Scuola Internazionale
Etica&Sicurezza
Milano - L'Aquila

Diritto alla privacy e sicurezza
Milano, 26 marzo 2019

avv. Guglielmo Troiano

Scuola Internazionale
Etica&Sicurezza
Milano - L'Aquila

Scuola Internazionale
Etica&Sicurezza
Milano - L'Aquila

AGENDA

- Regolamento Europeo GDPR e implicazioni nei servizi/impianti di security (tvcc, controllo accessi, gps, remotizzazione controlli)

- Videosorveglianza nei luoghi di lavoro, Privacy e Statuto dei lavoratori

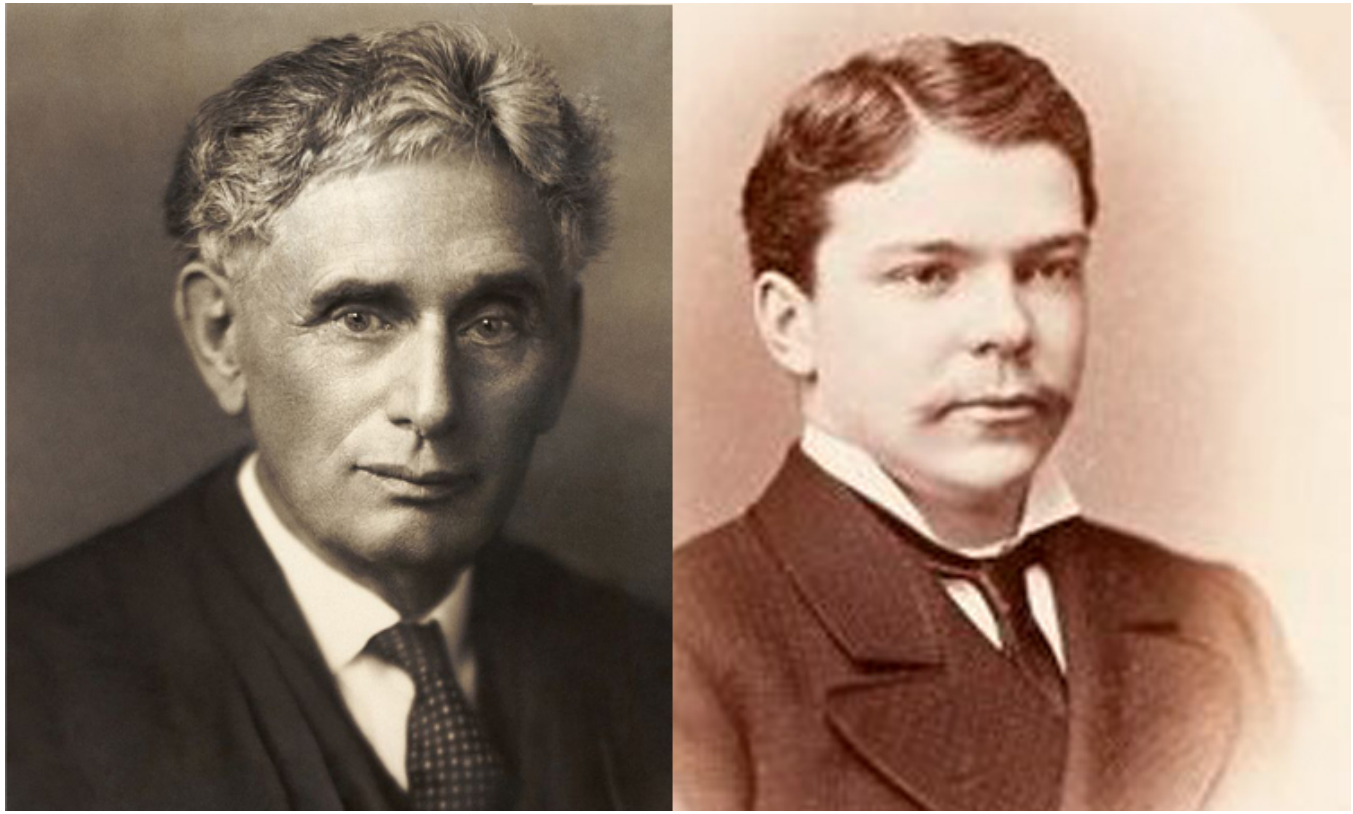
- Analisi giurisprudenza e suggerimenti attenzioni da tenere in sede di vendita dei sistemi

IL TRATTAMENTO DEI DATI PERSONALI

ALCUNI CONCETTI FONDAMENTALI

RISERVATEZZA, TRATTAMENTO DI DATI, INFORMAZIONE, SICUREZZA

il concetto giuridico di **Privacy** è stato ideato negli USA nel 1890, esattamente quando due giuristi, **Samuel Warren e Louis Brandeis**, pubblicarono un approfondimento scientifico sulla Harvard Law Review intitolato "Right to Privacy".



In quell'articolo, per la prima volta, venne analizzato il bilanciamento tra il diritto all'informazione, cioè il diritto di informare ed essere informati, ed il diritto alla privacy, da intendersi come diritto individuale alla "**riservatezza**"

RISERVATEZZA, TRATTAMENTO DI DATI, INFORMAZIONE, SICUREZZA

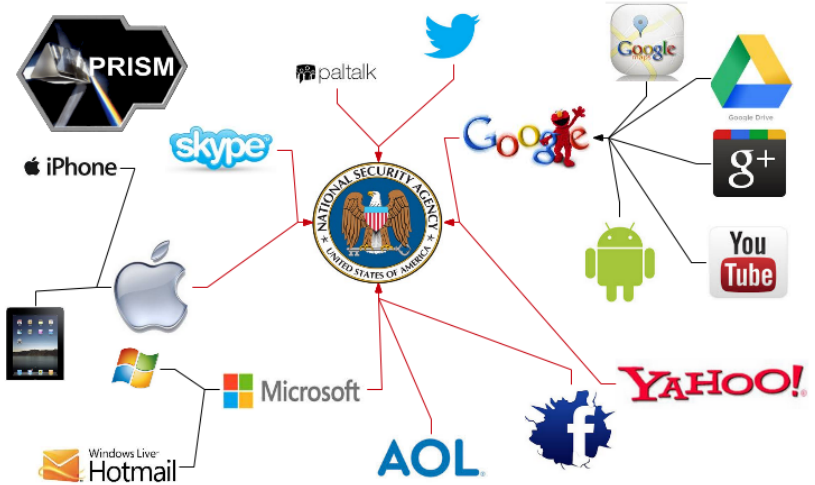
“to be let alone”, essere lasciato solo: rifiuto della privacy come isolamento, abbandono voler essere lasciati in pace non significa assolutamente voler rimanere soli
la «privacy» mi consente di scegliere quando esibirmi o quando, invece, rimanere al riparo dagli occhi del pubblico

La Corte Suprema degli USA, nei primi anni del 1900, inizia ad affermare che le persone **pubbliche** hanno una **aspettativa** di privacy inevitabilmente **inferiore** a quella dei comuni cittadini. I cittadini come elettori, ad esempio, hanno diritto a conoscere particolari della vita privata di un candidato.

“voglio essere lasciata sola, non essere sola”

Greta Garbo

RISERVATEZZA, TRATTAMENTO DI DATI, INFORMAZIONE, SICUREZZA



"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say." *Edward Snowden*

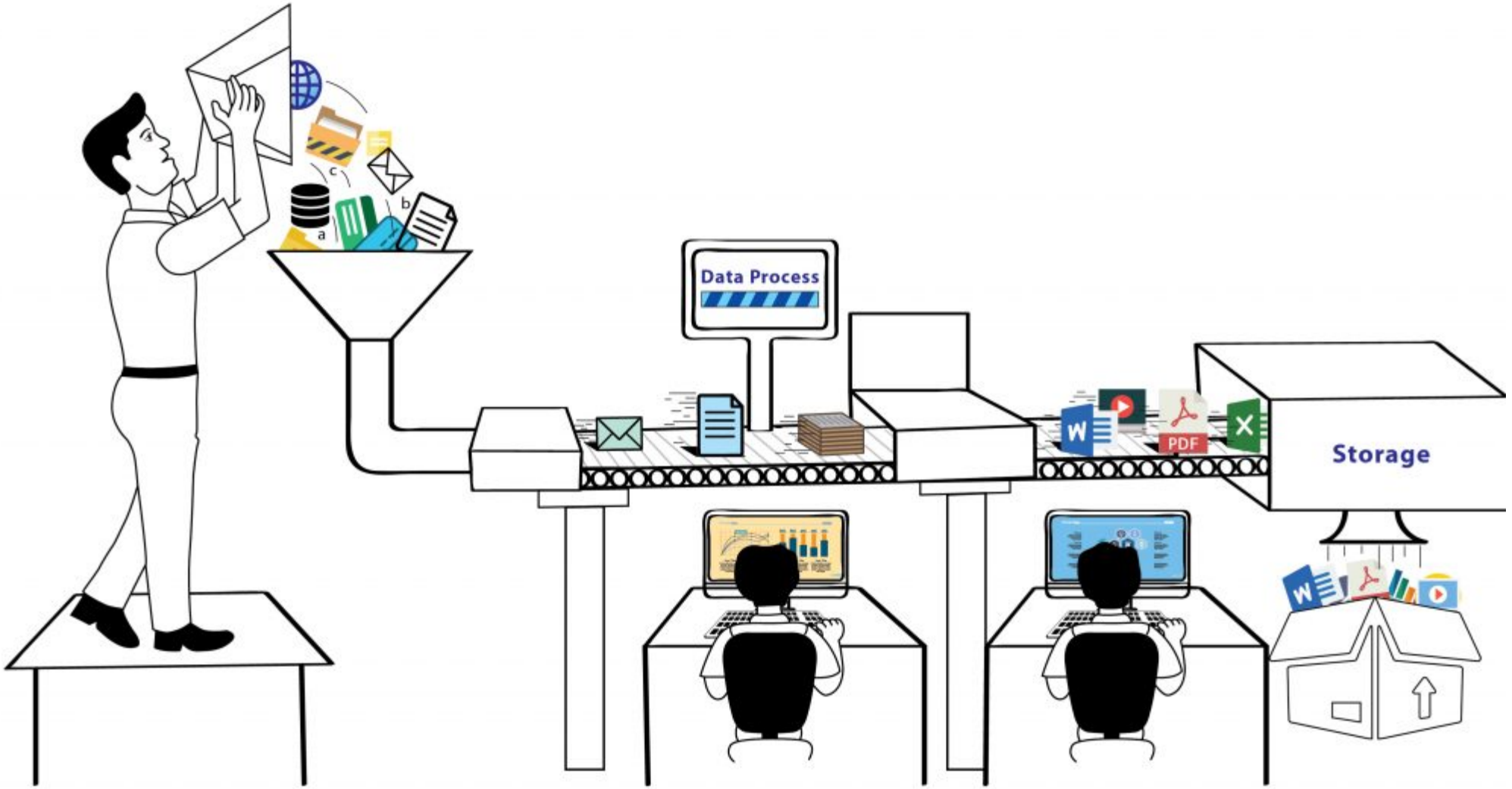
RISERVATEZZA, TRATTAMENTO DI DATI, INFORMAZIONE, SICUREZZA

- il DATO P. è la FONTE dell'INFORMAZIONE nel quale questa è contenuta
- dal singolo DATO P. o dall'insieme dei DATI P. l'INFORMAZIONE può essere estratta o inferita
- l'INFORMAZIONE NON necessariamente COINCIDE con il DATO P.
- l' INFORMAZIONE è l'elaborazione di un DATO P.
- il DATO PERSONALE non è necessariamente un DATO RISERVATO

Quali sono i dati non personali se il dato personale è ogni informazione riferibile a qualsivoglia soggetto?

