Ordine Ingegneri di Forlì-Cesena

GENERAL DATA PROTECTION REGULATION EU 679/2016

MISURE TECNICHE E ORGANIZZATIVE ADEGUATE E IMPATTO SUI SISTEMI INFORMATIVI

16 Maggio 2018

Carolina Maggioli
carolina@maggioli.net
+39 335 5270262

Agenda

Diritti dell'interessato e Principi del Trattamento

***Accountability* (Art. 24)**

***Registro del Trattamento* (Art. 30)**

Misure tecniche e organizzative adeguate (Art. 25):

- ***Privacy by Design***
- ***Privacy by Default***
- Minimizzazione
- **Pseudonimizzazione**
- **Cifratura**
- Anonimizzazione

Sicurezza del Trattamento (Art. 32)

Il **rischio GDPR**

Valutazione di impatto (DPIA) (Art. 35)

Gestione delle violazioni (*Data Breach)* (Artt. 33, 34)

Un possibile percorso di adeguamento

Cambio di prospettiva rispetto al vigente Codice Privacy (196/2003)
Conformità non più alle SOLUZIONI ma ai ***PRINCIPI* del Trattamento**

OBIETTIVI

La protezione dei dati per proteggere gli interessati e dei loro ***DIRITTI***

Approccio "***user-centric***" durante tutto il Ciclo di vita del trattamento

Accountability del Titolare (Art. 24):

- **maggiore libertà** e ***responsabilizzazione*** nelle valutazioni riguardanti il trattamento
  - nel rispetto dei Principi del trattamento
  - nel rispetto dei Diritti dell'interessato

- obbligo di ***comprovare*** tali valutazioni, decisioni (analisi preventive, monitoraggio continuo, ...)

6 PRINCIPI del TRATTAMENTO (Artt. 5,6)

1	LICEITÀ, CORRETTEZZA e TRASPARENZA
2	LIMITAZIONE delle FINALITÀ
3	MINIMIZZAZIONE dei DATI
4	ESATTEZZA
5	LIMITAZIONE della CONSERVAZIONE
6	INTEGRITÀ e RISERVATEZZA

Raccolta

Registrazione

Organizzazione

Strutturazione

Conservazione

Adattamento o modifica

Estrazione

Consultazione

Utilizzo

Comunicazione mediante trasmissione

Diffusione o qualsiasi altra forma di messa a disposizione

Raffronto o interconnessione

Limitazione, cancellazione o distruzione

CON O SENZA L'AUSILIO DI PROCESSI AUTOMATIZZATI

I DATI PERSONALI DEVONO ESSERE:

trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («**liceità, correttezza e trasparenza**»);

raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità («**limitazione della finalità**»);

adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione dei dati**»);

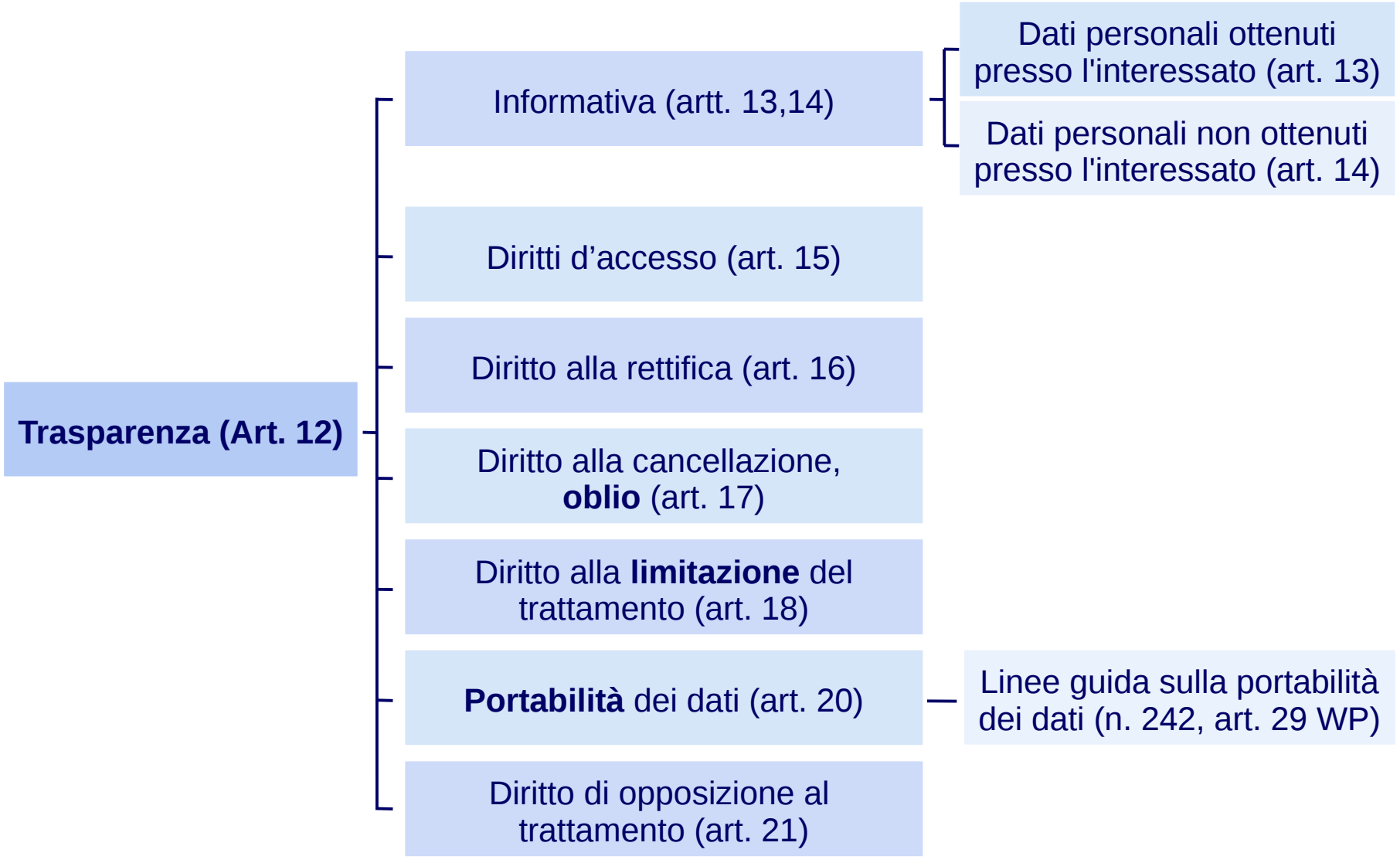
esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («**esattezza**»);

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; («**limitazione della conservazione**»);

trattati in maniera da garantire un'adeguata sicurezza dei dati personali, («**integrità e riservatezza**»).

