PRINCIPI GENERALI DEL GDPR 2016/679
e novità salienti

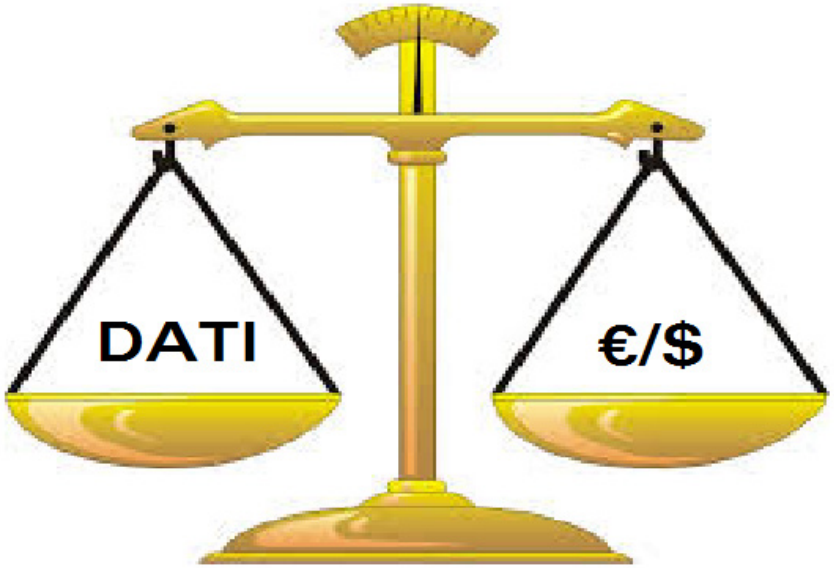
Dott. Emanuele Vettorello (vice presidente ASSO DPO)

Milano 12 marzo 2018

PRINCIPI GENERALI DEL GDPR 2016/679

⇨QUESITO: Qual è il valore dei dati?

Attribuite un valore ….



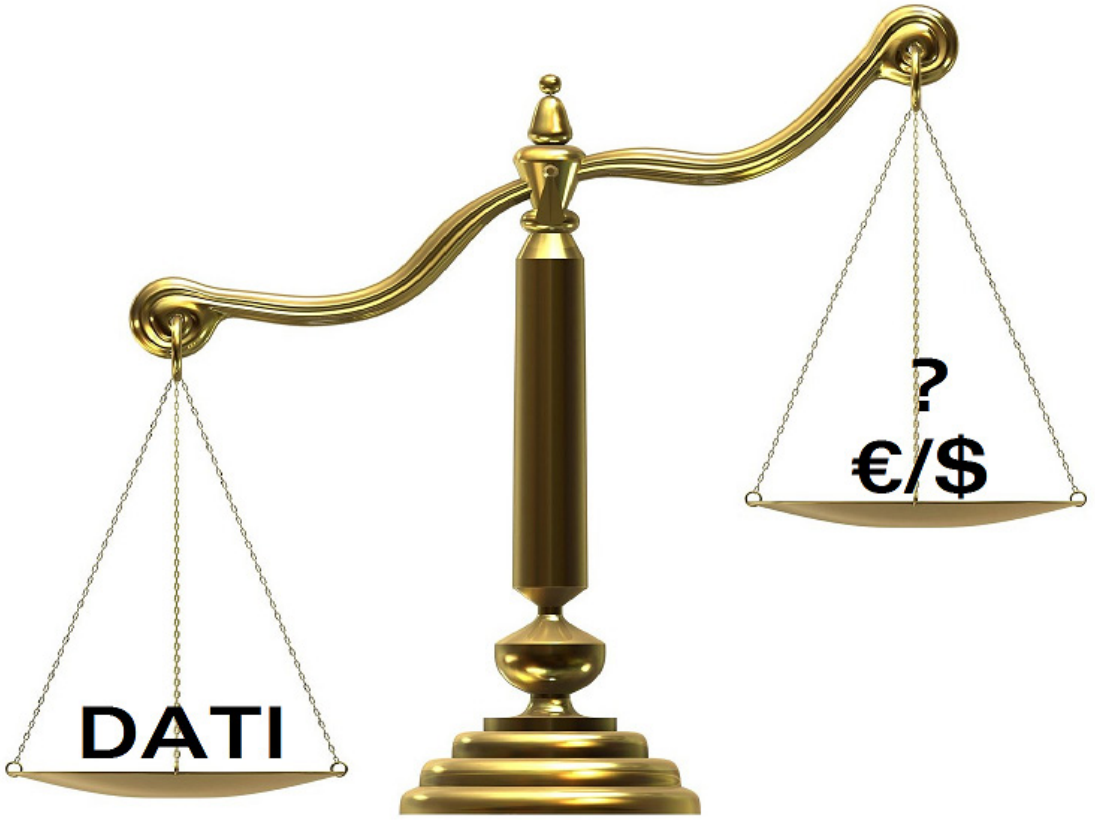
The INTERNATIONAL COUNCIL OF MANAGEMENT CONSULTING INSTITUTES
CMC - GLOBAL

Organismo accreditato per la qualificazione
CMC
CERTIFIED MANAGEMENT CONSULTANT

RISPOSTA AL QUESITO:

PRINCIPI GENERALI DEL GDPR 2016/679

E' INQUANTIFICABILE



The INTERNATIONAL COUNCIL OF MANAGEMENT CONSULTING INSTITUTES
CMC - GLOBAL

Organismo accreditato per la qualificazione
CMC
CERTIFIED MANAGEMENT CONSULTANT

PRINCIPI GENERALI DEL GDPR 2016/679 – evoluzione normativa

DIRETTIVA EUROPEA
24 ottobre 1995
95/46/CE

→ **CON OBBLIGO PER GLI STATI MEMBRI DI GARANTIRE SICUREZZA DEI DATI PERSONALI**

↓

recepita in Italia con → **Legge 31 dicembre N. 675/96**

abrogata e sostituita con

CODICE PRIVACY
D.LGS 196/2003

↓

Cd. *Pacchetto protezione dati:*

REGOLAMENTO EUROPEO
del 27/04/2016
Pubblicazione in GU Ue il 4 maggio 2016

Entrata in vigore dal

25 maggio 2016

→ **IL REGOLAMENTO EUROPEO 2016/679** *ABROGA la Direttiva 95/46/CE . Si applica a decorrere dal 25 maggio 2018*

→ **DIRETTIVA EUROPEA 2016/680** *SOSTITUISCE la Direttiva 95/46/CE. Gli Stati membri adottano e pubblicano, entro il 6 maggio 2018, le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla nuova direttiva. Deroga per motivi eccezionali entro il 6 maggio 2023*

→ **DIRETTIVA EUROPEA 2016/681** *del 27 aprile 2016 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi. In vigore a decorrere dal 24 maggio 2016*

PRINCIPI GENERALI DEL GDPR 2016/679 – evoluzione normativa

Linee Guida sul diritto alla portabilità dei dati 16/EN W9 242 rev.01 WP 29	Adottate il 13 dicembre 2016 ed emendata e adottata il 5 aprile 2017
Linee Guida sui DPO 16/EN W9 243 rev.01 WP 29	Adottate il 13 dicembre 2016 ed emendata e adottata il 5 aprile 2017
Linee Guida per l'individuazione dell'Autorità di controllo capofila in rapporto a uno specifico TDT o RDT 16/EN W9 244 rev.01 WP 29	Adottate il 13 dicembre 2016 ed emendata e adottata il 5 aprile 2017
Opinione 2/2017 sul trattamento dei dati sul posto di lavoro 17/EN WP 249 WP 29	Adottata l'8 giugno 2017
Linee guida sul processo decisionale e profiling automatizzato individuale ai fini del Regolamento 2016/679 17/EN W 251 WP 29	Adottate il 3 ottobre 2017