Le leggi sulla protezione dei dati personali sono onnipervasive e NON si occupano SOLO della RISERVATEZZA in senso stretto ma del TRATTAMENTO DELLE INFORMAZIONI

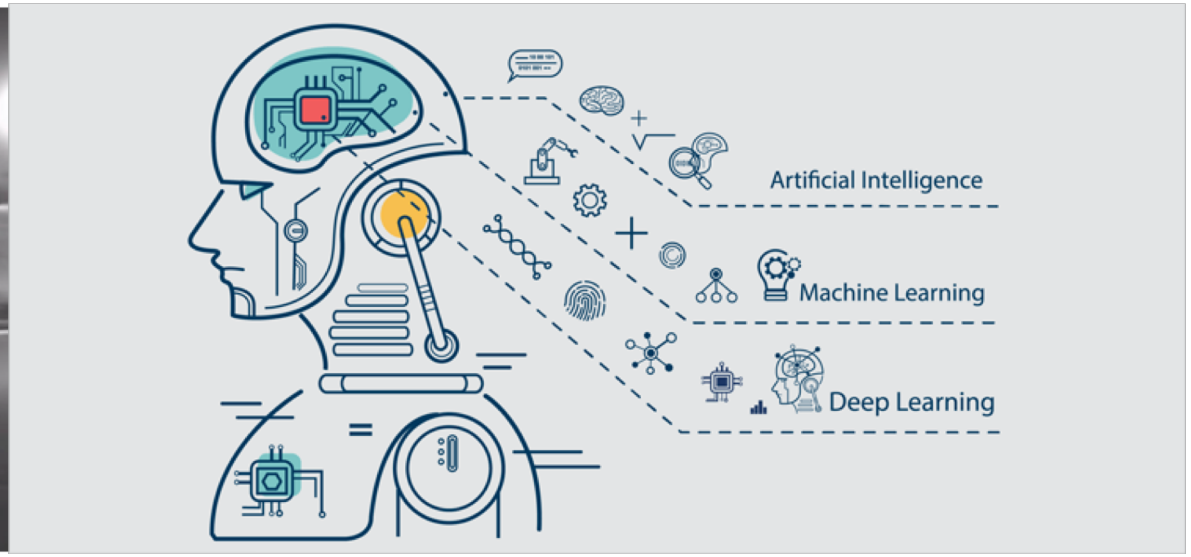
RISERVATEZZA, TRATTAMENTO DI DATI, INFORMAZIONE, SICUREZZA



RISERVATEZZA, TRATTAMENTO DI DATI, INFORMAZIONE, SICUREZZA

Ces 2019, il funerale del robot investito da una Tesla

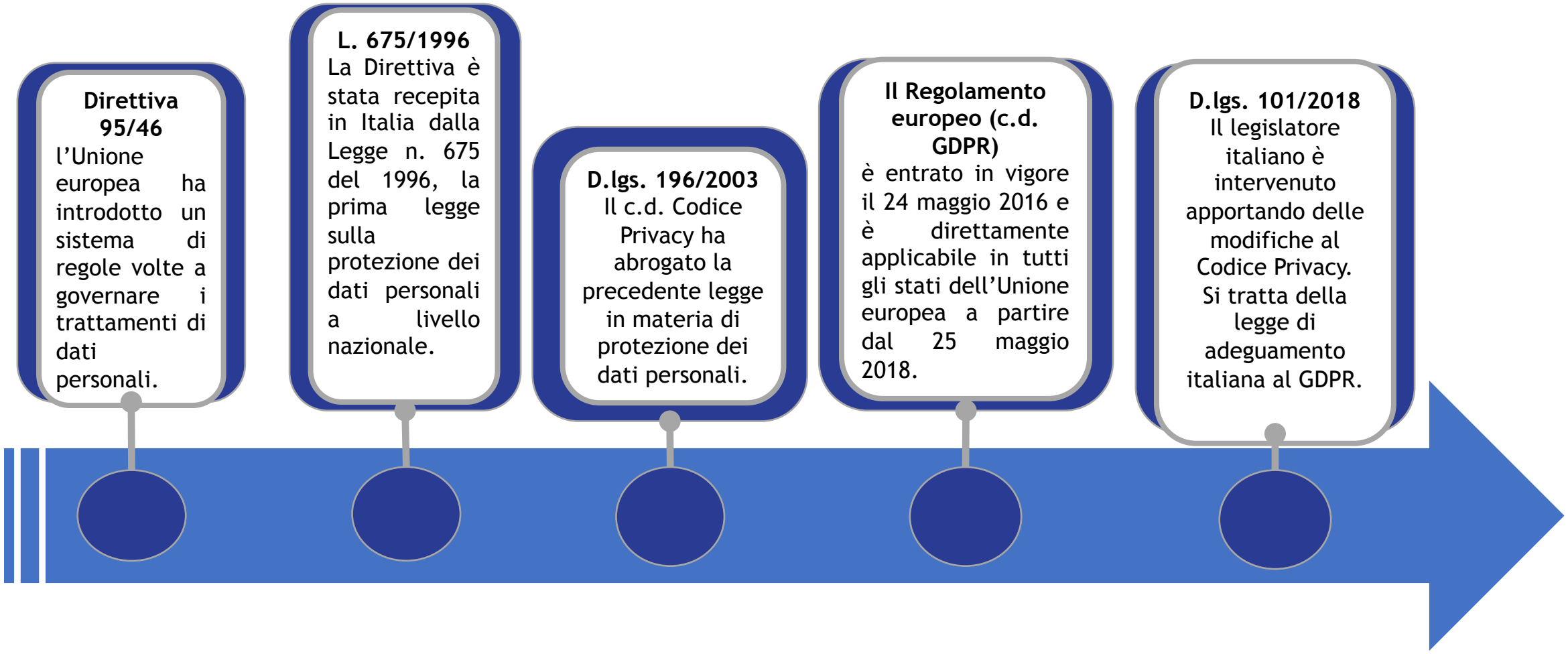
Alla fiera di Las Vegas il primo incidente al mondo in cui la vittima è un automa, di cui sono state celebrate le esequie



IL TRATTAMENTO DEI DATI PERSONALI

GDPR: INQUADRAMENTO

Evoluzione normativa



Un nuovo strumento giuridico

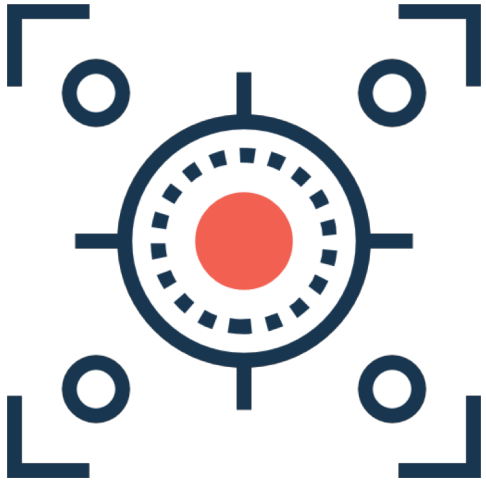
Il **REGOLAMENTO** (non più una direttiva) è **direttamente applicabile** in tutti gli stati membri **senza bisogno di trasposizioni nazionali**

L'obiettivo originario (testimoniato proprio dall'adozione dello strumento regolamentare invece di quello della direttiva) era quello di creare una regolamentazione uniforme all'interno dell'UE…

MA

i compromessi raggiunti successivamente (al fine di raggiungere l'accordo politico sul testo finale) hanno invece creato diverse "zone grigie" nell'impianto che lasciano aperta la porta a svariate interpretazioni e difformi applicazioni. Lo stesso GDPR consente infatti alcune specificazioni o limitazioni, come pure deroghe o esenzioni da parte delle legislazioni nazionali. Permarranno quindi differenze fra paese e paese

Principali obiettivi del legislatore europeo



ADEGUARE la NORMATIVA (risalente ormai a 20 anni fa…) alle **NUOVE TECNOLOGIE** (Social Network, Cloud Computing, App web e mobile, Big Data, etc)

ARMONIZZARE ed **UNIFORMARE** la NORMATIVA a livello europeo, creando un quadro legislativo comune in modo da evitare di far fronte a normative differenti in ciascuno stato membro

Ambito di applicazione territoriale

Il GDPR si applica al trattamento effettuato:

da un Titolare o da un Responsabile stabiliti **in UE**, anche se il trattamento è effettuato extra UE

Il GDPR si applica al trattamento effettuato:

Da un Titolare o da un Responsabile stabiliti **extra UE,** che **offrono beni o servizi a interessati che "si trovano" in UE*** o che **monitorano il loro comportamento all'interno dell'UE**

- Considerando 23: per accertare tale intenzione non è sufficiente la semplice accessibilità di un sito web dall'UE, ma l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare beni o servizi in tale lingua.
- Considerando 24: a tal fine, è opportuno verificare se c'è un tracciamento su Internet, ivi inclusa la profilazione .

Ambito di applicazione territoriale

Sono «**interessati**» anche **i <u>cittadini di paesi extra-UE</u>** che **<u>SI TROVANO MOMENTANEAMENTE nell'Unione Europea</u>** e che **<u>utilizzano servizi di un provider EXTRA UE che offre beni e servizi nell'UE</u>?**

Non essendo presente nel testo un esplicito riferimento al domicilio o alla residenza degli interessati all'interno dell'Unione Europea (riferimento quest'ultimo invece inizialmente presente nella proposta di Regolamento e, successivamente, superato), deve ritenersi sufficiente la «mera presenza» (e, quindi, uno stato transitorio) degli stessi nell'Unione ai fini dell'applicabilità del Regolamento.

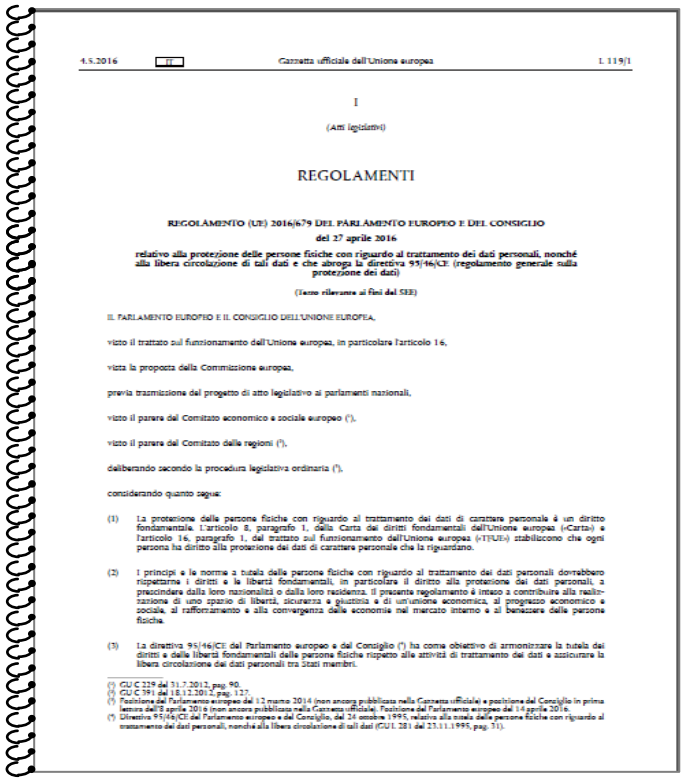
Quando previsto, **<u>l'azienda EXTRA UE deve applicare in toto il GDPR ?</u>**

L'assoggettamento di una azienda extra UE al GDPR implica che tutti gli obblighi materiali e formali sanciti dallo stesso siano rispettati, senza eccezioni, limitazioni o deroghe.