Il titolare del trattamento è competente per il rispetto dei suddetti principi e in grado di comprovarlo («responsabilizzazione»).

DIRITTI dell'INTERESSATO



Portabilità (Art. 20)

- L'interessato vuole ricevere alcuni suoi dati personali e memorizzarli su un proprio dispositivo per un successivo utilizzo personale
- L'interessato richiede la trasmissione dei dati personali da un Titolare ad un altro (es. Un diverso fornitore di servizi), *senza impedimenti* da parte del primo (*vendor lock-in*). Trasferibili direttamente (se tecnicamente possibili)

DATI PORTABILI:

- trattati con **mezzi automatizzati** (NO archivi cartacei)
- trattati sulla base del consenso dell'interessato o di un contratto stipulato con l'interessato (NO interesse pubblico o legittimo – considerando 68)
- **riferibili all'interessato** (NO anonimi)
- Possono contenere anche dati di terzi (tabulati telefonici, transazioni bancarie, contatti)
- *SOLO* i dati **forniti** dall'interessato… (non raccolti automaticamente, derivati o dedotti)

QUALE DEVE ESSERE IL FORMATO dei dati portabili?

INTEROPERABILE (Considerando 68)

- strutturato
- di uso comune
- leggibile
- non proprietario
- aperto

Esempio:

Portabilità dei messaggi contenuti in una casella di posta elettronica:

un formato **PDF non** sarebbe **adatto**

- i messaggi non sarebbero più riutilizzabili come nel formato originale
- l'interessato perderebbe le funzionalità tipiche della posta elettronica

Tempistica (Art. 13): ***Senza ingiustificato ritardo e comunque entro un mese dal ricevimento della richiesta***
in casi di particolare complessità, entro un massimo di 3 mesi
(interessato informato entro un mese dall'originale richiesta)

COME GARANTIRE AGLI INTERESSATI QUESTO DIRITTO?

Individuare le misure e gli strumenti più adeguati:

- Moduli standard che l'utente può compilare per avanzare la propria richiesta

- Tool informatici che permettano di soddisfare la richiesta dell'utente

Queste si possono definire le ***nuove misure minime, sia tecniche che organizzative.*** I mezzi per attuarle non sono stabiliti in termini fissi

Registro dei Trattamenti (Art. 30)

Il Regolamento UE 679/2016 in materia di protezione dei dati personali introduce il **registro dei trattamenti di dati personali**, disciplinato dall'art. 30, che ricorda in parte l'abrogato ***DPS*** (Documento Programmatico sulla sicurezza) tuttavia, rispetto allo stesso, 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

Obbligatorietà del registro dei trattamenti (Art. 30)

Le GDPR imprese con meno di 250 dipendenti non hanno l’obbligo di tenuta del registro dei trattamenti le 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 consigliato***, 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.

Regole per la costruzione del registro dei trattamenti

Occorre ricordare che ***non esiste una regola generale*** che stabilisca le modalità attraverso le quali costruire il registro dei trattamenti:

l'art. 30 del GDPR, infatti, si limita ad indicare quali sono gli elementi che il registro deve necessariamente contenere.

Potrebbe comunque essere costituito da ***più moduli per individuare i trattamenti*** e gli applicativi/servizi di riferimento

inoltre, potrebbe contenere informazioni ulteriori rispetto a quelle obbligatorie sulla base di quanto previsto dal GDPR… "per la costruzione di uno strumento che consenta di":

• impostare un modello che possa garantire la dimostrabilità degli adempimenti previsti dalla normativa;

• mantenere un collegamento diretto con i principali «oggetti aziendali» (es. mappa dei processi aziendali, database, software gestionali, etc.)

MISURE da adottare in fase di PROGETTAZIONE

Si tratta di nuove ***misure tecniche e organizzative.*** I mezzi per attuarle non sono stabiliti in termini fissi

Le impostazioni di Privacy by Design, by Default riguardano soprattutto chi progetta, crea, gestisce i sistemi hardware e software.

A noi spetta però **controllare** che i fornitori si adeguino. Con il tempo diventerà normale richiedere queste impostazioni e caratteristiche per i nostri database, sistemi gestionali, etc.

Privacy fin dalla progettazione - *Privacy by Design* (Art. 25)

Il principio è di non pensare a proteggere i dati, **ma di progettarli in modo da non avere bisogno di proteggerli.**

Dove possibile si usano dati **anonimi** (quindi il GDPR non si applica)

altrimenti si adotta il principio di **minimizzazione** (mettiamo a disposizione degli incaricati solo la minima parte dei dati personali che devono essere trattati)