PRINCIPI GENERALI DEL GDPR 2016/679 – evoluzione normativa

Linee guida sulla valutazione dell'impatto sulla protezione dei dati (DPIA) e sulla determinazione se la trasformazione "rischia di provocare un rischio elevato" ai fini del regolamento 2016/679
17/EN WP 248 rev. 01
WP 29

→ Approvato il 4 aprile 2017 Come ultimo aggiornato e adottato il 4 ottobre 2017

Linee guida sulla notifica di violazione dei dati personali ai sensi del regolamento 2016/679 (DATA BREACH)
17/EN WP 250
WP 29

→ adottato il 3 ottobre 2017

PRINCIPI GENERALI DEL GDPR 2016/679 – evoluzione normativa

Linee guida Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE) n. 2016/67917/IT WP 253 WP 29

→ **adottato il 3 ottobre 2017**

CONSENSO → in progress

consultazione pubblica delle Linee guida elaborate da WP29 in materia di **consenso**, definite in base alle previsioni del GDPR 2016/679

TRASPARENZA → in progress

consultazione pubblica delle Linee guida elaborate da WP29 in materia di **trasparenza**, definite in base alle previsioni del GDPR 2016/679

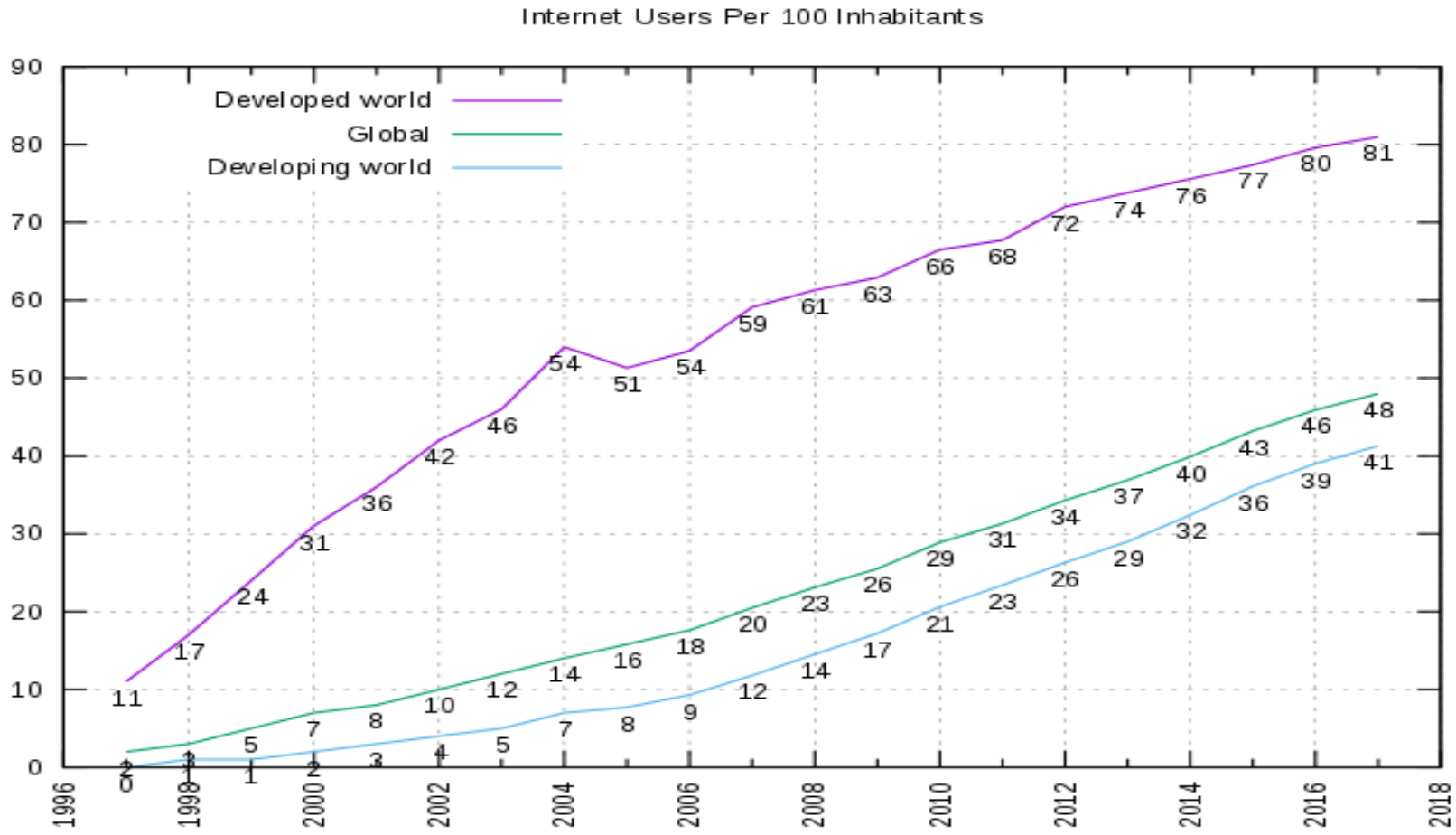
ACCREDITAMENTO ORGANISMI DI CERTIFICAZIONE → in progress

consultazione pubblica delle Linee guida elaborate da WP29 in materia di **accreditamento** degli organismi di certificazione, definite in base alle previsioni del GDPR 2016/679

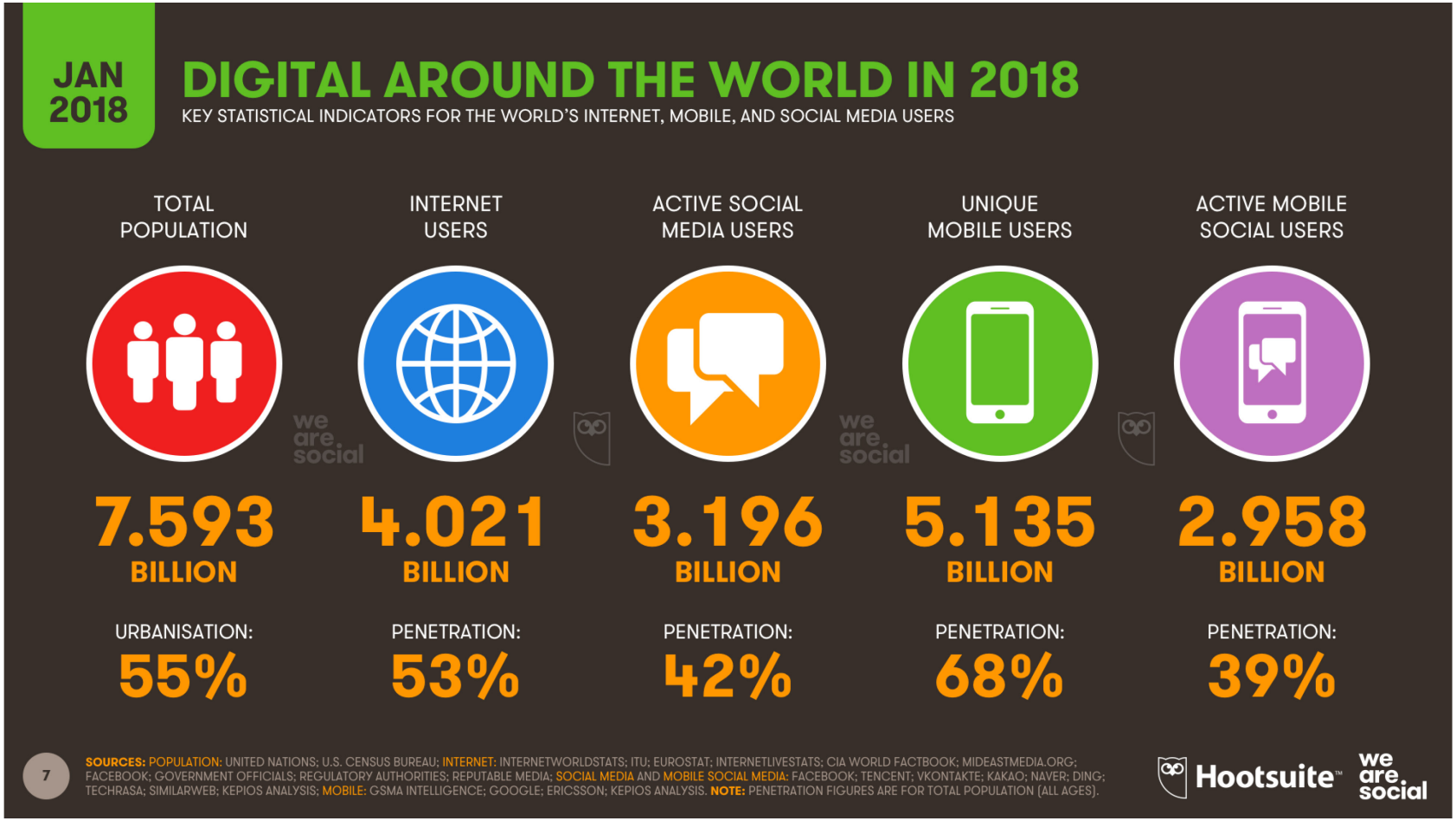
⇨QUESITO: perché il GDPR 2016/679 ?