Ambito di applicazione territoriale

	APPLICABILITÀ GDPR		NOTE
	Filiale UE	**Filiale stabilita extra-UE**	
RESIDENTI IN UE SU TERRITORIO UE	**Sì (Art.3 par. 1 e 2, GDPR)**	**Sì**	
RESI EXTRA-UE IN TERRITORIO UE	**Sì**	**Sì**	
RESIDENTI IN UE SU TERRITORIO EXTRA-UE	**Sì (Art.3 par. 1 e 2, GDPR)**	**NO**	(«…the processing of personal data of EU citizens or residents that takes place in a third country does not trigger the application of the GDPR, as long as the processing is not related to a specific offer directed at individuals in the EU or to a monitoring of their behaviour in the Union»). *EDPB, Guidelines 3/2018*
RESIDENTI EXTRA-UE IN TERRITORIO EXTRA-UE	**Sì**	**NO**	

Rapporto con le direttive



4.5.2016 IT Gazzetta ufficiale dell'Unione europea L 119/1

I

(Atti legislativi)

REGOLAMENTI

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
del 27 aprile 2016
relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 16,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo (1),

visto il parere del Comitato delle regioni (2),

deliberando secondo la procedura legislativa ordinaria (3),

considerando quanto segue:

(1) La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

(2) I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche.

(3) La direttiva 95/46/CE del Parlamento europeo e del Consiglio (4) ha come obiettivo di armonizzare la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati e assicurare la libera circolazione dei dati personali tra Stati membri.

(1) GU C 229 del 31.7.2012, pag. 90.
(2) GU C 391 del 18.12.2012, pag. 127.
(3) Posizione del Parlamento europeo del 12 marzo 2014 (non ancora pubblicata nella Gazzetta ufficiale) e posizione del Consiglio in prima lettura dell'8 aprile 2016 (non ancora pubblicata nella Gazzetta ufficiale). Posizione del Parlamento europeo del 14 aprile 2016.
(4) Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31).

Il GDPR

ABROGA la **Direttiva 95/46/CE**, con l'effetto di abrogare anche le normative nazionali emanate in applicazione di tale Direttiva, come il **Codice Privacy**, almeno nelle parti di diretta trasposizione di tale Direttiva

MA

NON la **Direttiva 2002/58/CE** (cd. «*Direttiva e-Privacy*») che prevede obblighi specifici per i fornitori di servizi di comunicazioni elettroniche (e quindi, nel nostro ordinamento le disposizioni del Codice Privacy di attuazione della stessa).

IL TRATTAMENTO DEI DATI PERSONALI

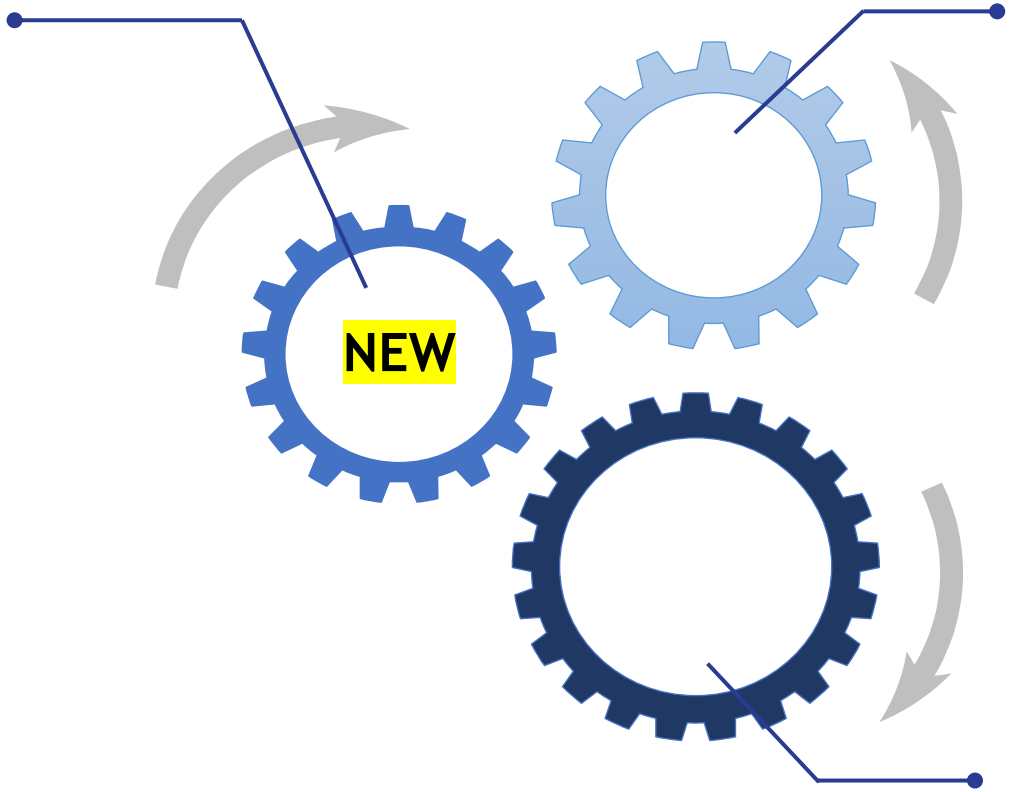
E IL CODICE PRIVACY ITALIANO?

D.Lgs. 10 AGOSTO 2018, N.101

Cos'è?

Decreto legislativo n.101/2018

- Il decreto legislativo è finalizzato ad adeguare il quadro normativa nazionale alle disposizioni del GDPR e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE
- In relazione all'elaborazione di questo testo è stata istituita una commissione di studio con decreto del Ministro del 14 dicembre 2017, che ha potuto incominciare i lavori il 4 gennaio 2018. Com'è noto, il GDPR è direttamente applicabile dal 25 maggio 2018. L'adeguamento dell'ordinamento italiano deve essere coerente temporalmente con tale data e dunque la commissione ha potuto operare in un tempo limitato
- La legge di delegazione europea n. 163 del 2017 ha quindi stabilito all'art. 13 comma 3, i criteri della delega



Regolamento (UE) 2016/679 (GDPR)

Decreto legislativo 196/2003 (Codice Privacy)

D.Lgs. 10 AGOSTO 2018, N.101

Cosa ha fatto il Governo?

AZIONE 1

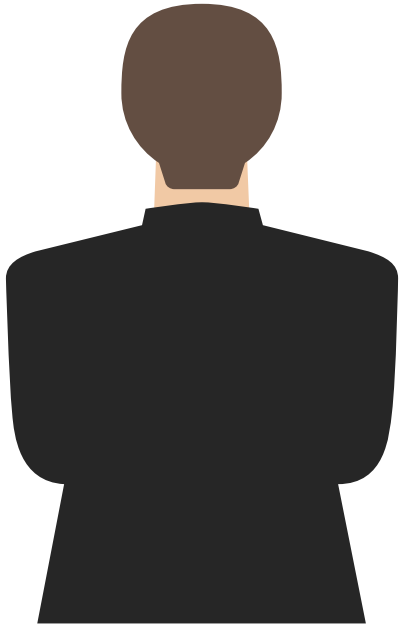
Abrogare espressamente le disposizioni del Codice Privacy (d.lgs. 196/2003 - «Codice») incompatibili con le disposizioni contenute nel GDPR

AZIONE 2

Modificare il Codice limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel GDPR

AZIONE 3

Coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal GDPR



AZIONE 4

Prevedere il ricorso a **specifici provvedimenti attuativi e integrativi** adottati dal Garante nell'ambito e per le finalità previsti dal GDPR

AZIONE 5

Adeguare il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del GDPR

D.Lgs. 10 AGOSTO 2018, N.101

Perché si è reso necessario?

Il GDPR

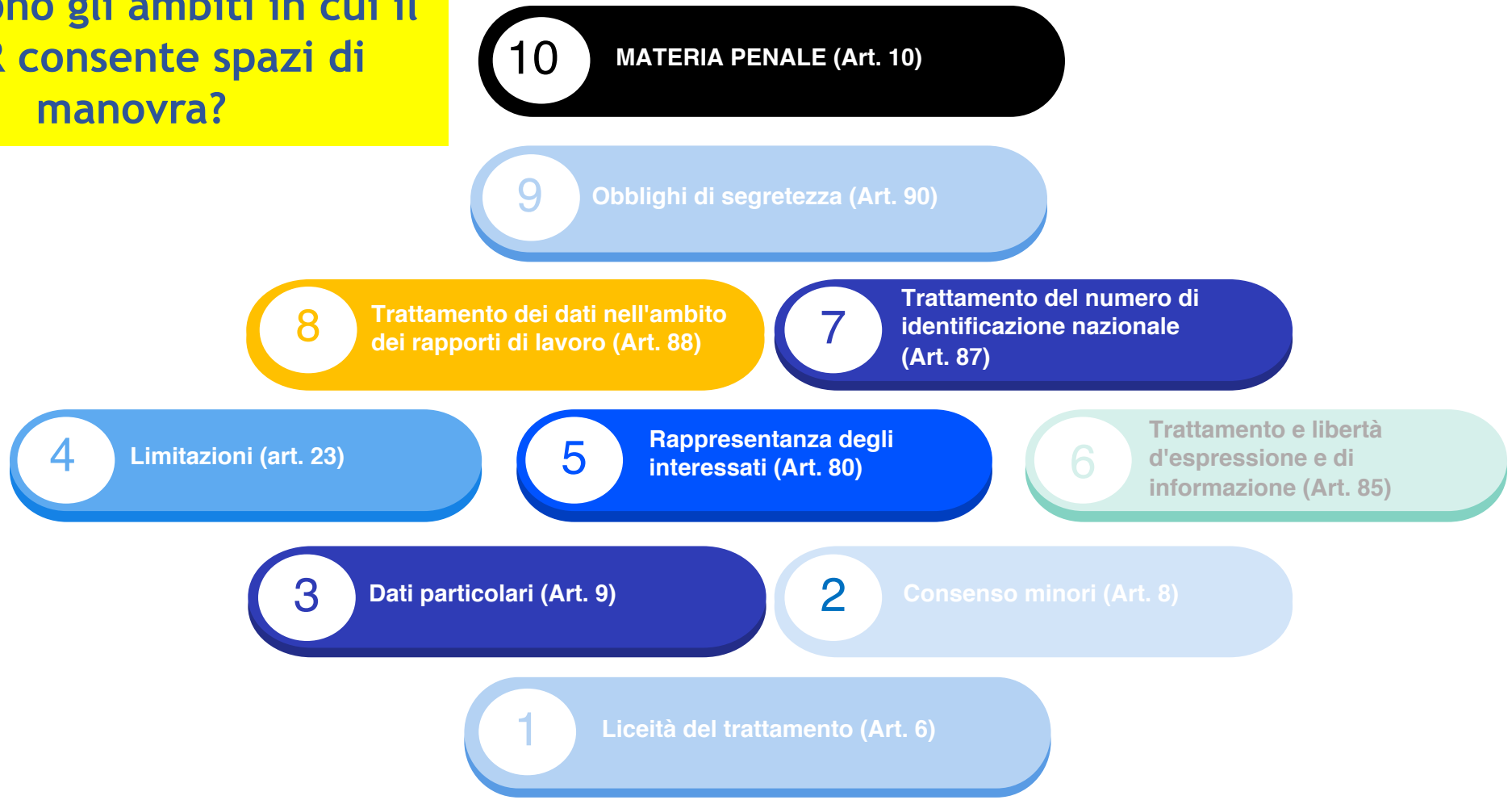
- è direttamente applicabile in tutti gli Stati membri
- non necessita di alcuna legge statale di recepimento
- prevede espressamente la possibilità, per ciascuno Stato Membro, di disciplinare autonomamente determinati ambiti

Il D.lgs. 10 agosto 2018, n.101

- va a **disciplinare quegli ambiti che il Regolamento permette a ciascuno Stato di normare in autonomia** (si è reso necessario perché il Regolamento ha concesso tale ulteriore adempimento)
- **armonizzare le previsioni del Codice Privacy al GDPR**