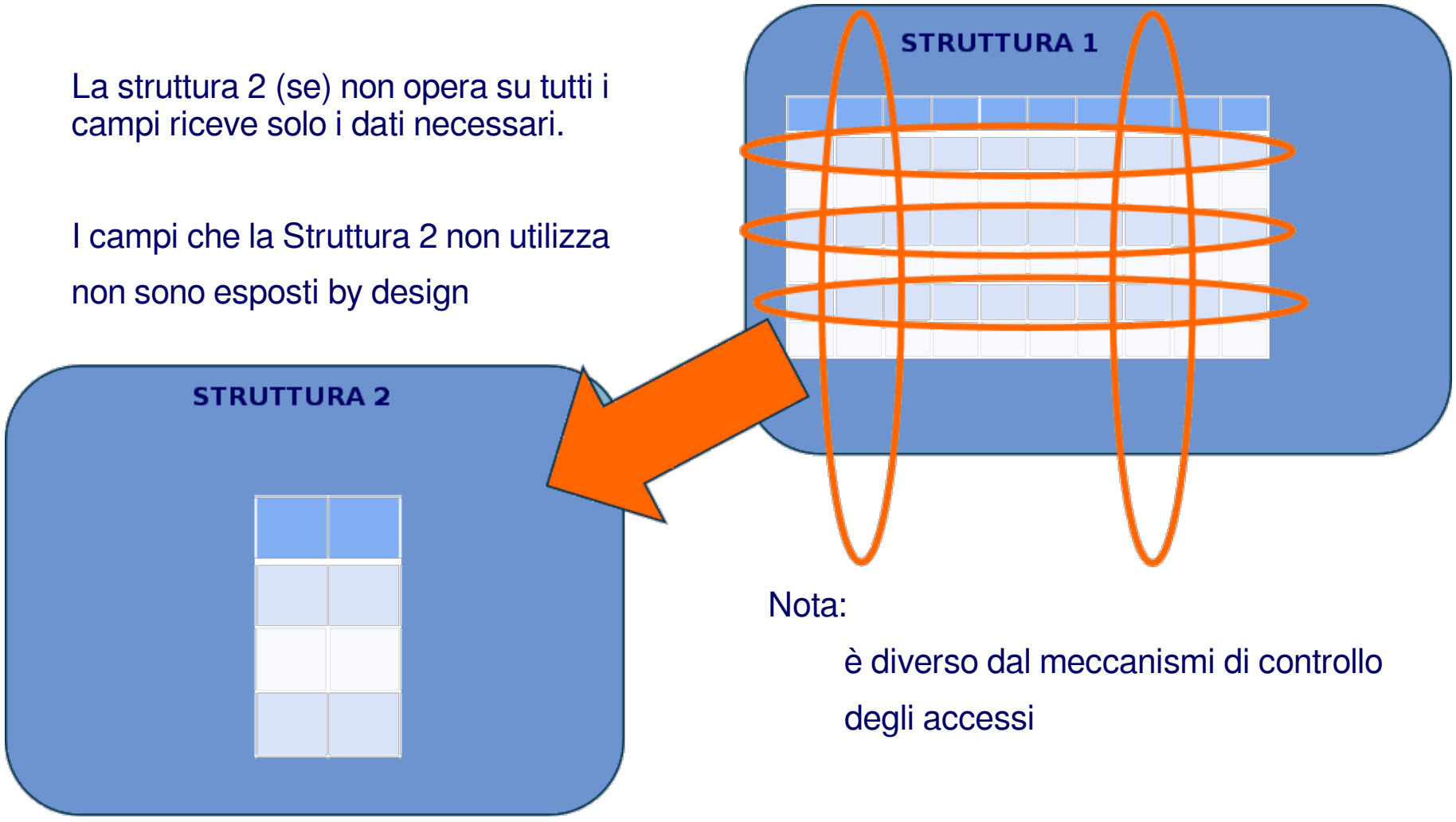
Si mantiene l'***identificazione*** solo quando è **necessaria** alle finalità del trattamento.

Minimizzazione

È un **principio** del trattamento dei dati personali

La struttura 2 (se) non opera su tutti i campi riceve solo i dati necessari.

I campi che la Struttura 2 non utilizza non sono esposti by design



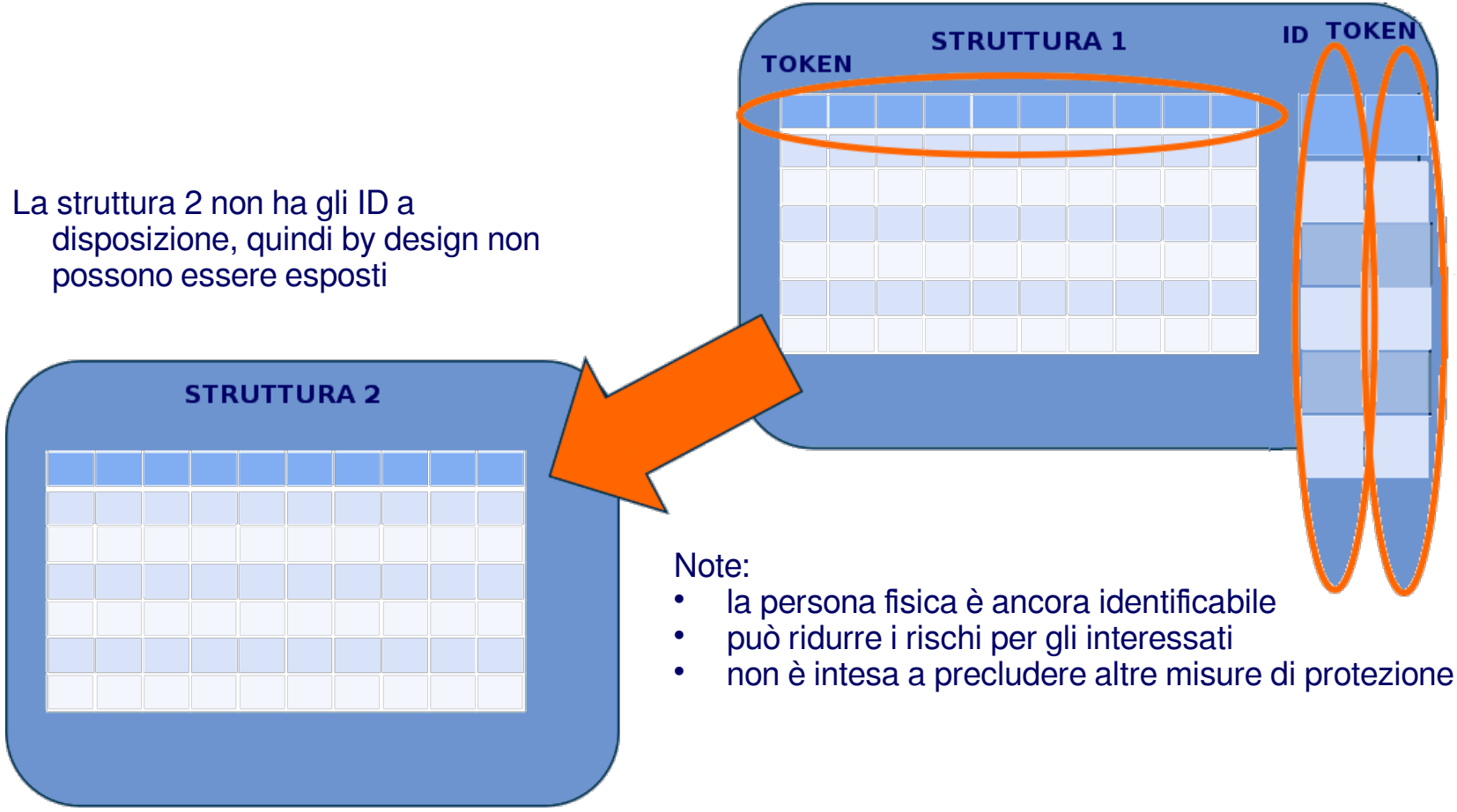
Nota:

