Deloitte.

ASSOCIAZIONE ITALIANA
SISTEMI INFORMATIVI IN SANITÀ

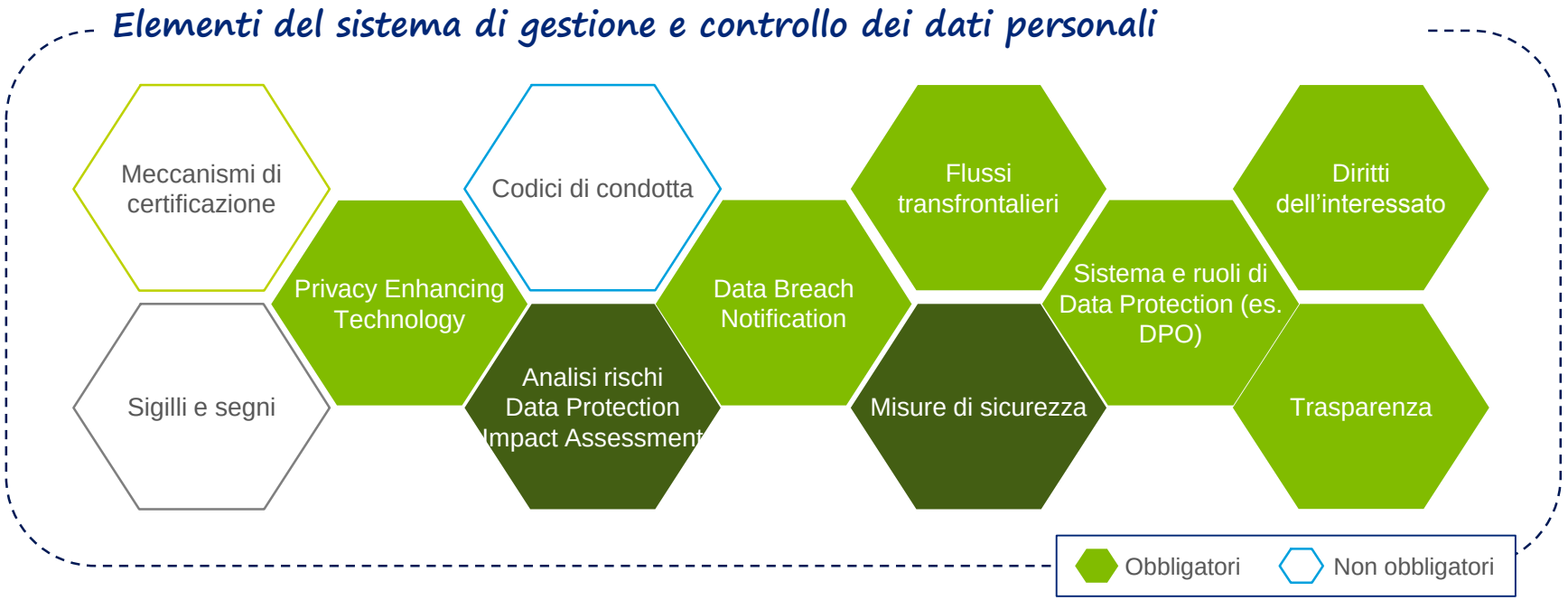
Regolamento in materia di protezione dei dati personali n. 679 del 2016

Analisi dei rischi e valutazione di impatto

Tommaso Stranieri, 13 Ottobre 2017

Il nuovo regolamento UE in materia di data protection
Principio di accountability e sistema di protezione dei dati personali

Il Regolamento stabilisce una responsabilità globale del Titolare, denominata **accountability**. Le nuove disposizioni «dettagliano **l'obbligo di responsabilità del Titolare di rispettare il presente regolamento e di dimostrare tale conformità**, anche mediante l'adozione di politiche interne e meccanismi per garantire tale rispetto»



L'accountability e il sistema di gestione e controllo dei dati personali sono elementi strettamente correlati

Dalla valutazione dei rischi alle misure di sicurezza adeguate
Gli strumenti del mestiere

La valutazione dei rischi e degli impatti, e l'individuazione delle misure di sicurezza adeguate richiedono l'adozione costante di «due strumenti del mestiere»:

- Un **«microscopio»** per valutare rischi e gli impatti
- Un **«bilancino»** per identificare le misure adeguate di protezione

Il nuovo regolamento UE in materia di data protection
Valutazione dei rischi e degli impatti

Le misure di cifratura e pseudonimizzazione dei dati devono essere considerati nell'ambito dell'**analisi dei rischi** e della **valutazione degli impatti** dei trattamenti di dati personali