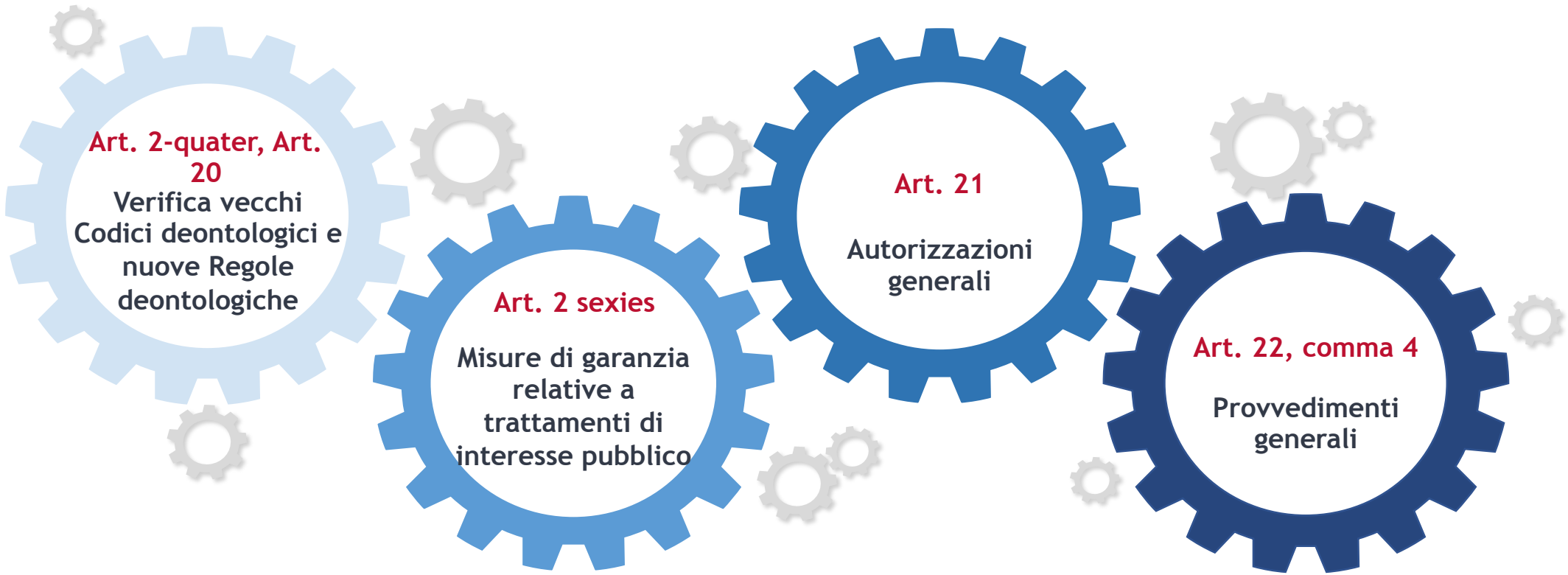
D.Lgs. 10 AGOSTO 2018, N.101

Quali sono gli ambiti in cui il GDPR consente spazi di manovra?



D.Lgs. 10 AGOSTO 2018, N.101

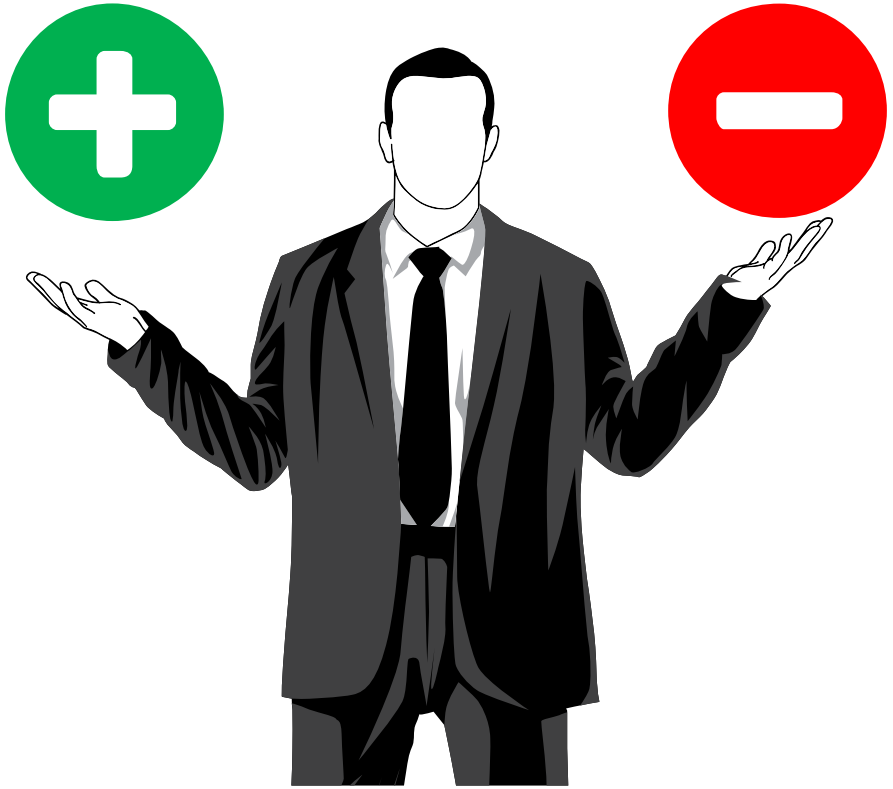
Quale ruolo ricoprirà il Garante per la protezione dei dati personali?



D.Lgs. 10 AGOSTO 2018, N.101

Quale ruolo ricoprirà il Garante per la protezione dei dati personali?

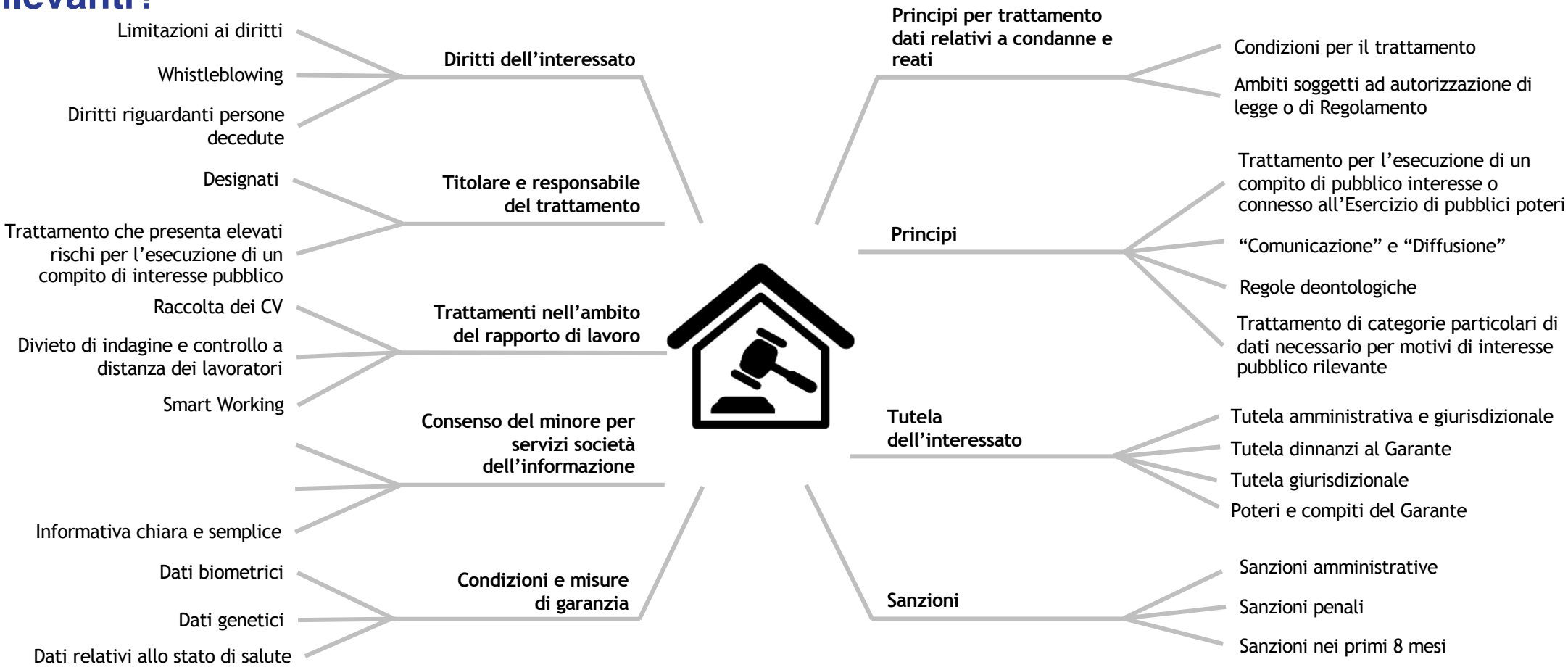
Al Garante vengono attribuiti ampi e significativi poteri di ***soft law*** che permetteranno di favorire una maggiore flessibilità nell'adeguamento della normativa alle reali esigenze concrete (ad es. per innovazioni tecnologiche)



Un'eventuale inadempienza porterebbe a situazioni poco chiare (ad es. sopravvivenza di norme del vecchio Codice espressamente abrogate)

D.Lgs. 10 AGOSTO 2018, N.101

Quali sono gli aspetti più rilevanti?



GDPR: COSA NON CAMBIA O VARIA MARGINALMENTE NEL REGOLAMENTO

GDPR: cosa non cambia o varia marginalmente nel regolamento

- Definizione di dato personale
- Definizione di trattamento
- Soggetti che effettuano il trattamento (salvo DPO)
- Principi relativi al trattamento di dati
- Liceità del trattamento
- Informativa
- Consenso
- Protezione delle sole persone fisiche

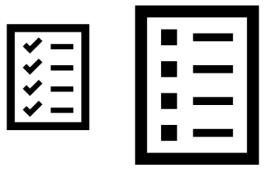
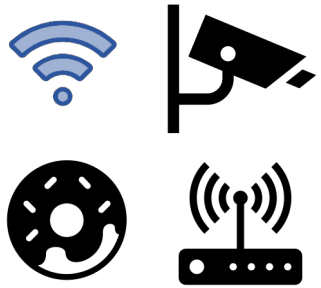
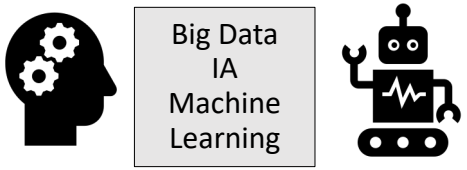
Definizione di dato personale (GDPR)

qualsiasi informazione *riguardante una* ***persona fisica***
identificata o identificabile *(«interessato»)*

si considera identificabile la persona fisica che può essere identificata ***direttamente o indirettamente***

il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

Tipologie di dati personali

Provided Data	Observed Data	Derived Data	Inferred Data
Dati FORNITI consapevolmente e volontariamente dati dagli individui, ad es. quando si compila un modulo online. 	**Dati OSSERVATI,** raccolti automaticamente, ad es. tramite **cookie** o **CCTV** collegati al riconoscimento facciale, domotica, elettrodomestici smart, **IoT** 	**Dati DERIVATI,** prodotti da altri dati in modo relativamente semplice e diretto, ad esempio calcolando la redditività del cliente dal numero di visite a un negozio e agli oggetti acquistati. 	**Dati DEDOTTI,** prodotti utilizzando un metodo analitico complesso per trovare le correlazioni tra i set di dati e utilizzarli per categorizzare o profilare le persone, ad esempio calcolare i punteggi di credito o predire i futuri risultati di salute. Si basano sulle probabilità e possono dunque essere meno "certi" dei dati derivati. 