è diverso dal meccanismi di controllo degli accessi

Pseudonimizzazione (Art. 4)

Misura di sicurezza dei dati personali in modo tale che **non possano più essere attribuiti a un interessato** specifico senza l'utilizzo di informazioni aggiuntive

a condizione che tali informazioni aggiuntive siano **conservate separatamente** e soggette a misure tecniche e organizzative intese a **garantire** che tali dati personali non **siano attribuiti a una persona fisica identificata o identificabile**



La struttura 2 non ha gli ID a disposizione, quindi by design non possono essere esposti

Note:

- la persona fisica è ancora identificabile
- può ridurre i rischi per gli interessati
- non è intesa a precludere altre misure di protezione dei dati

Cifratura (Art. 34)

È una **misura** di sicurezza dei dati personali, ***destinata a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi*** (Art. 34)

È matura in quanto ampiamente usata per garantire la sicurezza informatica in ambiti diversi da quello della Data Protection (Firma digitale, navigazione sicura HTTPS)

Gli sforzi di implementazione sono già facilmente stimabili

In caso di violazione di dati protetti da cifratura non è richiesta la comunicazione all'interessato .

Anonimizzazione

È una **tecnica** per far **perdere** ai dati la qualifica di dato personale

Le norme sulla protezione dei dati non si applicano a informazioni anonime, vale a dire:

- informazioni che non si riferiscono a una persona fisica identificata o identificabile

- dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato (Considerando 26)

Privacy by Default (Art. 25)

È soprattutto un principio organizzativo: **privacy come impostazione predefinita**

Saranno trattati solo i dati personali necessari per ogni specifica finalità di trattamento.

Il ***default*** è che i requisiti di privacy e il trattamento corretto si applicano sempre e in toto, salvo dove ci siano eccezioni giustificate per riduzioni o limitazioni

Questo principio deve essere implementato a tutti i livelli dalle *policy* ai ***processi***, alle ***procedure***, alle ***configurazioni applicate***

Esempio: Politica aziendale e procedura operativa

Policy: un dato personale è trattato solo quando ne è stata esplicitamente valutata la necessità,

Trattamento: titolari e/o responsabili, nei diversi contesti, verificano che questa valutazione sia disponibile e li comprenda, prima di iniziare il trattamento

E PER GARANTIRE LA SICUREZZA DEL TRATTAMENTO IN TUTTE LE FASI DEL SUO CICLO DI VITA?

Altre misure tecniche e organizzative adeguate (Artt. 24, 32) ad assicurare, garantire e mettere in atto:

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

Lucchetti e serrature

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

Firewall

Antivirus/antimalware

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

Allarmi anti-intrusione

Sistemi di sorveglianza

Resilienza dei sistemi e dei servizi che trattano i dati personali

Backup, Recovery

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

Disaster Recovery

Business Continuity

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

Governance,

Risk & Compliance

Selezione di altre tecnologie e strumenti: implementazione ***tool IT GRC***

Come si valuta l'ADEGUATEZZA

Si deve tener conto dei rischi presentati da trattamenti di dati derivanti in particolare:

- dalla distruzione,
- dalla perdita,
- dalla modifica,
- dalla divulgazione non autorizzata
- dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, memorizzati o comunque trattati.

Rischio (definizione)

Rischio - è il risultato finale, diretto, indiretto o consequenziale ad un’azione volontaria, involontaria o ad un evento accidentale.

La definizione più utilizzata nelle metodologie di analisi dei rischi analisi dei rischi identifica il rischio come prodotto fra impatto [danno] e probabilità che un evento pericoloso si realizzi

Concetto di RISCHIO

Non più una specifica tecnica per addetti ai lavori, bensì criterio di valutazione utilizzato in moltissime aree, componenti come ***probabilità*** e ***impatto*** sono ormai di uso comune

Nel GDPR il rischio è nominato più di 70 volte in diversi ambiti e contesti:

- Valutazione d'impatto (***Data Protection Impact Assessment***) (Art. 35)

- Gestione delle violazioni (***Data breach Notification***) (Artt. 33,34)

IGNORATO
Un determinato asset non è considerato critico

ACCETTATO
Valutate le implicazioni del rischio associato a un asset si è ritenuto che nessun provvedimento fosse necessario

MITIGATO
Definito un processo strutturato di gestione del rischio introducendo opportune soluzioni e procedure

TRASFERITO
Stipulate polizze assicurative che coprono il rischio associato a un determinato asset

Valutazione dei rischio

- Il costo dell'analisi deve essere congruente con i beni da proteggere. Il livello di granularità dell'analisi è una scelta di chi effettua la valutazione.
- Se la valutazione del rischio viene effettuata secondo una logica minaccia/asset senza tenere in giusta considerazione la relazione fra gli asset potrebbe esserci una non corretta valutazione del rischio e del rapporto costo beneficio di una particolare contromisura.
- Una contromisura che potrebbe apparire non conveniente se rapportata ad una singola minaccia/asset potrebbe risultare conveniente se ripartita su più asset fra loro correlati, ovvero se tutela anche rispetto ad altre minacce.
- Ad esempio un impianto antincendio che tuteli un edificio, automaticamente tutela anche i beni in esso contenuti. Considerare queste relazioni, anche se molto difficile, è particolarmente importante.