RISPOSTA AL QUESITO:

PRINCIPI GENERALI DEL GDPR 2016/679



PRINCIPI GENERALI DEL GDPR 2016/679



IOT

INTERNET OF THINGS

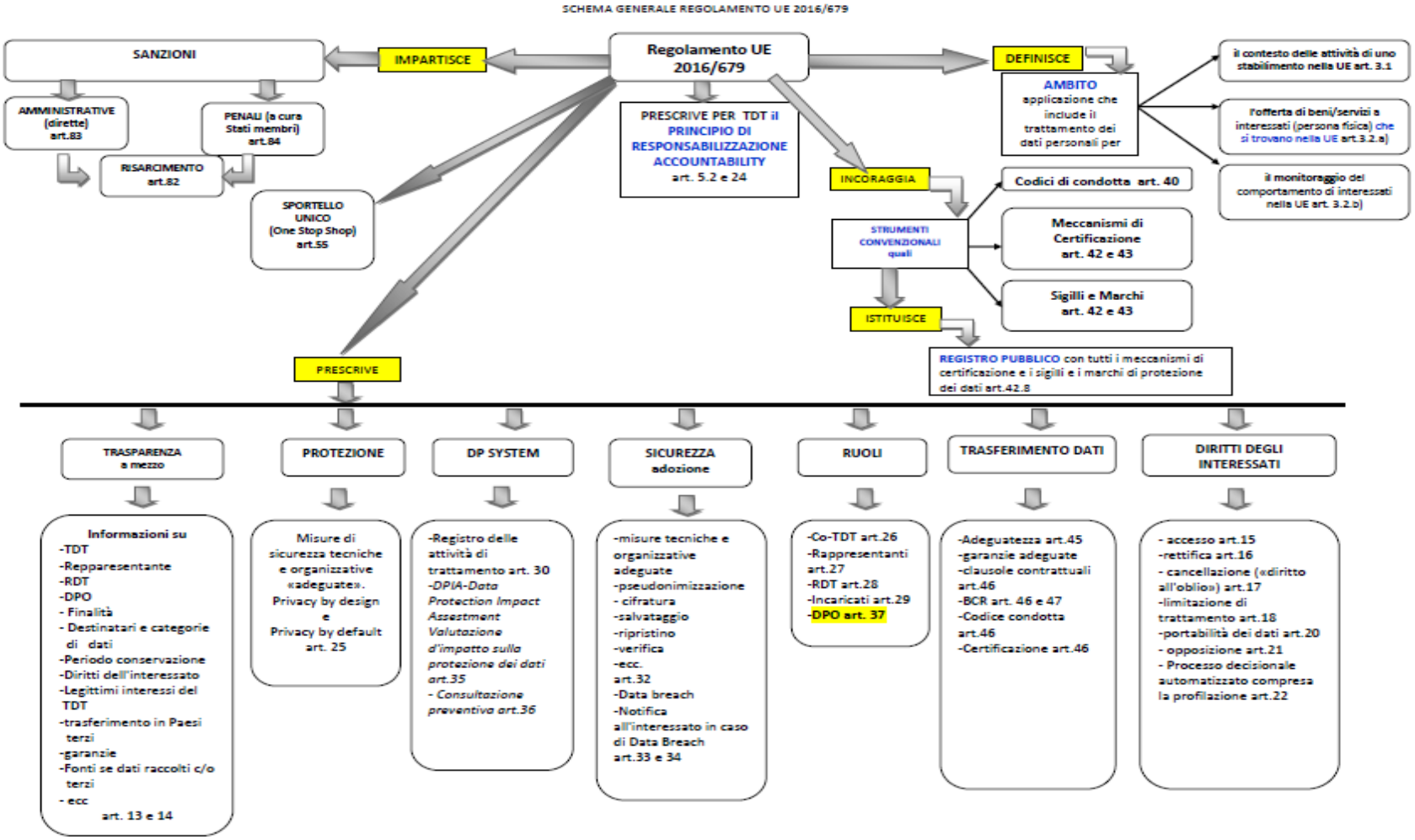
PRINCIPI GENERALI DEL GDPR 2016/679

= PROTEZIONE DEI DATI PERSONALI

= TUTELA DELLA PRIVACY

= NECESSITA' DI ARMONIZZAZIONE UE

PRINCIPI GENERALI DEL GDPR 2016/679



PRINCIPI GENERALI DEL GDPR 2016/679

COSA CAMBIA

- FONDAMENTI DI LICEITA' DEL TRATTAMENTO
- INFORMATIVA
- DIRITTI DEGLI INTERESSATI
- TITOLARE, RESPONSABILE, INCARICATO DEL TRATTAMENTO
- REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO
- REGISTRO DEI DATA BREACH
- DPIA - DATA PROTECTION IMPACT ASSESSMENT
- DPO – DATA PROTECTION OFFICER
- APPROCCIO BASATO SUL RISCHIO E MISURE DI ACCOUNTABILITY (RESPONSABILIZZAZIONE) DI TITOLARI E RESPONSABILI
- SEMPLIFICAZIONI
- SISTEMA SANZIONATORIO

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA FONDAMENTI DI LICEITA' DEL TRATTAMENTO

Il GDPR CONFERMA che ogni trattamento deve trovare fondamento in un'idonea base giuridica; i **fondamenti di liceità del trattamento** sono indicati all'art. 6 e coincidono, in linea di massima, con quelli previsti attualmente dal Codice privacy - d.lgs. 196/2003 (**consenso**, adempimento obblighi contrattuali, **interessi vitali della persona interessata o di terzi**, obblighi di legge cui è soggetto il titolare, **interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi** cui i dati vengono comunicati).