** Definizioni della Foundation for Accountability Information*

Categorie di dati personali

DATI COMUNI

- Dati anagrafici (es. nome e cognome)
- Dati di contatto (es. indirizzo fisico e di posta elettronica)
- Dati fiscali (es. codice fiscale)
- Dati contabili (es. IBAN)
- Immagini
- (…)

CATEGORIE PARTICOLARI DI DATI

- Dati genetici
- Dati biometrici (es. impronta digitale)
- Dati relativi allo stato di salute
- Dati che rilevano l'appartenenza sindacale
- Dati che rivelano opinioni politiche
- (..)

RELATIVI A CONDANNE PENALI E REATI

- Qualità di imputato o indagato
- Casellario giudiziale
- Carichi pendenti

Definizione di trattamento

«Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali»

Soggetti che effettuano i trattamenti

TITOLARE («CONTROLLER»)
«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»

INCARICATI («PERSONS IN CHARGE OF THE PROCESSING")
«le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile».

RESPONSABILE («PROCESSOR»)
«la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento»

INTERESSATO («DATA SUBJECT»)
«la persona fisica cui si riferiscono i dati personali».

La figura dell'incaricato non è più espressamente prevista nel GDPR, ma il Garante nella "*Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali*" ha precisato che le disposizioni attuali che prevedono la sua designazione sono pienamente compatibili con la struttura e la filosofia del Regolamento. Anche il nuovo Codice Privacy conferma questa impostazione.

DATORE DI LAVORO AZIENDA SERVICE CUSTOMER

SERVICE PROVIDER

CLIENTI UTENTI DIPENDENTI

INDIVIDUAZIONE TRATTAMENTI DEL RESPONSABILE *CON CONTRATTO O ALTRO ATTO GIURIDICO*

RESPONSABILE PROCESSOR

TITOLARE CONTROLLER

INTERESSATI DATA SUBJECT

NEW!

SUB-RESPONSABILE

CO-TITOLARE ALTRO TITOLARE AUTONOMO

Principi generali del trattamento

liceità, correttezza e trasparenza

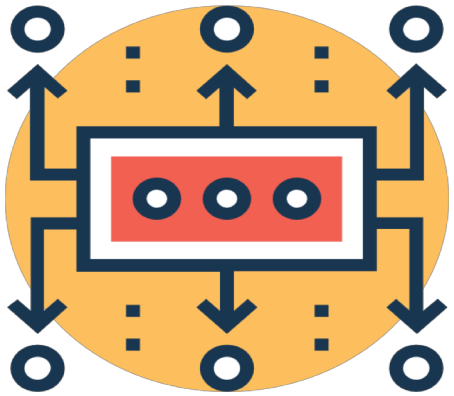
I dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.

limitazione della finalità

I dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità

esattezza

I dati personali sono 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



minimizzazione dei dati

I dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati

limitazione della conservazione

I dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

integrità e riservatezza

I dati personali sono 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, dalla distruzione o dal danno accidentali

Il titolare del trattamento è responsabile del rispetto del principi sopra indicati e deve essere in grado di dimostrarlo («***accountability***») - art. 5 co 2.

Informativa

Ogni volta che vengono raccolti i dati personali, deve essere fornita agli interessati un'**informativa** che riporti tutti i dettagli relativi al trattamento ed in particolare :

l'**identità** e i **dati di contatto** del **titolare** del trattamento e, ove applicabile, del suo rappresentante	
i **dati di contatto** del **DPO**	Novità introdotta dal GDPR
le **finalità** del trattamento nonché la **base giuridica**	La base giuridica è una novità introdotta dal GDPR
le **categorie di dati** personali in questione	Da inserire qualora i dati non siano raccolti presso l'interessato
gli **eventuali destinatari** o le eventuali categorie di destinatari dei dati personali	
l'intenzione del titolare del trattamento di **trasferire dati personali extra UE**	
il **periodo di conservazione** dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo	Novità introdotta dal GDPR

Informativa

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 dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla **portabilità** dei dati

l'esistenza del diritto di **revocare il consenso** in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca

il diritto di proporre **reclamo** a un'autorità di controllo → Novità introdotta dal GDPR

la **fonte** da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico → Da inserire qualora i dati non siano raccolti presso l'interessato

l'esistenza di un **processo decisionale automatizzato**, compresa la profilazione, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. → Novità introdotta dal GDPR

Consenso (Art. 6 co. 1, lett. A)

L'**art. 6** del GDPR («liceità del trattamento») elenca le condizioni che costituiscono le basi giuridiche sussistendo le quali il trattamento può dirsi lecito (condizioni di liceità).

a) Il **consenso espresso** dell'interessato al trattamento dei propri dati per una o più specifiche finalità.

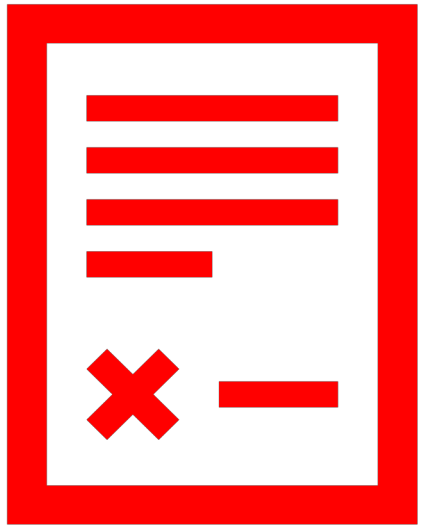
Il consenso costituisce una condizione di liceità *al pari* delle altre. È posto sullo stesso piano di quelle che nel sistema italiano sarebbero le «clausole di esonero» dal consenso.

Consenso

IL TRATTAMENTO DEI DATI PERSONALI

GDPR: COSA CAMBIA

GDPR: cosa cambia?



- Accountability del titolare
- Legittimo interesse
- Diritti degli interessati (oblio, portabilità)
- Registro dei trattamenti
- Data Protection Officer (DPO)
- Responsabilità solidale di titolare e responsabile
- Misure di sicurezza
- Privacy by design e valutazione di impatto
- Data breach
- Entità delle sanzioni

Accountability

Le definizioni ed i principi generali previsti dal Codice Privacy restano sostanzialmente invariati, ma **cambia la filosofia.**

- Viene introdotto un nuovo approccio metodologico, ***risk-based***, basato sulla protezione dei dati dell'utente e sull'effettivo rischio per ogni azienda

- Si passa da un sistema di tipo formalistico (basato sulla previsione di regole formali e su un elenco di adempimenti e misure minime da adottare), ad un sistema di governance dei dati personali basato su un'alta responsabilizzazione sostanziale («***accountability***») del **Controller**, a cui è richiesto proattività, cioè di prevenire e non correggere, nonché di **dimostrare,** tramite l'elaborazione di un idoneo sistema **documentale** di gestione della privacy (che includa l'adozione di specifici modelli organizzativi, analoghi a quelli utilizzati nell'applicazione della 231, e di appropriate **policy interne,** da esibire in caso di richiesta da parte dell'Autorità), **la conformità al GDPR** e l'adeguatezza delle proprie scelte/valutazioni.

- La «privacy» deve essere calata all'interno dei processi e dell'organizzazione aziendale, non più come elemento/adempimento successivo, ma presupposto da considerare già nella fase di progettazione dei processi, servizi, prodotti o applicativi (cfr. «**privacy by design**»).

Implicazione dell'accountability per il titolare

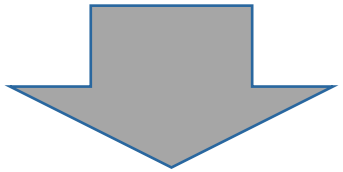
La **maggiore discrezionalità** per i TITOLARI di **DECIDERE** le **MODALITÀ** attraverso le quali conformarsi alle sue disposizioni è gravata dall'ONERE di essere IN GRADO DI DIMOSTRARE le **RAGIONI** che hanno portato a tali decisioni e le **MOTIVAZIONI** alla base delle scelte

Sarà per esempio necessario essere in grado di documentare il processo che ha portato alla valutazione di un determinato rischio in materia di sicurezza, alla decisione di notificare o meno agli interessati un «data breach», di aver attuato in relazione ad un nuovo trattamento le necessarie valutazioni legate alla privacy «by design»

Focus su accountability (art. 4, co.2 e 24)

Il TITOLARE è responsabile per la *compliance* ai principi privacy e deve essere in grado di DIMOSTRARLA (art. 4, co.2)

Tenuto conto di
NATURA, AMBITO, CONTESTO, FINALITA', RISCHI



Mette in atto

Misure **TECNICHE** ed **ORGANIZZATIVE ADEGUATE** per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR. Dette misure sono riesaminate ed aggiornate qualora necessario.

Ciò implica l'adozione di un **MODELLO PER LA PROTEZIONE DEI DATI PERSONALI** che consenta di gestire nel tempo la compliance

Legittimo interesse (art. 6 co. 1, lett. F)

Il trattamento è necessario per il perseguimento del **legittimo interesse** del titolare 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.

Il titolare deve effettuare un **BILANCIAMENTO** fra l'interesse legittimo proprio/di terzi e i diritti dell'interessato.

Legittimo interesse (art. 6 co. 1, lett. F)

Affinché il Titolare possa basare il trattamento su tale condizione di liceità è necessario che **NON prevalgano** gli **interessi** o i diritti e le libertà fondamentali dell'interessato.

Interesse legittimo del titolare

Interessi e diritti dell'interessato

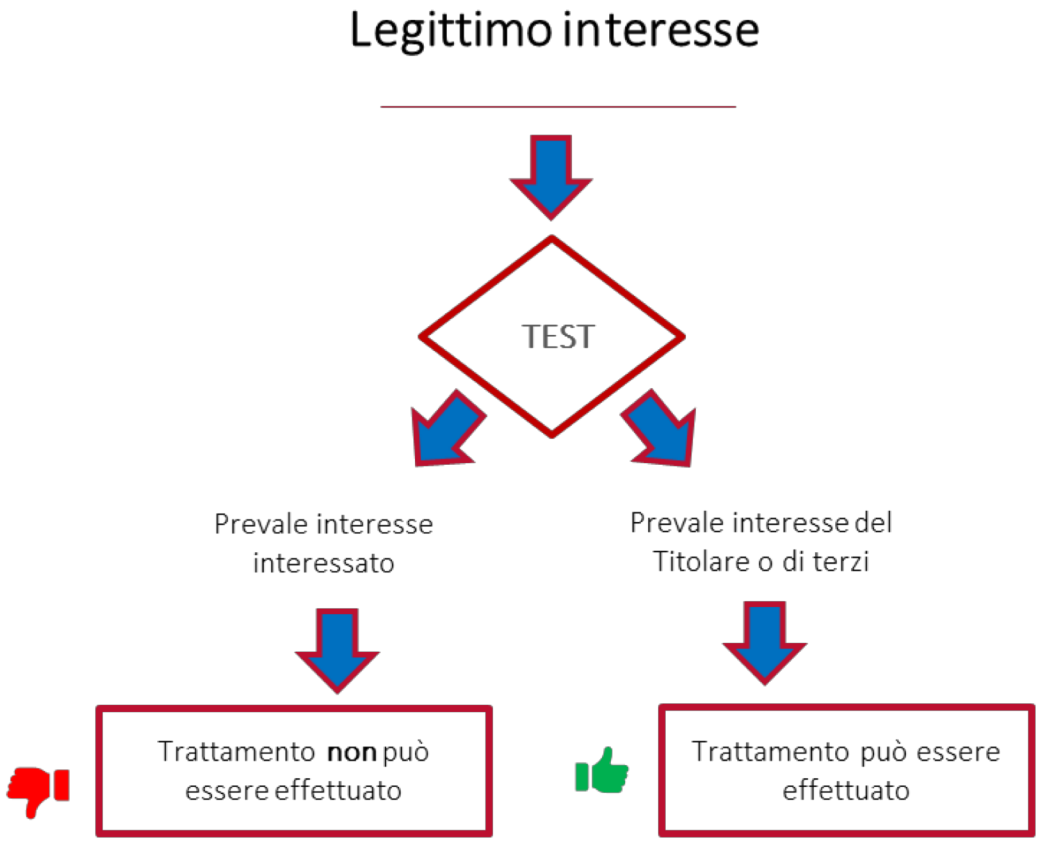
Il risultato del test di bilanciamento determinerà se il titolare **può basare o meno il trattamento su tale base giuridica.**

Bilanciamento di interessi

Altri basi giuridiche:

- **Consenso**
- **Esecuzione contratto**
- **Obbligo legale**
- **Salvaguardia interessi vitali**
- **Compito interesse pubblico**

Il trattamento è lecito *a priori* (si considera quindi soddisfatto il bilanciamento tra interessi del titolare/terzi e dell'interessato) ed è subordinato solo all'osservanza delle altre disposizioni normative applicabili.