VALUTAZIONE DI IMPATTO
(DPIA - *DATA PROTECTION IMPACT ASSESSMENT*) (Art. 35)

È una ***analisi preventiva*** volta a valutare il contesto di trattamento e i relativi **rischi**

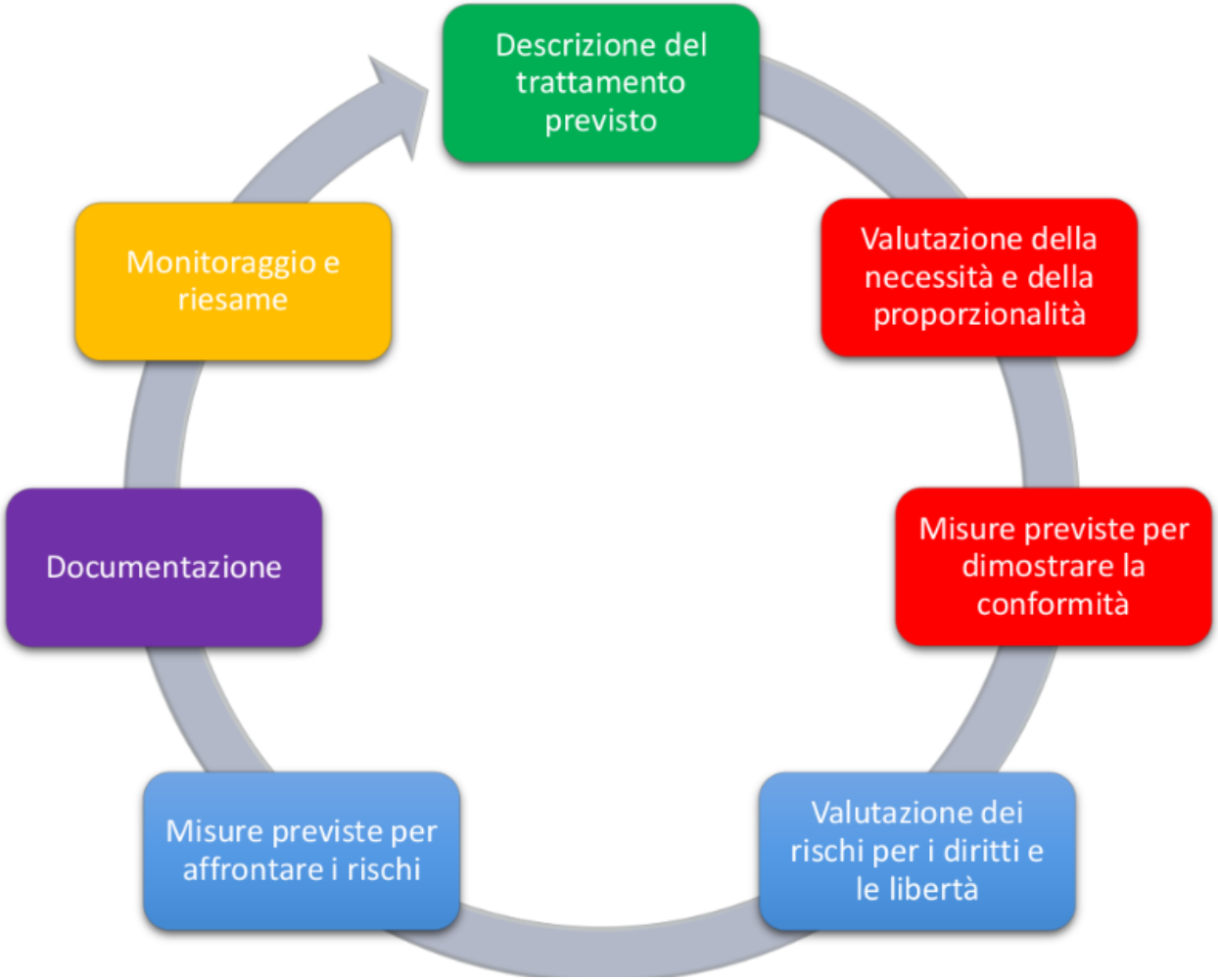
- in house oppure affidata all'esterno (outsourcing)
- il titolare dovrebbe consultarsi con responsabili del trattamento, D.P.O. e, ove possibile, con i soggetti interessati o i loro rappresentanti

Obbligatoria quanto il trattamento presenta ***rischi elevati***, come:

- trattamento di dati relativi a interessati vulnerabili (es: minori, lavoratori dipendenti)
- trattamento che fa uso innovativo o applica ***nuove soluzioni tecnologiche od organizzative*** (es: riconoscimento biometrico basato sull'impronta digitale)
- valutazione sistematica e globale di aspetti personali relativi a persone fisiche basata su ***trattamenti automatizzati o profilazione***
- trattamento su ***larga scala*** di dati sensibili
- trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la ***sorveglianza sistematica di un'area accessibile al pubblico***

Misura CONSIGLIATA anche nei casi facoltativi (Linee Guida su DPIA WP29, 4 Ottobre 2017)

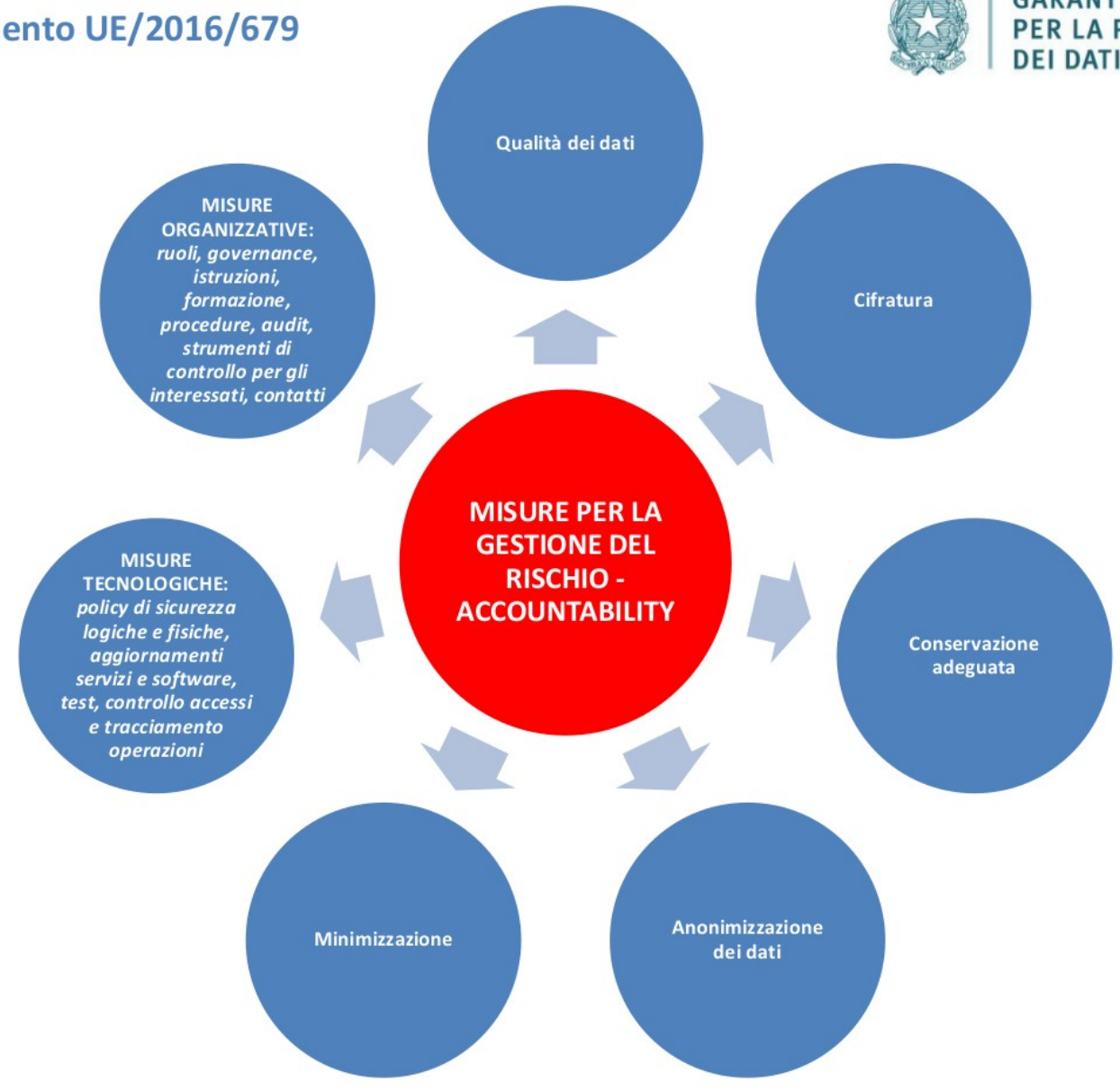
DPIA: un processo che accompagna l'intero CICLO DI VITA del trattamento dei dati