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA FONDAMENTI DI LICEITA' DEL TRATTAMENTO

CONSENSO nel GDPR, il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: (C40)

a)	l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; (C42, C43)
b)	il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; (C44)
c)	il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; (C45)
d)	il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; (C46)
e)	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; (C45, C46)

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA FONDAMENTI DI LICEITA' DEL TRATTAMENTO

CONSENSO nel GDPR, il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: (C40)

f)	il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. (C47-C50)
	In particolare
⇨	- Per i "dati particolari " (ex sensibili) il consenso DEVE essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – art. 22). [Sono attualmente in consultazione pubblica, le Linee - guida in materia di profilazione e decisioni automatizzate recentemente pubblicate dal Gruppo "Articolo 29" (WP 251)]
⇨	- NON deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i dati particolari); inoltre, il titolare (art. 7.1) **DEVE** essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.
⇨	- Il consenso dei minori è valido a partire dai 16 anni; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA FONDAMENTI DI LICEITA' DEL TRATTAMENTO

INTERESSE VITALE DI UN TERZO	Si può invocare tale base giuridica **solo** se nessuna delle altre condizioni di liceità può trovare applicazione *(si veda considerando 46)*
INTERESSE LEGITTIMO PREVALENTE DI UN TITOLARE O DI UN TERZO	Il **bilanciamento** fra legittimo interesse del titolare o del terzo e diritti e libertà dell'interessato **NON SPETTA** all'Autorità ma **è compito dello stesso titolare**; si tratta di una delle principali espressioni del principio di «**responsabilizzazione**» introdotto dal nuovo pacchetto protezione dati.

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA INFORMATIVA

CONTENUTI DELL'INFORMATIVA	Sono **elencati in modo tassativo** negli artt. 13, paragrafo 1, e 14, paragrafo 1, del GDPR e in parte sono più ampi rispetto al Codice.
in particolare il titolare DEVE SEMPRE specificare	
⇨	i dati di contatto del RPD-**DPO** (Responsabile della protezione dei dati **- Data Protection Officer**), ove esistente
⇨	la base giuridica del trattamento, qual è il suo interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.).

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA INFORMATIVA

CONTENUTI DELL'INFORMATIVA	Sono **elencati in modo tassativo** negli artt. 13, paragrafo 1, e 14, paragrafo 1, del GDPR e in parte sono più ampi rispetto al Codice.
in particolare il titolare DEVE SEMPRE specificare	
Il GDPR prevede anche ulteriori informazioni in quanto "**necessarie per garantire un trattamento corretto e trasparente**"	
⇨	il titolare deve specificare: -il **periodo di conservazione dei dati** o i criteri seguiti per stabilire tale periodo di conservazione, e -il **diritto di presentare un reclamo** all'autorità di controllo.
⇨	Se il trattamento comporta ***processi decisionali automatizzati*** (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA DIRITTI DEGLI INTERESSATI

TEMPI DELL'INFORMATIVA	Nel caso di dati personali non raccolti direttamente presso l'interessato (art. 14 GDPR), l'informativa deve essere fornita: - **entro un termine ragionevole che non può superare 1 mese dalla raccolta**, oppure - **al momento della comunicazione** (NON della registrazione) **dei dati** (a terzi o all'interessato) (*diversamente da quanto prevede attualmente l'art. 13, comma 4, del Codice*).

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA INFORMATIVA

MODALITÀ DELL'INFORMATIVA	deve avere forma concisa (?!) , trasparente, intelligibile per l'interessato e facilmente accessibile; occorre utilizzare un linguaggio chiaro e semplice, e per i minori occorre prevedere informative idonee (C 58).
⇨	è data, **in linea di principio, per iscritto** e **preferibilmente in formato elettronico** (soprattutto nel contesto di servizi online: si vedano art. 12, paragrafo 1, e considerando 58), anche se sono ammessi "altri mezzi", quindi può essere fornita **anche oralmente**, ma nel rispetto delle caratteristiche di cui sopra (art. 12, paragrafo 1). Il regolamento ammette, soprattutto, l'**utilizzo di icone** per presentare i contenuti dell'informativa in forma sintetica, **ma solo "in combinazione"** con l'informativa estesa (art. 12, paragrafo 7); *queste icone dovranno essere identiche in tutta l'Ue e saranno definite prossimamente dalla Commissione europea.*

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA INFORMATIVA

ESONERO DELL'INFORMATIVA	Sono inoltre parzialmente diversi i requisiti che il GDPR fissa per l'esonero dall'informativa (si veda art. 13, paragrafo 4 e art. 14, paragrafo 5 del regolamento, oltre a quanto previsto dall'articolo 23, paragrafo 1, di quest'ultimo)
⇨	spetta al titolare, in caso di dati personali raccolti da fonti diverse dall'interessato, valutare se la prestazione dell'informativa agli interessati comporti uno **sforzo sproporzionato** (si veda art. 14, paragrafo 5, lettera b)) – a differenza di quanto prevede l'art. 13, comma 5, lettera c) del Codice.

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA DIRITTI DEGLI INTERESSATI

TERMINE PER LA RISPOSTA	Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), **1 mese, estendibili fino a 3 mesi in casi di particolare complessità**; il titolare deve comunque dare un riscontro all'interessato **entro 1 mese dalla richiesta, anche in caso di diniego**.
RISCONTRO ALL'INTERESSATO	Spetta al titolare: 1. valutare la complessità del riscontro all'interessato e 2. stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive (anche ripetitive) (art. 12.5) 3. ovvero se sono chieste più "copie" dei dati personali nel caso del diritto di accesso (art. 15, paragrafo 3); in quest'ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti.

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA TITOLARE, RESPONSABILE, INCARICATO DEL TRATTAMENTO

CONTITOLARITA' DEL TRATTAMENTO	impone ai titolari di definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti con particolare riguardo all'esercizio dei diritti degli interessati, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente; (art. 26)

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA TITOLARE, RESPONSABILE, INCARICATO DEL TRATTAMENTO

NOMINA DEL RISPOSABILE DEL TRATTAMENTO	fissa le caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento attribuendogli specifici compiti: . deve trattarsi, infatti, di un contratto (o altro atto giuridico conforme al diritto nazionale) . e deve disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'art. 28 al fine di dimostrare che il responsabile fornisce "**garanzie sufficienti**" – quali, in particolare: ⇨la natura, ⇨durata e finalità del trattamento o dei trattamenti assegnati, ⇨le categorie di dati oggetto di trattamento, ⇨le misure tecniche e organizzative **adeguate** a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento;

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA TITOLARE, RESPONSABILE, INCARICATO DEL TRATTAMENTO

NOMINA DEL SUB-RESPONSABILE DEL TRATTAMENTO	• Il GDPR consente la nomina di sub-responsabili del trattamento da parte di un responsabile (si veda art. 28, paragrafo 4), per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; •quest'ultimo risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile" (art. 82, paragrafo 1 e paragrafo 3); •La nomina del sub responsabile può avvenire PREVIA AUTORIZZAZIONE SCRITTA da parte del titolare

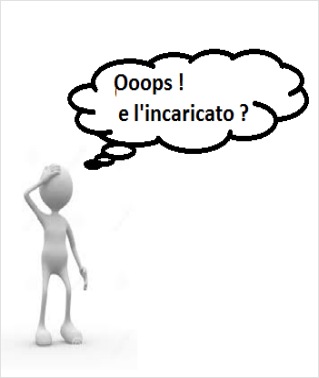
PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA TITOLARE, RESPONSABILE, INCARICATO DEL TRATTAMENTO

OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO	Sono distinti da quelli pertinenti ai rispettivi titolari. In particolare: ✓la tenuta del registro dei trattamenti svolti (ex art. 30, paragrafo 2); ✓l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti (ex art. 32 regolamento); ✓la designazione di un RPD-DPO
RESPONSABILE DEL TRATTAMENTO EXTRA UE	anche il responsabile non stabilito nell'Ue dovrà designare un rappresentante in Italia quando ricorrono le condizioni di cui all'art. 27, paragrafo 3, del GDPR.