Il test deve basarsi su elementi oggettivi, in quanto la valutazione di legittimità potrebbe essere sempre smentita da parte dell'Autorità, in tutti i casi in cui il legittimo interesse non corrisponda ad uno degli esempi cristallizzati in via generale nella norma o in provvedimenti del Garante.

Diritti degli interessati

Gli interessati hanno diritto di:

chiedere al Titolare l'**accesso** ai dati che li riguardano (cioè ottenere informazioni sul trattamento e i dati trattati)

revocare il consenso prestato in qualsiasi momento e di opporsi, in tutto od in parte, all'utilizzo dei dati

ottenere la loro **rettifica**, la **cancellazione**, l'**integrazione** dei dati incompleti, la **limitazione** del trattamento

proporre reclamo all'Autorità (etc)

ricevere i dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico (***"diritto alla portabilità"***)

Il registro dei trattamenti

Il Regolamento UE 679/2016 in materia di protezione dei dati personali, definitivamente applicabile a decorrere dal 25 maggio 2018 introduce il registro dei trattamenti di dati personali, disciplinato **dall'art. 30**

Il registro dei trattamenti **ricorda in parte l'abrogato DPS** (Documento Programmatico sulla sicurezza) tuttavia, rispetto all'abrogato DPS, risponde ad **una pluralità di finalità**, in quanto:

È volto a tenere traccia delle operazioni di trattamento effettuate all'interno della singola organizzazione

costituisce uno **strumento operativo di lavoro** mediante il quale censire in maniera ordinata le banche dati e gli altri elementi rilevanti per assicurare un sano «ciclo di gestione» dei dati personali

rappresenta un **documento probatorio** mediante il quale il Titolare del trattamento può dimostrare di aver adempiuto alle prescrizioni del Regolamento, nell'ottica del principio di *accountability*

L’obbligatorietà del registro

Occorre ricordare che il **co. V** dell’art.**30** del GDPR **esonera dall’obbligo** di **tenuta** del registro dei trattamenti le **imprese con meno di 250 dipendenti**, a meno che:

- il **trattamento** che esse effettuano possa presentare un **rischio per i diritti e le libertà dell'interessato**
- il **trattamento non sia occasionale**
- vengano **trattati categorie particolari di dati** di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10

Ad ogni modo, anche per le imprese con un **numero di dipendenti inferiore**, **la tenuta del registro** dei trattamenti costituisce un **adempimento consigliabile**, in quanto permette di mappare in maniera ordinata i trattamenti effettuati all’interno della singola organizzazione e di **dimostrare la conformità** ai principi contenuti nel Regolamento. Ciò in quanto il Titolare del trattamento è tenuto ad assolvere al principio di accountability su di lui gravante, principio che rimane pienamente valido anche per le PMI

I registri di titolare e responsabile

Il Regolamento parla di due tipologie di registri:

IL REGISTRO DEL TITOLARE

il **co. I dell'art. 30** disciplina il registro dei trattamenti del Titolare, stabilendo che ogni **Titolare del trattamento** e, ove applicabile, il suo rappresentante, tengono un registro delle **attività di trattamento svolte sotto la propria responsabilità**

IL REGISTRO DEL RESPONSABILE

il **co. II dell'art. 30** disciplina invece il registro dei trattamenti del Responsabile, stabilendo che ogni **Responsabile del trattamento** e, ove applicabile, il suo rappresentante, tengono un registro di tutte le categorie di **attività relative al trattamento svolte per conto di un Titolare del trattamento**

La tenuta del registro

Per quanto attiene alle **modalità** attraverso le quali provvedere alla **tenuta del registro**, il co. III dell'art. 30 stabilisce che:

1) i registri debbano essere tenuti in **forma scritta**

2) potranno essere tenuti anche in **formato elettronico**

Il DPO

Il Data Protection Officer (DPO) costituisce il **fulcro del nuovo sistema di *governance* in tema di protezione dati personali**, dovendo facilitare l'osservanza delle disposizioni del GDPR, minimizzare il rischio deli violazioni e agire quale intermediario fra i vari *stakeholder* (autorità di controllo, interessati e diverse *business unit* aziendali).

Nello specifico, il Data Protection Officer (DPO) è una figura di controllo e consulenza, priva di responsabilità esecutive, che:

- ✓ non deve ricevere istruzioni nell'esecuzione dei compiti e nell'interpretazione da dare a una specifica questione
- ✓ ha compiti definiti per legge:
  - controlla e supporta l'applicazione degli obblighi della nuova normativa, fornendo anche consulenza su ambiti verticali
  - funge da punto di contatto con le Autorità di controllo e gli interessati per questioni connesse al trattamento
- ✓ può "*svolgere altri compiti e funzioni*", ma a condizione che "*tali compiti e funzioni non diano adito a un conflitto di interessi*"

Obbligatorietà del DPO

- L'art. 37, primo paragrafo, del GDPR richiede la designazione del DPO in tre ipotesi:

✓ *Trattamento svolto da Autorità pubblica o da Organismo pubblico*

✓ *Attività principali del titolare o del responsabile consistono in trattamenti richiedono il monitoraggio regolare e sistematico degli interessati su larga scala*

✓ *Attività principali del titolare o del responsabile consistono nel trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e reati di cui all'art. 10 del GDPR*

- Vale la pena di sottolineare subito che l'**indeterminatezza e genericità dei criteri e termini utilizzati** nel GDPR (come ad esempio quello di "*larga scala*") determinano notevoli dubbi interpretativi e rischiano di creare incertezze sul piano giuridico.
- In proposito, importanti indicazioni sui criteri e la terminologia utilizzata nell'art. 37, paragrafo 1 del GDPR sono fornite dal Gruppo di Lavoro articolo 29 in materia di protezione dei dati personali nelle *Linee Guida sul DPO* («Guidelines on Data Protection Officers («DPOs»), emendate e revisionate il 5 aprile 2017 (WP243), che però non consentono di fugare ogni dubbio in materia.

Attività del DPO

Il Regolamento **non assegna al DPO esclusivamente un ruolo di controllo dell'applicazione del Regolamento,** ma anche di consulente interno in merito a questioni di varia natura (es. DPIA) e di punto di contatto per Autorità di controllo e interessati, oltre che per i Referenti interni del trattamento. Nello specifico:

DPO

1. *Informare e fornire consulenza al Data Controller o al Data Processor (art. 39 GDPR)*
2. *Sorvegliare l'osservanza del Regolamento (art. 39 GDPR; 4.1 Guidelines on DPOs, 5 Aprile 2017)*
3. *Cooperare con l'autorità di controllo e fungere da punto di contatto (art. 39 GDPR; 4.3 Guidelines on DPOs, 5 Aprile 2017)*
4. *Fornire, se richiesto, un parere in merito alla valutazione d'impatto (DPIA) (art. 39 GDPR; 4.2 Guidelines on DPOs, 5 Aprile 2017)*
5. *Elaborare e mantenere aggiornato un registro delle attività di trattamento (4.5 Guidelines on DPOs, 5 Aprile 2017)*
6. *Considerare debitamente i rischi inerenti al trattamento (trasversale) (art. 39 GDPR; 4.4 Guidelines on DPOs, 5 Aprile 2017)*

Requisiti del DPO

Per ricoprire il ruolo di DPO, Regolamento GDPR e WP29 («Linee Guida sui responsabili per la protezione dei dati») indicano una serie di **requisiti da rispettare**:

1) Autonomia e indipendenza
2) Assenza conflitto di interessi
3) Qualità professionali (*)
4) Capacità di assolvere i propri compiti
5) Risorse finanziarie, infrastrutture e, ove opportuno, personale (**)
6) Tempo per l'espletamento dei compiti
7) Formazione

*(*) **Conoscenza specialistica normativa e prassi in materia di protezione dei dati** ed eventuale conoscenza di settore di attività, struttura organizzativa, operazioni di trattamento svolte, sistemi informativi ed esigenze di sicurezza e protezione dell'azienda*

*(**) Alla luce delle dimensioni e della struttura del Gruppo o della singola azienda, può risultare necessario costituire un **ufficio o un gruppo di lavoro DPO** (formato dal DPO stesso e dal rispettivo personale)*

Ambito di azione del DPO

Un **gruppo imprenditoriale può nominare un unico responsabile** della protezione dei dati, a condizione che costui sia "**facilmente raggiungibile da ciascuno stabilimento**" e sia in grado di adempiere efficacemente ai propri compiti (art. 37 co. 2, GDPR)

Il WP29 precisa che il DPO deve:

- essere in condizione di **comunicare efficacemente** con gli interessati e cooperare con le autorità di controllo
- anche in virtù dell'utilizzo della **medesima lingua** usata dalle autorità garanti e dagli interessati
- essere **personalmente disponibile** in modo che gli interessati possano contattarlo (*"The personal availability of a DPO (whether physically on the same premises as employees, via a hotline or other secure means of communication) is essential to ensure that data subjects will be able to contact the DP"*)

Awareness e sanzioni su posizione e compiti del DPO

RIFERIMENTO	INADEMPIMENTO	SANZIONE
Posizione DPO (art. 38 GDPR)	Assenza di tempestivo ed adeguato coinvolgimento del DPO; assenza di risorse necessarie per assolvere ai compiti del DPO; ingerenza sulla attività del DPO (istruzioni, penalizzazione e rimozione della sua attività)	**Fino a 10.000.000 EUR, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.**
Compiti DPO (art. 39 GDPR)	Ingerenza sull'adempimento dei compiti del DPO	

DATI PERSONALI

Gdpr, attenti: fare il DPO non è un mestiere. Ecco le sue vere funzioni

Home > Sicurezza Digitale

Troppi equivoci, nel mercato, su cosa sia il responsabile della protezione dei dati (DPO). E' una figura rilevante, ma certamente non è il "centro" del sistema posto in essere dal GDPR, che nel nuovo ordinamento è sempre il Titolare del trattamento. Ecco quali sono le sue funzioni, le competenze e il ruolo

29 Set 2017

Franco Pizzetti, Professore ordinario di Diritto Costituzionale presso la Facoltà di Giurisprudenza dell'Università di Torino

GARANTE PRIVACY

Data Protection Officer, non conta la certificazione: ecco le vere competenze necessarie

Home > Sicurezza Digitale

Le attestazioni delle competenze professionali raggiunte o della formazione eseguita possono essere utili per valutare un candidato ma non rappresentano e non equivalgono a una "abilitazione" allo svolgimento del ruolo del DPO

29 Set 2017

Misure di sicurezza – art. 32 GDPR

I presupposti (tenendo conto di)

- Stato dell'arte
- Costi di attuazione
- Natura
- Oggetto
- Contesto
- Finalità del trattamento
- Rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche

Ma anche di (in special modo di)
rischi presentati dal trattamento (su dati personali trasmessi, conservati o comunque trattati)
che derivano in particolare **da:**

- Distruzione
- Perdita
- Modifica
- Divulgazione non autorizzata
- Accesso, in modo accidentale o illegale