Effetti complessivi del trattamento
Danno per la reputazione
Discriminazione
Furto d'identità
Perdite finanziare
Danni fisici o psicologici
Perdita di controllo dei dati
Altri svantaggi economici o sociali
Impossibilità di esercitare diritti, servizi o opportunità

Regolamento UE/2016/679

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



Esempi di trattamento	Possibili criteri pertinenti	È Richiesta
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 di dati 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.	
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.	
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 estremamente personale.	

Esempi di trattamento	Possibili criteri pertinenti	È Richiesta
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 - Dati sensibili o dati aventi carattere estremamente personale.	**SI**
Conservazione per finalità di archiviazione di dati sensibili personali pseudonimizzati 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.	
Un trattamento di "dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato" (considerando 91).	- Dati sensibili o dati aventi carattere estremamente Personale - Dati riguardanti soggetti interessati vulnerabili.	**NO**
Una rivista online che utilizza una lista di distribuzione per inviare una selezione quotidiana generica ai suoi abbonati.	- Trattamento di dati su larga scala.	
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.	

Gestione delle VIOLAZIONI - *Data Breach Notification* (Art. 33)

È uno degli obblighi di sicurezza e come la DPIA si basa sulla valutazione del rischio a partire dal registro dei trattamenti (Art. 30)

STEP PRATICI che è consigliabile adottare in tutti in casi:

- Le informazioni relative a tutti gli eventi relativi alla sicurezza devono essere indirizzate a uno o più soggetti interni con il compito di affrontare gli incidenti, stabilendo l'esistenza di una violazione e valutandone l'eventuale il rischio.

- Deve quindi essere valutato il rischio per gli individui a seguito di una violazione (probabilità di non rischio, rischio o alto rischio), con le pertinenti funzioni dell'organizzazione che vengono informate.

- Se necessario notificare il data breach all'Autorità Garante e all'interessato (artt. 33 e 34) e ad eventuali altre istituzioni

- Cooperare con l'autorità di controllo (art. 31)

- Agire per contenere e porre rimedio alla violazione.