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA TITOLARE, RESPONSABILE, INCARICATO DEL TRATTAMENTO

INCARICATO DEL TRATTAMENTO 	Pur non prevedendo espressamente la figura dell' "incaricato" del trattamento, il GDPR non ne esclude la presenza in quanto fa riferimento a : "*persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile*" (art. 4, n. 10, GDPR).

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA TITOLARE, RESPONSABILE, INCARICATO DEL TRATTAMENTO

Regolamento Europeo (EN)	Regolamento Europeo (IT)	T.U. Privacy Italiano D.Lgs. 196/03
Data Controller	Titolare del Trattamento	Titolare del Trattamento
Data Processor	Responsabile del Trattamento	Responsabile del Trattamento
Persons Authorised to Process (non definito/codificato)	Incaricato del Trattamento/ Persona autorizzata al trattamento	Incaricato del Trattamento
Data Protection Officer	Responsabile della Protezione dei Dati	Non Previsto

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO

REGISTRO DEL TRATTAMENTO DEL TITOLARE E DEL RAPPRESENTANTE	Ogni titolare del trattamento e, ove applicabile, il rappresentante designato **DEVE** tenere un Registro delle attività di trattamento svolte sotto la propria responsabilità
REGISTRO DEL TRATTAMENTO DEL RESPONSABILE	Ogni **responsabile del trattamento** designato **DEVE** tenere un Registro delle attività di trattamento svolte sotto la propria responsabilità
ESENZIONE	I Registri NON devono essere tenuti da imprese od organizzazioni che abbiano meno di 250 dipendenti, a meno che: • il trattamento presenti rischi specifici per diritti e libertà e non sia occasionale; o • il trattamento includa categorie particolari di dati; • il trattamento includa dati relativi a condanne e reati penali.

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA NOTIFICA DATA BREACH

DEFINIZIONE DATA BREACH	violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
NOTIFICA all'autorità di controllo	**entro 72 ore** dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo. Art. 33
NOTIFICA all'interessato	Quando la violazione dei dati personali presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo. La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione. Art. 34

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA NOTIFICA DATA BREACH

ESENZIONE NOTIFICA all'interessato	Quando il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura
ESENZIONE NOTIFICA all'interessato	Quando il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati
ESENZIONE NOTIFICA all'interessato	Quando detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile.

The INTERNATIONAL COUNCIL OF MANAGEMENT CONSULTING INSTITUTES
CMC - GLOBAL

Organismo accreditato per la qualificazione
CMC
CERTIFIED MANAGEMENT CONSULTANT

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA DPIA - DATA PROTECTION IMPACT ASSESSMENT

DPIA	DPIA ovvero Valutazione d'impatto sulla protezione dei dati
COSA E' ?	È una procedura prevista dall'articolo 35 del GDPR 2016/679 che mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntare misure idonee ad affrontarli. Una DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.
PERCHÉ ?	La DPIA è uno strumento importante in termini di responsabilizzazione (**accountability**) in quanto **aiuta il titolare** non soltanto a rispettare le prescrizioni del GDPR, ma anche ad **attestare** di aver adottato misure idonee a garantire il rispetto di tali prescrizioni. In altri termini, la DPIA è una procedura che permette di **VALUTARE E DIMOSTRARE** la conformità con le norme in materia di protezione dei dati personali. Vista la sua utilità, il **Gruppo Art. 29 suggerisce** di valutarne l'impiego per tutti i trattamenti, e non solo nei casi in cui il Regolamento la prescrive come obbligatoria.

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA DPIA - DATA PROTECTION IMPACT ASSESSMENT

DPIA	DPIA ovvero Valutazione d'impatto sulla protezione dei dati
IN GENERALE QUANDO SI REDIGE ?	Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate **obbliga i titolari a svolgere una valutazione di impatto PRIMA di darvi inizio.** Dovrebbe comunque essere previsto un **riesame continuo** della DPIA, ripetendo la valutazione a intervalli regolari.
IN CASO DI ?	1. Valutazione sistematica e globale di aspetti personali basata su trattamento automatizzato, compresa la profilazione 2. Trattamento, su larga scala di categorie particolari di dati o di dati relativi a condanne penali; 3. sorveglianza sistematica su larga scala di una zona accessibile al pubblico.
CHI ?	La responsabilità della DPIA **spetta al titolare**, **anche se la conduzione materiale della valutazione di impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione**. Il titolare ne monitora lo svolgimento consultandosi con il DPO e acquisendo - se i trattamenti lo richiedono - il parere di esperti di settore, del responsabile della sicurezza dei sistemi informativi (Chief Information Security Officer, CISO) e del responsabile IT.

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA TITOLARE, RESPONSABILE, INCARICATO DEL TRATTAMENTO

TITOLARE DEL TRATTAMENTO – RESPONSABILITA'

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA DPIA - DATA PROTECTION IMPACT ASSESSMENT

DPIA	DPIA ovvero Valutazione d'impatto sulla protezione dei dati
QUANDO LA DPIA E' OBBLIGATORIA CRITERI WP 29 ? Il WP29 Art. 29 individua alcuni **criteri specifici** a questo proposito mediante Linee Guida :	
1.	trattamenti valutativi o di scoring, compresa la profilazione;
2.	decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
3.	monitoraggio sistematico (es: videosorveglianza);
4.	trattamento di dati particolari, condanne e reati penali o di natura estremamente personale (es: informazioni sulle opinioni politiche);
5.	trattamenti di dati personali su larga scala;
6.	combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
7.	dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA DPIA - DATA PROTECTION IMPACT ASSESSMENT

DPIA	DPIA ovvero Valutazione d'impatto sulla protezione dei dati
QUANDO LA DPIA E' OBBLIGATORIA CRITERI WP 29 ? Il WP29 Art. 29 individua alcuni **criteri specifici** a questo proposito:	
8.	utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
9.	trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).
La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze – il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.	