Misure di sicurezza – art. 32 GDPR

MISURE DI SICUREZZA ADEGUATE

ORGANIZZATIVE **TECNICHE**

per garantire un livello di sicurezza adeguato al ***rischio***

Misure di sicurezza – art. 32 GDPR

Per ASSICURARE, GARANTIRE E METTERE IN ATTO:

Riservatezza ovvero garanzia di confidenzialità delle informazioni, riduzione dei rischi connessi all'accesso o all'uso delle informazioni in forma non autorizzata;

Integrità ovvero garanzia di correttezza dei dati, l'informazione non deve subire modifiche o cancellazioni;

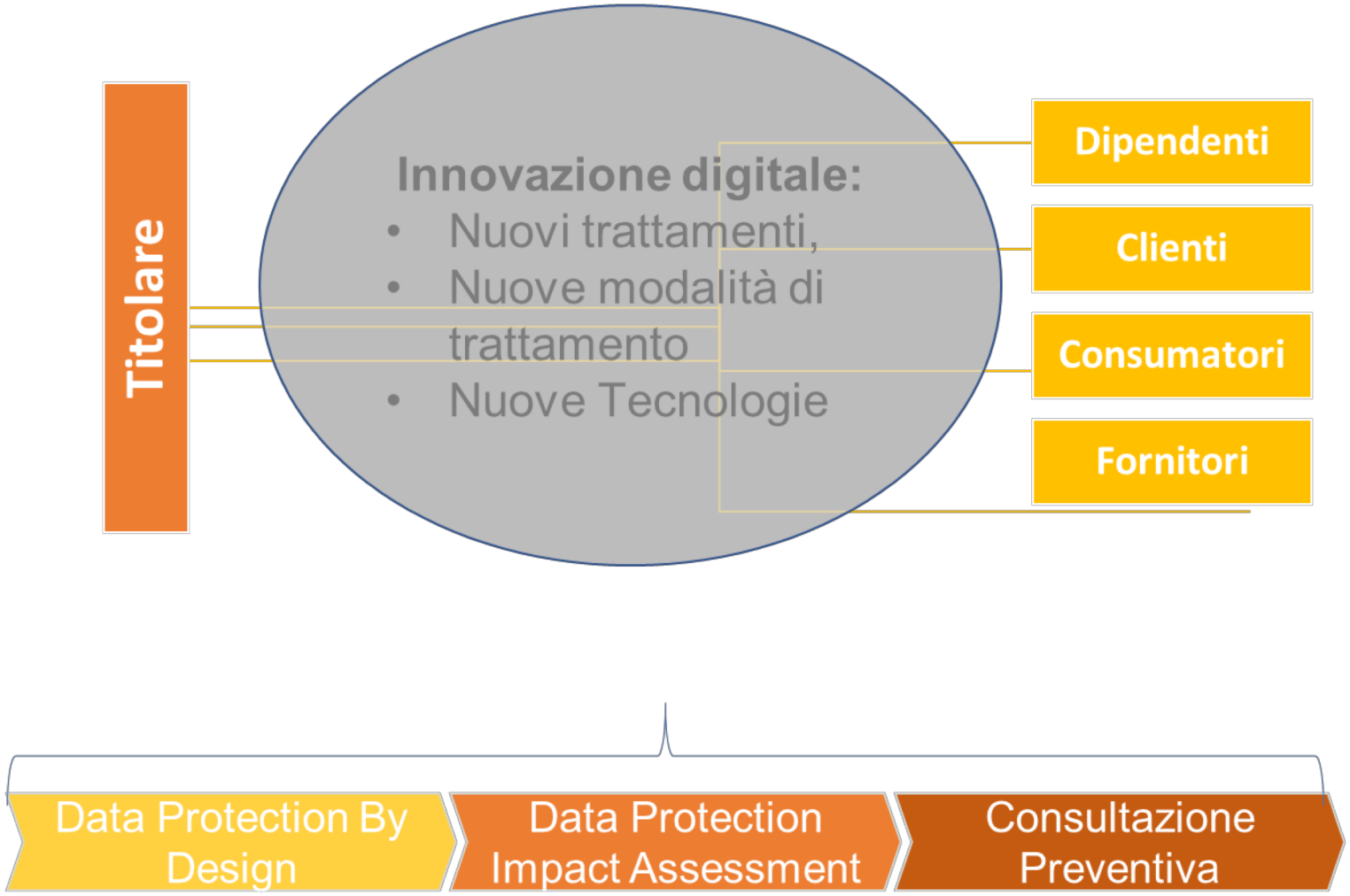
Disponibilità ovvero garanzia di accesso e di usabilità dei dati nei modi e nei tempi richiesti;

Resilienza dei sistemi e dei servizi che trattano i dati personali;

Ripristino tempestivo della disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;

Procedure per **provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative** al fine di garantire la sicurezza del trattamento.

La gestione dell'innovazione nel GDPR



Data Protection by Design

Articolo 25
Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

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.

E' pensata per essere una prassi operativa aziendale che riguarda tutti i nuovi trattamenti o la revisione sostanziale di trattamenti in corso.

Riguarda la fisiologia del trattamento, cioè come viene effettuato nella normalità operativa.

Non riguarda solo la sicurezza ma tutti i requisiti che un trattamento deve rispettare.

Richiede una metodologia documentata, non necessariamente complessa

Data Protection by Default

Articolo 25
Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

1. …
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.

Riguarda la configurazione dei prodotti e dei servizi all'atto dell'installazione.

Incide sulle procedure di rilascio dei prodotti e dei servizi

Valutazione d'impatto

Cosa è la «valutazione d'impatto»?

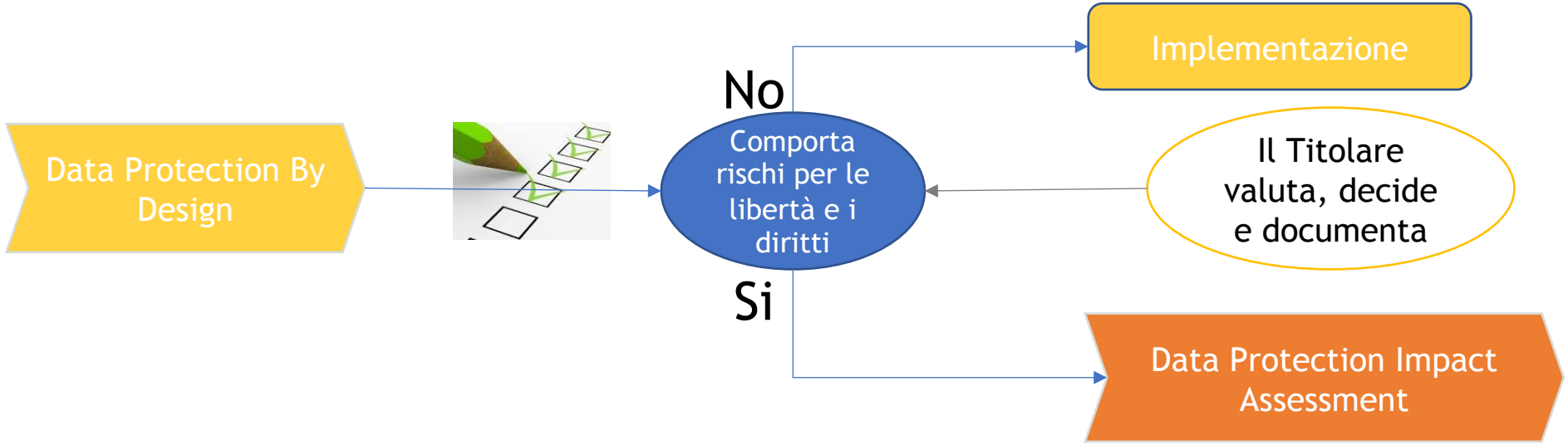
È un processo volto a **descrivere i trattamenti**, **valutarne** la **necessità** e la **proporzionalità** e aiutare a **gestire i rischi** per i diritti e le libertà delle persone fisiche derivanti dal trattamento, valutandoli e determinando le misure per indirizzarli.

La DPIA è uno strumento importante per l'*accoutability* in quanto non solo aiuta i titolari a **rispettare** i requisiti del GDPR, ma anche a **dimostrare** che sono state adottate misure appropriate per garantire il rispetto del regolamento.

Deve essere effettuata «**prima del trattamento**», in coerenza con i principi di privacy *by design* e by default.

«*In other words, a DPIA is a process for building and demostrating compliance*»

Data Protection by Design



Una procedura e una metodologia:

- Chi: individuare e formare
- Cosa: DP by design, DP Impact assessment
- Come: metodologia aziendale, linee guida, …
- Quando: change, innovation, update
- Dove: tutti i dipartimenti

Trattamenti con rischi elevati

Riferimento normativo
artt. 35 e 36 del GDPR

- L'istituto della «*notifica preliminare*» è sostanzialmente sostituito nel **GDPR** dall'obbligo, gravante **in capo al Titolare,** di effettuare la **valutazione d'impatto** di cui all'art. 35, la c.d. **DPIA**, «*quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un **rischio elevato** per i diritti e le libertà delle persone fisiche*».

- L'obbligo di consultazione al Garante è rimasto residuale ai sensi dell'art. 36 per le ipotesi in cui la valutazione d'impatto indichi che il trattamento presenterebbe un **rischio elevato** che non può essere attenuato con «*misure opportune in termini di tecnologia disponibile e costi di attuazione*» (così considerando 84).

Principi di base della DPIA

In linea con il *risk-based approach* di cui al GDPR, la DPIA

NON È OBBLIGATORIA per tutte le operazioni di trattamento…

… **ma È RICHIESTA** qualora il trattamento, allorché prevede in **particolare l'uso di nuove tecnologie**, comporta un **RISCHIO ELEVATO** per i diritti e le libertà delle persone fisiche

Si pone quindi la necessità di individuare dei **CRITERI COMUNI** a tutti i Titolari del trattamento al fine di **individuare le operazioni di trattamento che necessitano dell'effettuazione di una valutazione d'impatto.**

Soggetti coinvolti nella DPIA

Data Breach

VIOLAZIONE DEI DATI PERSONALI

«*La 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*»

Il Titolare deve **notificare alle Autorità Garanti**, senza ingiustificato ritardo (e, ove possibile, entro **72 ore**) eventuali violazioni dei dati e **comunicarle agli interessati** senza ingiustificato ritardo, laddove vi sia un rischio elevato per i diritti e le libertà delle persone fisiche.

Notifica dei Data Breach all'autorità

La notifica all'Autorità deve, fra l'altro, descrivere:

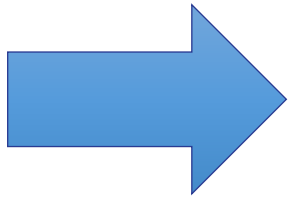
- la natura della violazione dei dati personali;
- ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio, al fine di consente all'autorità di controllo di verificare il rispetto di quanto previsto nell'art. 33.
Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

Notifica dei Data Breach all'autorità

Non tutti gli incidenti di sicurezza sono violazioni di dati personali: servono criteri predefiniti per decidere cosa fare

Il Titolare è tenuto a documentare il modo in cui viene a conoscenza della violazione. Ritardi nell'individuazione del data breach dovute a carenza di misure tecniche e organizzative o ad omessi controlli interni costituiscono elementi che il Garante dovrà vagliare in sede di provvedimenti o di misure sanzionatorie.



72 ore sono poche: bisogna aver pre impostato la strategia di risposta all'incidente per essere in grado di rispettare i termini.

Comunicazione dei Data Breach all'interessato

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento è tenuto a comunicare la violazione all'interessato senza ingiustificato ritardo.

Tale comunicazione è volta a ridurre il danno che può derivare all'interessato in conseguenza della violazione (consentendogli di adottare contromisure idonee a contenere gli effetti dannosi della violazione).