DATA BREACH:
VIOLAZIONE
ACCIDENTALE
O ILLECITA

Distruzione

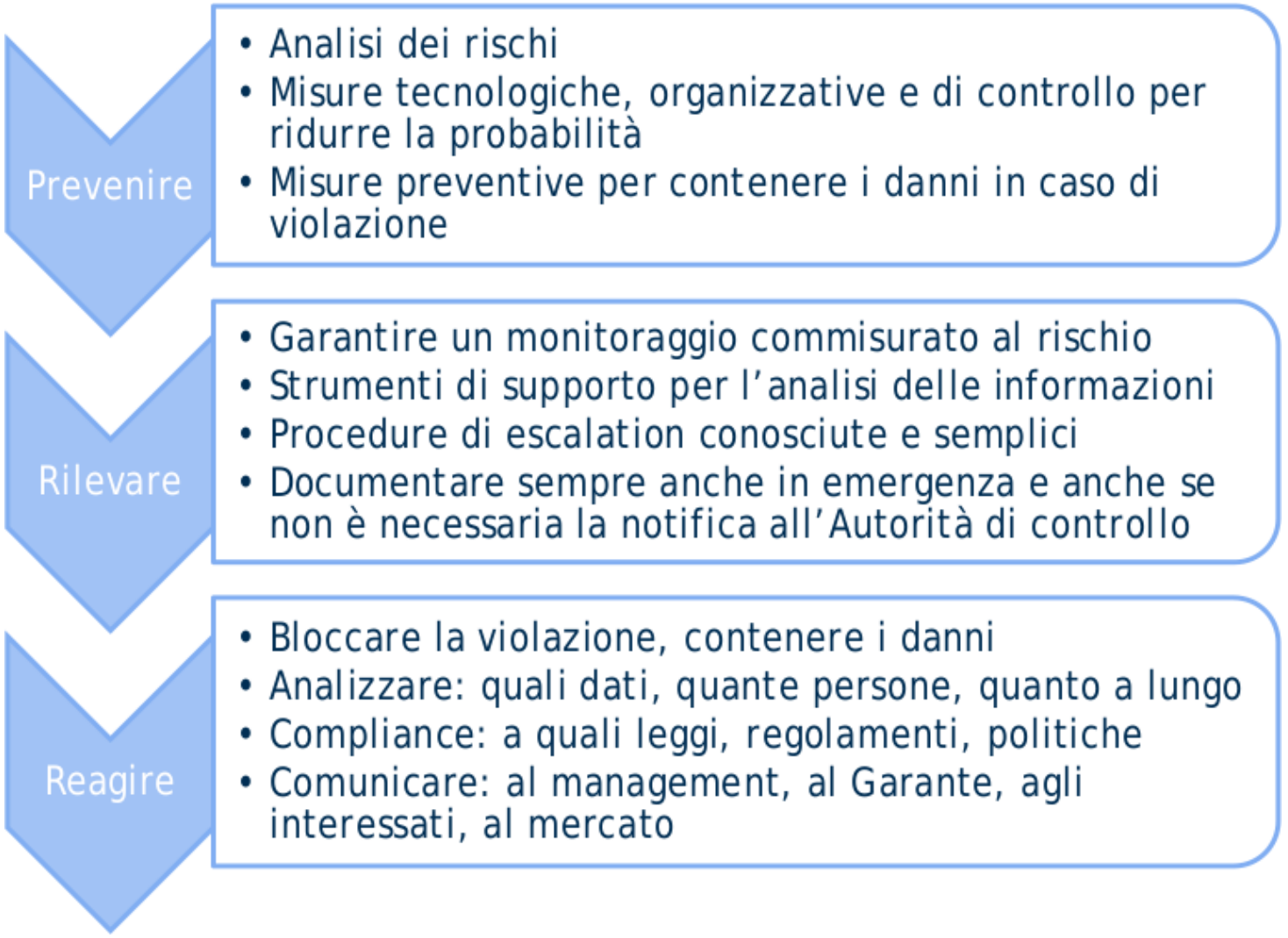
perdita

modifica,

divulgazione non autorizzata o l'accesso ai dati personali trasmessi,conservati o comunque trattati

(Art. 4 par 12)

Misure adeguate a ***prevenire***, ***rilevare*** e ***affrontare*** una violazione entro **72 ORE**



Esempio	Notifica all'Autorità di controllo?	Comunicazione agli interessati?	Note - raccomandazioni
Un Titolare fa una copia di back-up crittografata su CD di un archivio di dati personali. Il CD viene rubato.	No	No	La notifica non è necessaria se l'algoritmo crittografico è molto forte, la chiave crittografica non è stata rubata ed esiste un back-up dei dati. Se in un secondo momento i dati potrebbero essere decifrati la notifica dovrà essere fatta.
I dati personali di alcuni interessati sono sottratti dal sito web del Titolare durante un cyber-attacco. Il Titolare ha clienti solo in uno Stato Membro	Si, se ci sono potenziali conseguenze per gli interessati	Si, in base alla natura dei dati personali sottratti e all'alto rischio delle conseguenze potenziali sugli interessati	È necessario compiere un'attenta valutazione e analisi dei rischi.
Una breve interruzione di corrente di alcuni minuti presso il call center di un Titolare non permette ai clienti di contattarlo per accedere ai loro dati.	No	No	Non è una violazione da notificare, ma è comunque un evento da documentare nel registro dei data breach.

Esempio	Notifica all'Autorità di controllo?	Comunicazione agli interessati?	Note - raccomandazioni
Un Titolare subisce un attacco ransomware che provoca la crittografia di tutti i dati. Non sono disponibili back-up e i dati non possono essere ripristinati. Durante le indagini, diventa chiaro che l'unica funzionalità del ransomware consisteva nel crittografare i dati e che non esistevano altri malware presenti nel sistema.	Sì, se ci sono potenziali conseguenze per gli interessati in quanto si tratta di una perdita di disponibilità.	Sì, in base alla natura dei dati personali crittografati e all'eventuale effetto che la mancanza di disponibilità dei dati può avere sugli interessati	Se c'è una copia di backup e i dati sono ripristinati in breve tempo, potrebbe non essere nemmeno necessaria la notifica all'Autorità né la comunicazione agli interessati. In ogni caso l'Autorità di controllo dovrebbe investigare per valutare la conformità delle misure di sicurezza ai requisiti previsti dall'art. 32
Le cartelle cliniche di un ospedale non sono disponibili per un periodo di 30 ore a causa di un attacco informatico.	Sì, l'ospedale è obbligato a notificare in quanto lo stato di salute e la privacy del paziente sono da considerarsi "ad alto rischio".	Si, ai pazienti coinvolti	

Il ruolo del Business

- Conosce il valore dei processi e le possibili conseguenze in caso di problemi (non necessariamente la causa tecnica degli stessi)
- Gestisce quotidianamente i (ed è “titolare” dei) rischi di impresa
- E’ più sensibilizzabile di quanto solitamente creda l’IT

Opportunità

- Creazione di **cultura e sensibilizzazione** rispetto al **GDPR** e alle **policy di sicurezza**
- **Indirizzamento di altre compliance** a livello settoriale o trasversale, sfruttando le sinergie in fase di mappatura (es. 231, PCI-DSS, ISO 27001)
- **Analisi approfondita su specifiche aree** / **processi aziendali** (es. ripensamento modello gestione acquisti)
- **Strutturazione di knowledge base aziendale**:

  mappa dei processi aggiornata/creata

  mappa applicativi aggiornata/creata

  funzionigramma aggiornato/creato

  (...)

Ogni singola organizzazione dovrà occuparsi di analisi, revisione, aggiornamento dei singoli documenti e contratti

Rivedere **tutte le documentazioni interne relative a dati clienti, utenti, immagini webcam)**

Rivedere **i contratti di fornitura (cloud, marketing)**

Verificare il ricorso, da parte del responsabile, a **codici di condotta o meccanismi di certificazione** può certamente costituire u**n *indice di garanzia ed affidabilità***

Esempio: **outsourcing tradizionale**, catene di subfornitura più limitate e si può anche intervenire in caso di modifiche

Esempio: **cloud provider**
- catene di contratti di subfornitura anche molto lunghe e dislocate geograficamente
- caratteristiche di multiutenza

Difficilmente il titolare che dà I dati in outsourcing potrà richiedere o opporsi a modifiche all'impianto della catena di subfornitura, molto probabilmente nei contratti di servizio cloud computing si accorderà un diritto di recesso nel caso il titolare obietti sulla catena di sub fornitura

Come viene recepito il GDPR dalle organizzazioni aziendali?