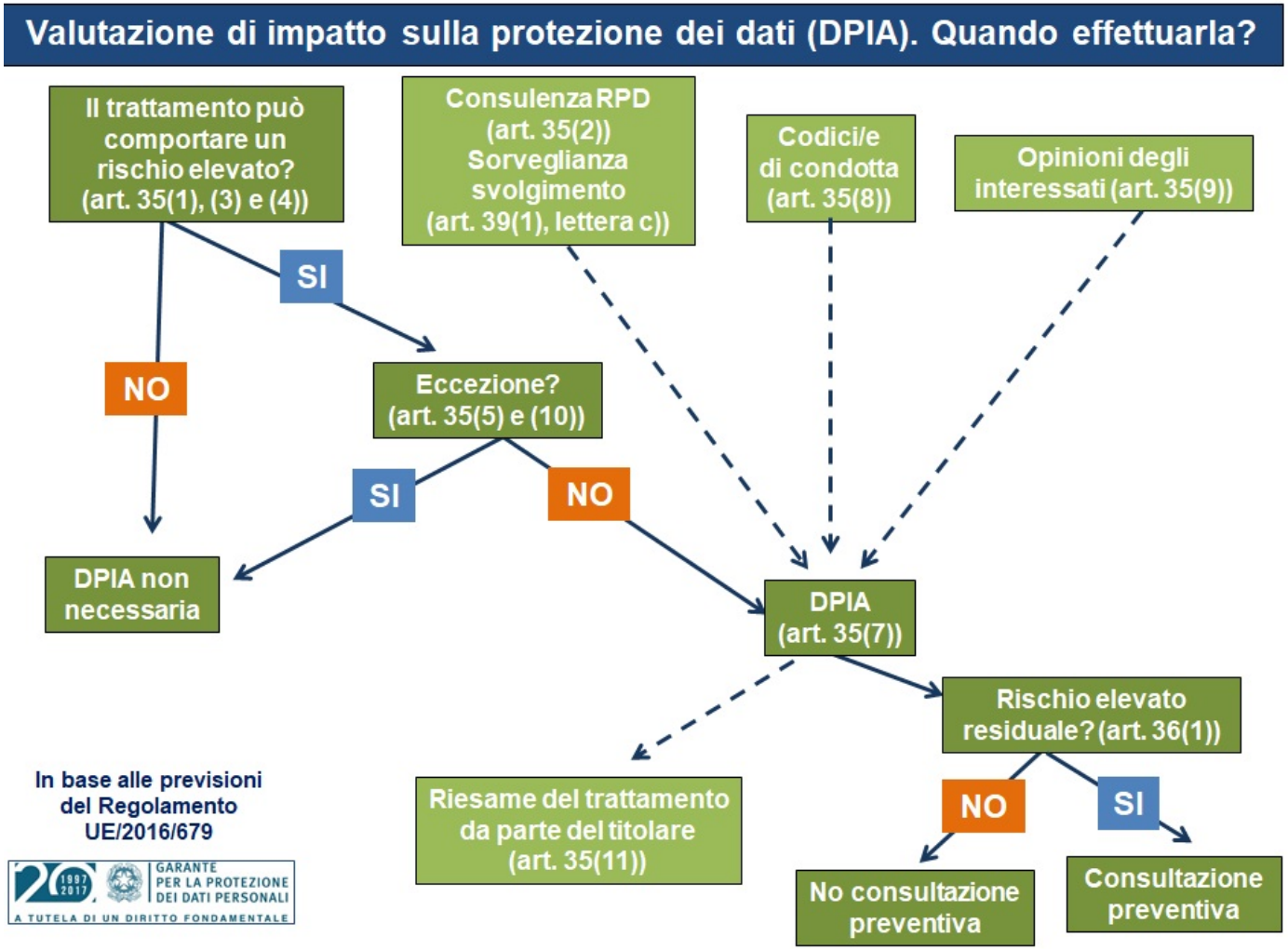
PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA DPIA - DATA PROTECTION IMPACT ASSESSMENT

DPIA	**DPIA ovvero Valutazione d'impatto sulla protezione dei dati**
QUANDO LA DPIA NON E' OBBLIGATORIA/NECESSARIA CRITERI WP 29 ? Il WP29 Art. 29 individua alcuni **criteri specifici** a questo proposito mediante Linee Guida :	
per i trattamenti che:	
A)	non presentano rischio elevato per diritti e libertà delle persone fisiche;
B)	hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
C)	sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
D)	sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
E)	fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA DPIA - DATA PROTECTION IMPACT ASSESSMENT



The INTERNATIONAL COUNCIL OF MANAGEMENT CONSULTING INSTITUTES
CMC - GLOBAL
Organismo accreditato per la qualificazione
CMC
CERTIFIED MANAGEMENT CONSULTANT

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA DPIA - DATA PROTECTION IMPACT ASSESSMENT

Esempi di trattamento	Possibili criteri pertinenti	DPIA ?
Un ospedale che tratta i dati genetici e sanitari dei propri pazienti (sistema informativo ospedaliero).	Dati sensibili o dati aventi carattere estremamente personale Dati riguardanti soggetti interessati vulnerabili. - Trattamento su larga scala.	Si
L'uso di un sistema di telecamere per monitorare il comportamento di guida sulle autostrade. Il titolare del trattamento prevede di utilizzare un sistema intelligente di analisi video per individuare le auto e riconoscere automaticamente le targhe.	- Monitoraggio sistematico; - Uso innovativo o applicazione di soluzioni tecnologiche od organizzative.	Si
Un'azienda che monitora sistematicamente le attività dei suoi dipendenti, controllando anche la postazione di lavoro dei dipendenti, le loro attività in Internet, ecc.	- Monitoraggio sistematico. - Dati riguardanti soggetti interessati vulnerabili.	SI

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA DPIA - DATA PROTECTION IMPACT ASSESSMENT

Esempi di trattamento	Possibili criteri pertinenti	DPIA ?
La raccolta di dati pubblici dei media sociali per la generazione di profili.	Valutazione o assegnazione di un punteggio. Trattamento di dati su larga scala. Creazione di Corrispondenze o combinazione di insiemi di dati. Dati sensibili o dati aventi carattere esclusivamente personale	Si
Un'istituzione che crea una banca dati antifrode e di gestione del rating del credito a livello nazionale.	Valutazione o assegnazione di un punteggio. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente. - Impedisce agli interessati di esercitare un diritto o utilizzare un servizio o un contratto.	Si

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA DPIA - DATA PROTECTION IMPACT ASSESSMENT

Esempi di trattamento	Possibili criteri pertinenti	DPIA ?
Un trattamento di "dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato" (considerando 91).	Dati riguardanti soggetti interessati vulnerabili. Dati sensibili o dati aventi Carattere esclusivamente personale	NO
Conservazione per finalità di archiviazione di dati sensibili personali pseudoanonimizzati relativi a interessati vulnerabili coinvolti in progetti di ricerca o sperimentazioni cliniche.	Dati sensibili. Dati riguardanti soggetti interessati vulnerabili. Impedisce agli interessati di esercitare un diritto o utilizzare un servizio o un contratto.	Si

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA DPIA - DATA PROTECTION IMPACT ASSESSMENT

Esempi di trattamento	Possibili criteri pertinenti	DPIA ?
Una rivista online che utilizza una lista di distribuzione per inviare una selezione quotidiana generica ai suoi abbonati.	Trattamento di Dati Su larga scala.	NO
Un sito web di commercio elettronico che visualizza annunci pubblicitari per parti di auto d'epoca che comporta una limitata profilazione basata sugli articoli visualizzati o acquistati sul proprio sito web.	Valutazione o assegnazione di un punteggio.	NO