La comunicazione all'interessato non è richiesta se erano state applicate ai dati oggetto della violazione misure di sicurezza adeguate destinate a rendere i dati personali incomprensibili a (quali la cifratura) oppure se sono successivamente adottate misure atte a scongiurare un rischio elevato.

La valutazione sulla necessità della comunicazione è in capo al titolare, ma … l'autorità può obbligarlo ad effettuarla nel caso in cui non l'abbia ritenuta necessaria.

Illeciti e sanzioni

Illecito penale

Trasgressione di una norma posta a tutela della comunità (reato)

Le ipotesi di illecito penale sono tipizzate (Art. 25 2° comma Cost.)

Responsabilità penale

Ad oggi esistono pochi precedenti che confermano una responsabilità penale per illecito trattamento di dati. Nelle sentenze non rileva il ruolo «privacy» assunto dall'individuo che, trattandosi di responsabilità personale, prescinde dallo stesso.

Sanzione penale

Illecito amm.vo

Violazione di una norma giuridica cui viene comminata una sanzione amministrativa pecuniaria

Responsabilità amm.va

Vi sono numerosissimi precedenti che confermano la responsabilità amministrativa del titolare per illecito trattamento di dati (cfr. statistiche e dati del Garante Privacy).

Sanzione amm.va

Illecito civile

Responsabilità per attività pericolose (art. 2050 c.c.)

Il danneggiante è tenuto al risarcimento del danno patrimoniale e del danno non patrimoniale.

Responsabilità civile

Ad oggi vi sono precedenti giurisprudenziali che confermano una responsabilità civilistica del solo titolare per illecito trattamento di dati.

Risarcimento danno

L'art. 83 del GDPR distingue
due gruppi di sanzioni amministrative

Sanzioni più alte

fino a € **20.000.000** o
al **4%** del fatturato globale annuo

- **violazione delle obbligazioni di titolare e responsabile** inclusi gli obbligi di sicurezza e data breach notification (art. 83, par. 4 del GDPR)

Sanzioni più basse

fino a €. 10.000.000 o,
in caso di undertaking, al 2% del fatturato,
a seconda di quale risulti la sanzione più elevata

- **violazioni dei principi del trattamento**, incluse le condizioni per il consenso
- **violazione dei diritti degli interessati**
- **inosservanza delle norme in tema di trasferimento internazionale dei dati** (art. 83, par. 5 del GDPR)

La sanzioni non sono imposte in riferimento al fatturato della specifica società responsabile della violazione, ma alle revenue di un **"undertaking",** da intendersi, come chiarito dal WP29 n. 253, come gruppo di imprese

Sanzioni penali

Spetta agli **Stati Membri** stabilire le norme relative alle sanzioni penali per le violazioni del GDPR.

Tali sanzioni devono essere effettive, proporzionate e dissuasive.

Riferimento normativo
Considerando 149 e art. 84 co. 1

SANZIONI AMMINISTRATIVE NEL NUOVO CODICE PRIVACY

FATTISPECIE CON SANZIONE PIÙ BASSA

(Art. 166, co. 1)

- **violazione dell'obbligo di redigere un'informativa con linguaggio semplificato per i minori** (Art. 2, quinquies, co. 2)
- **violazione dei provvedimenti generali del Garante** con riguardo a **trattamenti per l'esecuzione di un compito di interesse pubblico che presentano rischi elevati** (Art. 2-quinquiesdecies)
- Violazioni relativi alle cartelle cliniche (**Art. 92, co. 1**) e a certifica certificati di assistenza al parto (**Art. 93, co. 1**)
- **Violazioni di norme relative ai servizi di comunicazione elettronica** (quali l'**Art. 123, co. 4** sull'informativa inerenti ai dati di traffico), l'**Art. 128 su**l trasferimento automatico delle chiamate , l'**Art. 129, co.2** sugli elenchi dei contraenti, l'**Art. 132-ter** sulla *a*lla sicurezza dei trattamenti effettuati da fornitori di servizi di comunicazione elettronica
- mancata effettuazione della valutazione di impatto di cui all'art. 110, co. 1, primo periodo per le **attività di ricerca medica, biomedica o epidemiologica** ovvero mancata sottoposizione del programma di ricerca a consultazione preventiva del Garante a norma del terzo periodo del predetto comma

10 milioni di euro

o

2% fatturato mondiale annuo

(art. 83, par. 4, GDPR)

SANZIONI AMMINISTRATIVE NEL NUOVO CODICE PRIVACY

FATTISPECIE CON SANZIONE PIÙ ALTA

- Violazione dell'*art. 2-ter* relativo alla base giuridica del trattamento effettuato per **l'esecuzione di un compito di interesse pubblico**
- Violazione dell'*art. 2-quinquies, co. 1* riguardante **il consenso del minore in relazione ai servizi della società dell'informazione**
- Violazioni *dell'Art. 2-sexies* relativo al trattamento di **categorie particolari di dati per motivi di interesse pubblico rilevante**
- Violazione delle misure di garanzia per il trattamento dei **dati biometrici** riguardo alle **procedure di accesso fisico e logico** da parte dei soggetti autorizzati (*art. 2-septies, co. 7)*
- Violazione dei principi relativi al trattamento di dati relativi a condanne penali e reati (*Art. 2-octies*)
- Violazione dei **diritti riguardanti le persone decedute** (*Art. 2-terdecies, co. 1, 2, 3 e 4*)
- Violazione della disciplina sulla **diffusione di provvedimenti giudiziari contenenti dati identificativi degli interessati** (*art. 52, co. 4 e 5*)
- Violazione degli adempimenti previsti per il **trattamento dei dati in ambito sanitario** (*Art. 75-78-79-80-82-92, co. 2- 93, co. 2 e 3)*
- Violazione della disciplina sul **trattamento dei dati relativi a studenti** (*Art. 96*)
- Violazione di disposizioni in materia di **trattamento dei dati a fini di archiviazione nel pubblico interesse, ricerca scientifica o storica o a fini statistici** (*Art. 99, 100, co. 1, 2 e 4, 101, 105, co. 1, 2 e 4, 110-bis, co. 2 e 3)*

(Art. 166, co. 2)

20 milioni di euro

o

4% fatturato mondiale annuo

(art. 83, par. 5, GDPR)

SANZIONI AMMINISTRATIVE NEL NUOVO CODICE PRIVACY

FATTISPECIE CON SANZIONE PIÙ ALTA

- Violazione delle disposizioni riguardanti il trattamento nell'ambito del lavoro (a*rt. 111-111-bis -116, co. 1)*
- Violazione dell'Art.120, co.2 relativo alle assicurazioni (banca dati dei sinistri)
- Violazioni di quasi tutte le previsioni relativa ai servizi di comunicazioni elettroniche (*artt.-122, 123, co. 1, 2, 3 e 5, 124, 125, 126-130, co. 1, 2, 3, 4 e 5,131, 132, 132-bis, co. 2,132-quater)*
- Violazione della disposizione in materia di **richiesta di informazioni e di esibizione di documenti** da parte del **Garante** (*Art. 157*)
- Violazione delle **regole deontologiche** di cui all'*art. 2-quater* previste per i trattamenti necessari per adempiere un obbligo legale o per l'esecuzione di un compito di interesse pubblico (Art. 6, par. 1, lett. c) ed e) GDPR), per il trattamento di dati genetici e biometrici relativi alla salute (Art. 9, par. 4 GDPR) e delle disposizioni di cui al Capo IX del GPDR relative a specifiche situazioni di trattamento di cui il Garante promuove l'adozione;
- Violazione delle **misure di garanzia** disposte dal Garante per il trattamento di dati genetici e biometrici relativi alla salute di cui all'*art. 2-septies*

(Art. 166, co. 2)

20 milioni di euro

o

4% fatturato mondiale annuo

(art. 83, par. 5, GDPR)

SANZIONI AMMINISTRATIVE NEL NUOVO CODICE PRIVACY

Organo competente ad irrogare le sanzioni è il Garante, il quale dovrà tener in debito conto le circostanze di cui all'art. 83, co. 2 GDPR, ossia:

- la natura, la gravità e la durata della violazione,
- il carattere doloso o colposo della stessa,
- le categorie di dati personali interessate dalla violazione,
- eventuali precedenti violazioni commesse ecc.

I proventi delle sanzioni, nella misura del **50%** del totale annuo, sono riassegnati al fondo destinato alle spese di funzionamento del Garante, per essere destinati alle specifiche attività di sensibilizzazione e di ispezione, nonché di attuazione del Regolamento.

SANZIONI PENALI NEL NUOVO CODICE PRIVACY

Vecchio codice	Nuovo codice
Trattamento illecito di dati (Art. 167)	Trattamento illecito di dati (Art. 167) **RIFORMULATO**
/	Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala (Art. 167-bis) NEW
/	Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala (Art. 167-ter) NEW
Falsità nelle dichiarazioni e notificazioni al Garante (Art. 168)	Falsità nelle dichiarazioni al Garante **e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante** (Art. 168)
Omissione delle misure minime di sicurezza (Art. 169)	**ABROGATO**
Inosservanza di provvedimenti del Garante (Art. 170)	Inosservanza di provvedimenti del Garante (Art. 170)
Altre fattispecie (art. 171)	**Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori (Art. 171)**

SANZIONI PENALI NEL NUOVO CODICE PRIVACY

Chiunque,
al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato:

→ REATI A DOLO SPECIFICO

ARRECA NOCUMENTO ALL'INTERESSATO

Art. 167, co. 1

Servizi di comunicazioni elettroniche

Violando le norme relative ai **dati di traffico**, ai dati relativi all'ubicazione, all'invio delle comunicazioni indesiderate e il provvedimento del Garante in tema di elenchi cartacei elettronici a disposizioni del pubblico ***(condotte inalterate rispetto al previgente art. 167)***

è punito con → Reclusione **da 6 mesi a 1 anno**

Art. 167, co. 2

Categorie particolari di dati e dati «giudiziari»

Trattando **categorie particolari di dati** o **dati relativi a condanne penali e reati** in violazione dell'artt. 2-sexies e 2-octies o delle misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute (art. 2-septies) ovvero operando in violazione delle misure prescritte dal Garante per i trattamenti svolti per l'esecuzione di un compito di interesse pubblico che possono presentare rischi elevati (art. 2-quinquiesdecies)

Art. 167, co. 3

Trasferimento extra-UE

Procedendo al **trasferimento dei dati extra-UE** al di fuori dei casi consentiti dal Regolamento ***(condotta già espressamente sanzionata in via amm. dal GDPR all'art. 83, 5° co.)***

è punito con → Reclusione **da 1 a 3 anni**

Salvo che il fatto costituisca più grave reato

SANZIONI PENALI NEL NUOVO CODICE PRIVACY

Chiunque,
al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato:

→ REATI A DOLO SPECIFICO

Art. 167-bis, co.

Comunica o diffonde un archivio automatizzato o una parte sostanziale di esso contenente dati personali trattati **su larga scala**

è punito con → Reclusione **da 1 a 6 anni**

Art. 167-bis co. 2

Comunica o diffonde, senza consenso (laddove questo sia richiesto) un archivio automatizzato o una parte sostanziale di esso contenente dati personali trattati **su larga scala**

è punito con → Reclusione **da 1 a 6 anni**

Art. 167-ter, co. 1

acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento **su larga scala**

è punito con → Reclusione **da 1 a 4 anni**

"LARGA SCALA"

Da notare che né il GPPR né il decreto contengono una definizione di "*larga scala*", tantomeno le linee guida del Working Party ex art. 29 chiariscono in modo certo e definitivo cosa debba intendersi con tale locuzione, offrendo criteri alternativi non fondati su elementi quantitativi, ma su indicazioni generiche suscettibili di diversa interpretazione.

Salvo che il fatto costituisca più grave reato