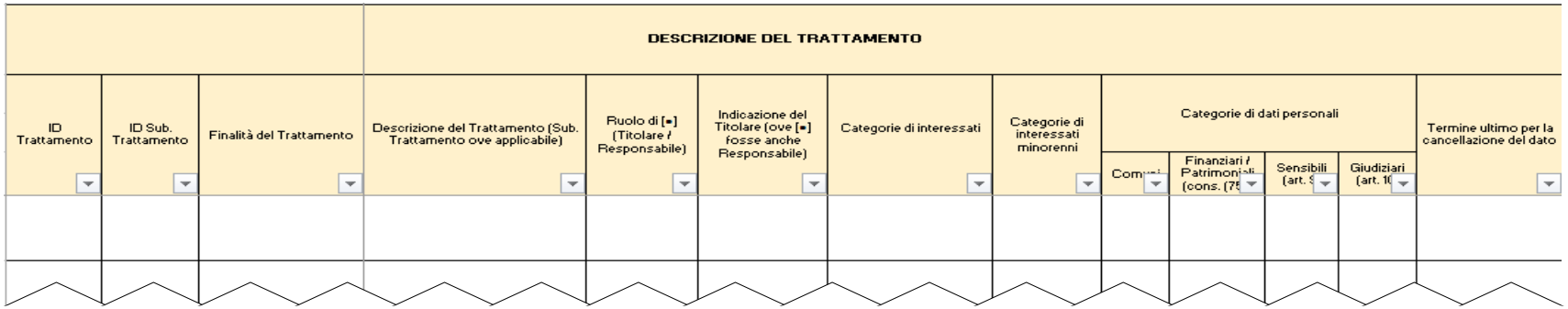
4%

Fatturato mondiale annuo

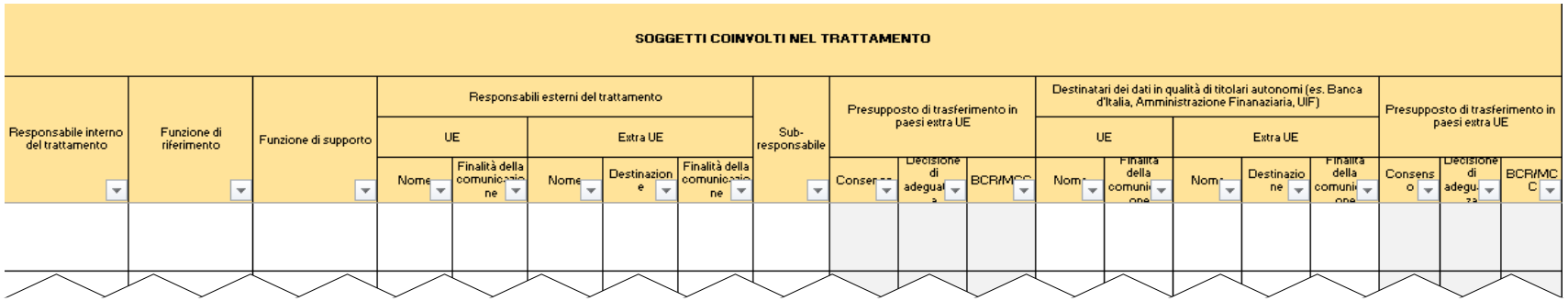
Il GDPR in pillole



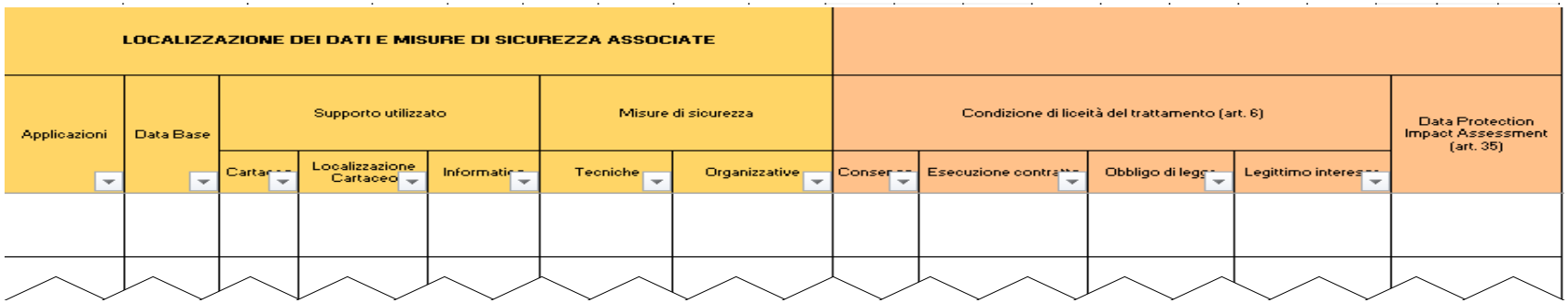
Il Registro delle attività di trattamento



			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. (75	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 Finanaziaria, UIF)					Presupposto di trasferimento in paesi extra UE		
			UE		Extra UE							UE		Extra UE					
			Nome	Finalità della comunicazione	Nome	Destinazione	Finalità della comunicazione		Consenso	Decisione di adeguatezza	BCR/MCC	Nome	Finalità della comunicazione	Nome	Destinazione	Finalità della comunicazione	Consenso	Decisione di adeguatezza	BCR/MCC



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	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: ✓ **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.	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

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