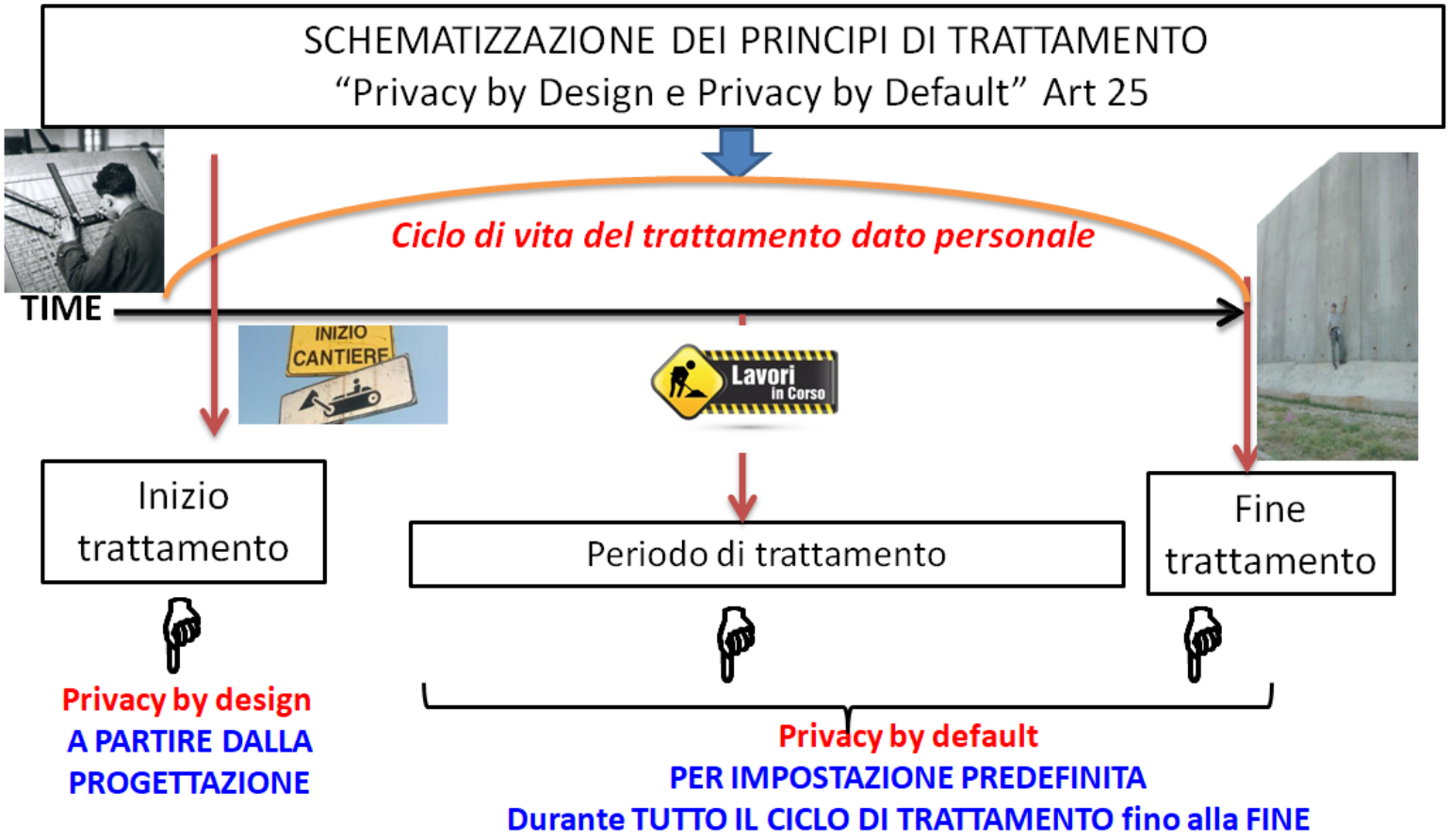
PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA ACCOUNTABILITY – PRIVACY BY DESIGN – PRIVACY BY DEFAULT

Accountability	È il principio di rendicontazione (c.d. "accountability"), secondo cui il Titolare del trattamento deve: conservare la documentazione di tutti i trattamenti effettuati sotto la propria responsabilità, indicando obbligatoriamente – per ognuno di essi – una serie "**nutrita**" di informazioni, tali da assicurare e comprovare – per ciascuna operazione – la conformità alle disposizioni del Regolamento.
Privacy by design	il principio di incorporazione della privacy **A PARTIRE DALLA PROGETTAZIONE**
Privacy by default	il principio di tutela della vita privata **PER IMPOSTAZIONE PREDEFINITA** Durante TUTTO IL CICLO DI TRATTAMENTO

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA ACCOUNTABILITY – PRIVACY BY DESIGN – PRIVACY BY DEFAULT



PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA DPO – DATA PROTECTION OFFICER O RPD -RESPONSABILE DELLA PROTEZIONE DEI DATI

CHI E' IL DPO (definizione)	*È persona che ha una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati, nel controllo del rispetto a livello interno del GDPR, che svolge la propria funzione e compiti incombenti in maniera indipendente e in assenza di conflitti di interesse .* Il titolare o il responsabile del trattamento dovranno mettere a disposizione del Responsabile della protezione dei dati le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.
CHI NOMINA IL DPO ?	Il titolare del trattamento o il responsabile del trattamento

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA DPO – DATA PROTECTION OFFICER O RPD

QUALI SONO I REQUISITI DEL DPO ?

1. possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati.

   Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, **anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze**.

2. adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse . In linea di principio, ciò significa che il DPO **non può essere un soggetto che decide sulle finalità o sugli strumenti del trattamento di dati personali**;

3. operare alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di servizio (RPD/DPO esterno).

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA DPO – DATA PROTECTION OFFICER O RPD

QUALI SONO I COMPITI DEL DPO ?	
indipendenza, autorevolezza, competenze manageriali	
a)	**sorvegliare** l'osservanza del regolamento, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;
b)	**collaborare** con il titolare/responsabile, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA);
c)	**informare e sensibilizzare** il **titolare** o il **responsabile** del trattamento, nonché i **dipendenti** di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;
d)	**cooperare** con il Garante e fungere da punto di contatto per il Garante su ogni questione connessa al trattamento;
e)	**supportare** il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un registro delle attività di trattamento .

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA DPO – DATA PROTECTION OFFICER O RPD

IN QUALI CASI E' OBBLIGATORIA LA NOMINA DEL DPO ?	
a)	amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie;
b)	tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; (*)
c)	tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.
Anche per i casi in cui il regolamento non impone in modo specifico la designazione di un DPO, è comunque possibile una nomina su base volontaria.	
Un gruppo di imprese o soggetti pubblici possono nominare un unico DPO	

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA DPO – DATA PROTECTION OFFICER O RPD

IN QUALI CASI E' OBBLIGATORIA LA NOMINA DEL DPO ? CONCETTO DI LARGA SCALA

(*) Nel GDPR non si dà alcuna definizione di *trattamento su larga scala*, anche se il considerando 91 fornisce indicazioni in proposito.

Il considerando in questione vi ricomprende, in particolare, "trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato". D'altro canto, lo stesso considerando prevede in modo specifico che "**Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato**". Si deve tener conto del fatto che il considerando offre alcune esemplificazioni ai due estremi della scala (trattamento svolto dal singolo medico / trattamento di dati relativi a un'intera nazione o a livello europeo) e che **fra tali estremi si colloca un'ampia zona grigia**. Inoltre, va sottolineato che il considerando citato si riferisce alle valutazioni di impatto sulla protezione dei dati; **ciò significa che non tutti gli elementi citati sono necessariamente pertinenti alla nomina di un DPO negli stessi identici termini.**

(*Linee - guida sui responsabili della protezione dei dati WP 29 16/EN WP 243 rev. 01 Adottate il 13 dicembre 2016 Versione emendata e adottata in data 5 aprile 2017*)

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA SEMPLIFICAZIONI MICRO – PICCOLE – MEDIE IMPRESE

I nuovi parametri dimensionali per le imprese

	Dipendenti (ULA)	Fatturato	Stato patrimoniale
Micro impresa	<10	<2M€uro	<2M€uro
Piccola impresa	<50	<10M€uro	<10M€uro
Media impresa	<250	<50M€uro	<43M€uro
Grande impresa	>250	>50M€uro	>43M€uro
Autonomia	L'azienda non deve essere posseduta per più del 24,9% da una o più aziende che non ricadano nella definizione di piccola e media impresa.		