CONTRO	PRO
I cambiamenti sono faticosi	Oggi è il business stesso ad imporre cambiamenti sempre più veloci. Per potersi adattare e vincere le sfide in tempo occorrono impostazioni organizzative più agili
GDPR un ostacolo al business	Business tradizionale ormai soppiantato da un business più sostenibile. Vogliamo aumentare e migliorare il nostro business anche attraverso la regolamentazione
Costi di adeguamento	Costo a breve termine BENEFICIO A LUNGO TERMINE

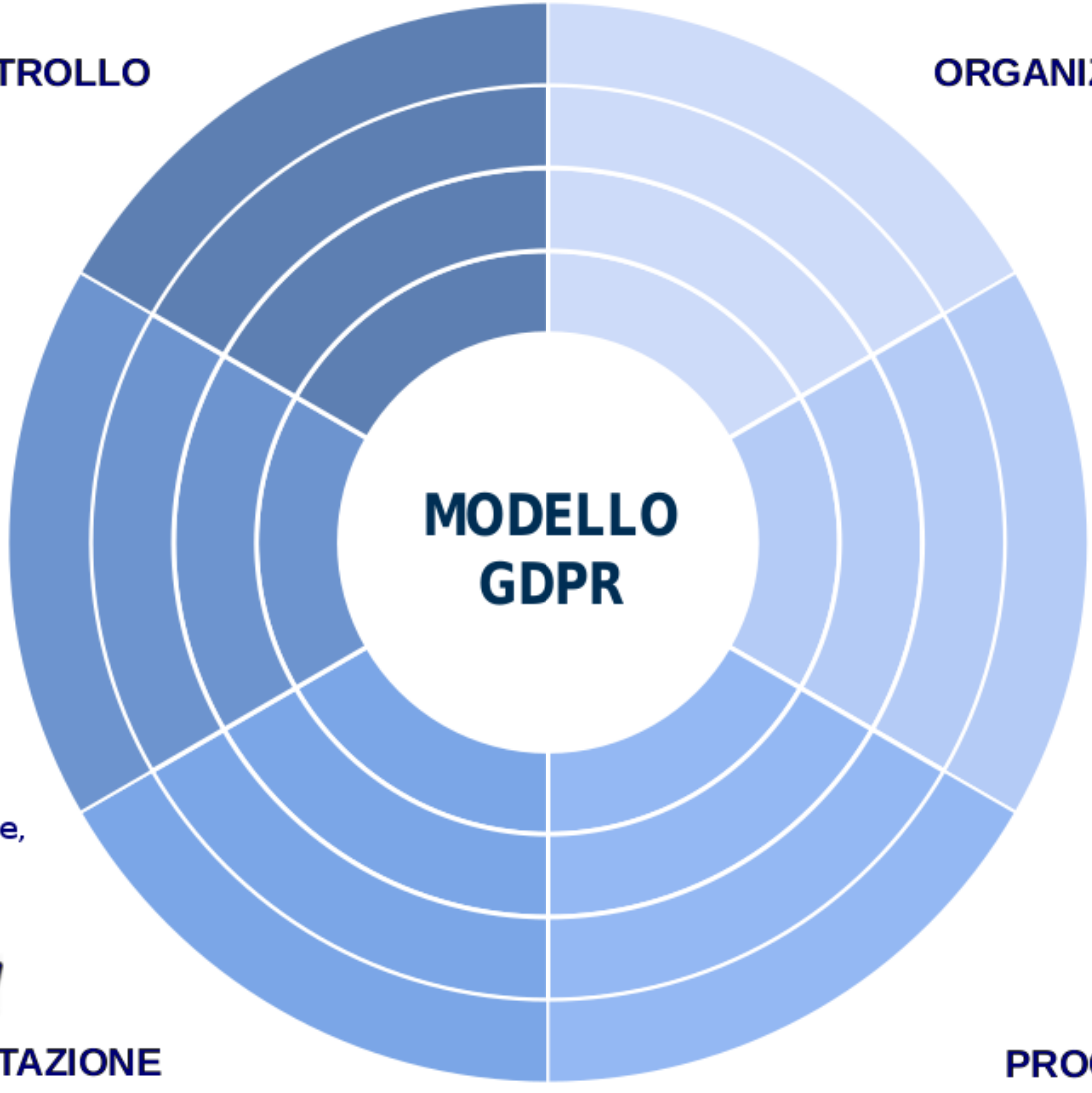
NOTA: I punti di raccolta delle informazioni sono tanti

è necessario collegare tali secondo criteri ben definiti e proceduralizzati

OCCORRE UN MODELLO ORGANIZZATIVO

Possibile Percorso di adeguamento

1. Identificazione, comprensione, classificazione dei **requisiti normativi**
2. Ingaggio di tutti gli **attori** che devono svolgere un ruolo «attivo»
3. Analisi del ***modello di funzionamento*** della data protection
4. M**appatura** preliminare dei trattamenti e identificazione trattamenti *critici*
5. Identificazione e classificazione dei **gap** da colmare
6. Definizione del ***piano di adeguamento complessivo****, inclusi* ***revisione*** *e* ***mantenimento***



SISTEMA DI CONTROLLO

Procedure,
internal audit,
disciplinari

ORGANIZZAZIONE E RUOLI

Titolare (Data Controller),
altri titolari,
Responsabile (Data Processor),
Sub-responsabile (Sub-processor),
DPO, Interessati, ...

TECNOLOGIA E STRUMENTI

Pseud, cifratura,
firewall, antivirus,
controllo accessi rete,
backup

PERSONE, CULTURA E COMPETENZE

Sensibilizzazione,
informazione,
formazione

DOCUMENTAZIONE

Organizzativa,
tecnologica,
legale

PROCESSI E REGOLE

Programma,
policies,
gestione misure,
monitoraggio

POLITECNICO MILANO 1863
SCHOOL OF MANAGEMENT

OSSERVATORI.NET
digital innovation

Fonti utilizzate

Testo di legge

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679

Sito del Garante

http://www.garanteprivacy.it/regolamentoue

http://garanteprivacy.it/documents/10160/0/Regolamento+UE+2016+679.+Con+riferimenti+ai+considerando

http://www.garanteprivacy.it/DPIA

Percorso di adeguamento Osservatori MIP

https://www.osservatori.net/it_it/percorsi/gdpr-cosa-occorre-fare-per-arrivare-in-regola-il-25-maggio-2018