The INTERNATIONAL COUNCIL OF MANAGEMENT CONSULTING INSTITUTES
CMC - GLOBAL

Organismo accreditato per la qualificazione
CMC
CERTIFIED MANAGEMENT CONSULTANT

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA SEMPLIFICAZIONI MICRO – PICCOLE – MEDIE IMPRESE

Nello specifico sono previste semplificazione per:
Tenuta del registro dei trattamenti a meno di trattamenti particolari (vedi art. 30);
Codici di condotta e certificazioni (C.98 | A. 40 e 42);
Criteri per la certificazione Privacy;
Misure di sensibilizzazione specifiche da parte delle DPA nazionali (C. 132);
Le competenze della Commissione si estendono alla possibilità di prescrivere misure specifiche di semplificazione per le micro, piccole e medie imprese (C. 167).

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA **SISTEMA SANZIONATORIO**

Principio di equivalenza (C 11)	**per le violazioni negli Stati Ue. Ovvero poteri equivalenti per controllare e assicurare il rispetto della norma sul Data protection.**
Livello (Principio) di coerenza per il Data protection. (C13)	Ovvero: a) Garanzia di certezza del Diritto; b) trasparenza agli operatori economici, comprese micro, piccole e medie imprese; c) medesimo livello di responsabilità dei TDT e RDT; d) sanzioni equivalenti.
Principio di cooperazione e coerenza tra DPA capofila e DPA di controllo cui è stato proposto il reclamo C (130)	Ovvero la DPA di capofila deve tenere nella massima considerazione il parere della DPA di controllo, competente quest'ultima, a svolgere indagini nel territorio del proprio Stato Ue.

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA SISTEMA SANZIONATORIO

Principio di gradualità e proporzionalità. (C 148)	Le DPA, nell'erogazione delle sanzioni le DPA devono tener conto di parametri posti dal GDPR e precisamente :	
della natura, gravità e durata della violazione	del carattere doloso o colposo ex art. 83 c.2 lett. b)	delle misure adottate per attenuare il danno subito dall'interessato
del grado di responsabilità	di precedenti violazioni pertinenti (recidive)	del modo in cui la DPA ha preso conoscenza della violazione (si pensi ad omessa notificazione DATA BREACH)
del rispetto di Provvedimenti disposti dalla DPA, nei confronti del TDT o del RDT	alla adesione a Codici di condotta (aggravante)	eventuali altri fattori aggravanti o attenuanti.

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA **SISTEMA SANZIONATORIO**

Principio di garanzia. (C 148)	**L'imposizione di tutti i tipi di sanzione deve essere soggetta a garanzie procedurali appropriate, nel rispetto dei Principi generali del diritto Ue e della Carta Ue, inclusi l'effettiva tutela giurisidizionale e il giusto processo**
Previsione sanzioni penali (C 149)	da parte dei singoli Stati Ue, nel rispetto del Principio "**ne bis in idem**"
Indice di riferimento per l'applicazione delle sanzioni amministrative (C 150)	**In capo alle imprese** (Rinvio agli artt. 101 e 102 TFUE) **In capo alle persone non imprese**
Principio di alternatività od aggiunta accessoria Art. 58 c.2 lett i)	Ogni DPA ha il potere di infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, **od altre misure** di cui all'art. 58 (poteri correttivi) **o in luogo delle predette**, in funzione delle circostanze di ogni singolo caso.
Caratteristiche delle sanzioni (C 152)	Tutte le sanzioni devono essere: EFFETTIVE, PROPORZIONATE E DISSUASIVE.

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA **SISTEMA SANZIONATORIO**

Il sistema sanzionatorio del GDRP si può classificare in diverse tipologie:
Sanzioni amministrative "Sanzioni correttive " = avvertimenti; ammonimenti; ingiunzioni; limitazioni provvisorie o definitive ; ordini di rettifica e cancellazione; revoca di certificazione od ordini di revoca certificazioni; ordini di sospensione flusso di dati.
Sanzioni amministrative pecuniarie = fino a **10.000.000 EUR**, o per le imprese, fino al **2 %** del fatturato mondiale totale annuo dell'esercizio precedente, se superiore a determinate condizioni.
Sanzioni amministrative pecuniarie = fino a **20.000.000 EUR**, o per le imprese, fino al **4 %** del fatturato mondiale totale annuo dell'esercizio precedente, se superiore a determinate condizioni.
Sanzioni penali = (in aggiunta) a cura (*a discrezione)* degli Stati membri Ue
Risarcimento del danno = Chiunque subisca un danno materiale o immateriale causato da una violazione del GDPR, ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento (art. 82 c.1)

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA **SISTEMA SANZIONATORIO**

SOGGETTI ATTIVI DELLE VIOLAZIONI
il TITOLARE DEL TRATTAMENTO: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali
il RESPONSABILE DEL TRATTAMENTO: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento
l'ORGANISMO DI CERTIFICAZIONE
l'ORGANISMO PER IL CONTROLLO.

Nota: I DPO non rispondono personalmente in caso di inosservanza del GDPR.
Il GDPR chiarisce che spetta al titolare o al responsabile del trattamento garantire ed essere in grado di dimostrare che le operazioni di trattamento sono conformi alle disposizioni del regolamento stesso (articolo 24, primo paragrafo).

L'onere di assicurare il rispetto della normativa in materia di protezione dei dati ricade quindi sul titolare o sul responsabile.

(Linee-guida WP 29 sui responsabili della protezione dei dati Adottate il 13/12/2016 - Versione emendata e adottata in data 5/4/2017)

PRINCIPI GENERALI DEL GDPR 2016/679

➢COSA CAMBIA **SISTEMA SANZIONATORIO**

confronto CODICE PRIVACY D.Lgs. 196/2003 REGOLAMENTO UE 2016/679

Caso: Google **GOOGLE STREET VIEW** Italia anno 2010.
Fatturato Google consolidato 2014: 66 miliardi di dollari
Provvedimento sanzionatorio: anno 2014 del Garante italiano per **violazione degli articoli 13, 162 e 164 del codice per la tutela della privacy**, a causa dell' ***assenza di informativa*** *agli utenti e della* ***creazione di una "banca dati di particolari dimensioni*** *in occasione della raccolta di dati effettuata dalla società mediante le cosiddette Google cars nell'ambito del servizio denominato Street View*"
Sanzione 2014: 1 **milione di euro** ($ dollari USD 1.114.578,69)

Caso ipotetico con il Regolamento a regime

Caso: **Alphabet** holding
Fatturato *Alphbet consolidato 2015:* 74,5 miliardi di Dollari
Sanzioni a regime 2018:
Sanzione applicabile (per *omessa informativa* art.12) Art. 83 comma 5 lettera b): pari al 4 % del fatturato mondiale totale $ 2.980.000.000,00 (Tasso di cambio **0,8054 07/03/2018) = €** 24.005.155.469.631,00
Sanzione applicabile (per *omessa consultazione preventiva* creazione banca dati art. 36) Art. 83 comma 4 lettera a): pari al 2 % del fatturato mondiale totale $ 1.490.000.000,00 (Tasso di cambio **0,8054 07/03/2018) = € 1.200.046.000,00**

… per un Informativa e una banca dati di particolari dimensioni (senza tener conto dell'omessa DPIA a suo tempo non prevista)!

GRAZIE PER L'ATTENZIONE

Relatore: Dott. Emanuele VETTORELLO

Vice Presidente di ASSO DPO –
Associazione Data Protection Officer

Data Protection Officer
Certificato CEPAS - Bureau Veritas Italia S.p.A. n° DPO0037
Schema DPO sviluppato in accordo alla ISO/IEC 17024:2012