- Per ogni trattamento di dati personali deve essere effettuata una **valutazione preliminare di rischio** al fine di individuare il rischio potenziale del trattamento
- Per i **trattamenti ai rischio non elevato** deve essere effettuata una valutazione di adeguatezza delle misure tecnico organizzative rispetto ai rischi che insistono sul trattamento
- Per i **trattamenti ai rischio elevato** deve essere effettuata una valutazione di impatto dei rischi che insistono sul trattamento
- Per i trattamenti che - al termine della valutazione di impatto e della implementazione delle ulteriori misure tecnico organizzative – presentano **un rischio residuo non basso**, deve essere effettuata una consultazione preventiva all'Autorità Garante

Dalla valutazione dei rischi alle misure di sicurezza adegua
La valutazione di adeguatezza

Per ogni trattamento di dati personali il Titolare deve effettuare una **valutazione di adeguatezza** dei presidi e delle misure in essere relativamente a:

SICUREZZA
Per il livello di sicurezza da garantire *(art. 32)*

MISURE TECNICO-ORGANIZZATIVE
Per la scelta delle misure da attuare *(artt. 6 e 24)*

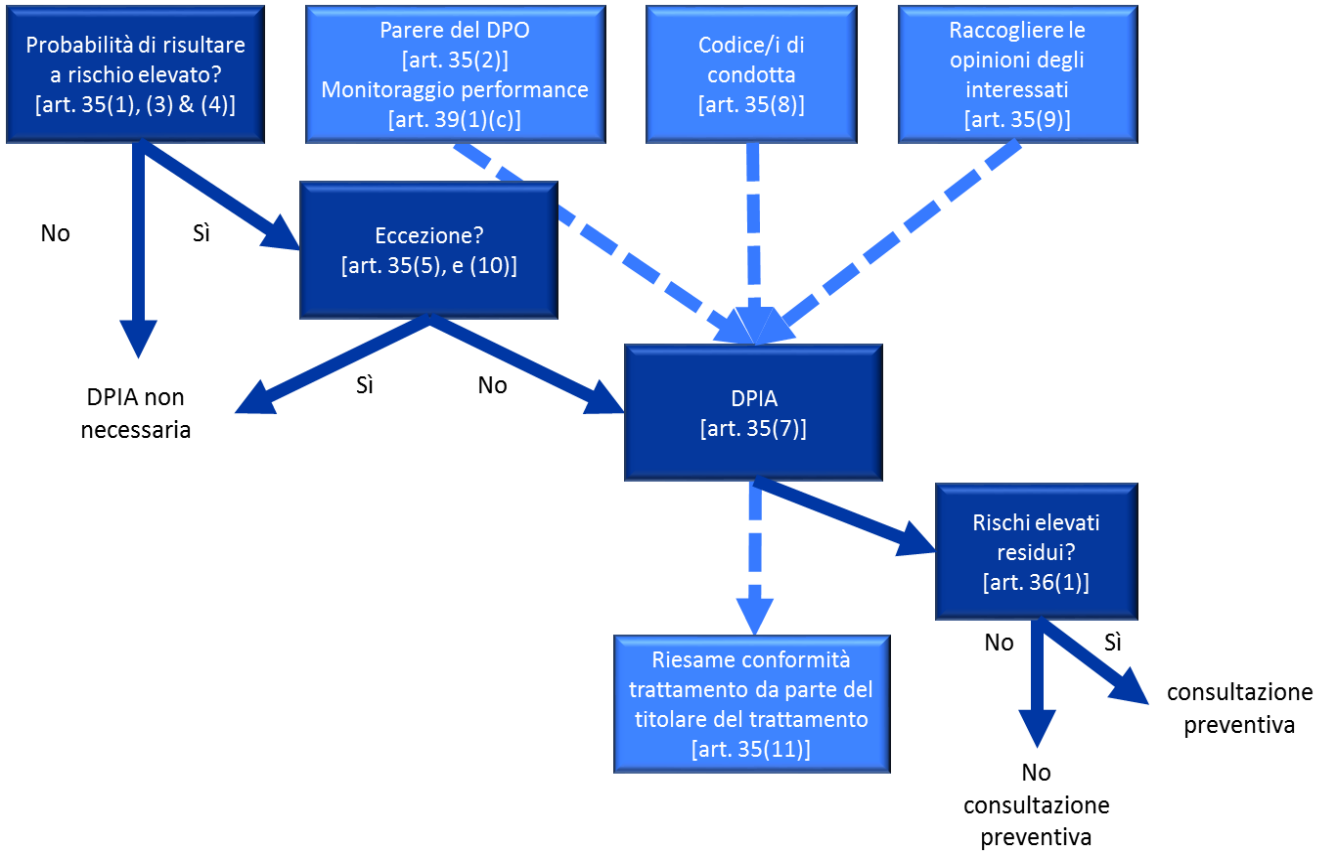
TRASPARENZA
Per corretta informazione all'interessato e facilitare esercizio diritti *(artt. 12, 14 e 28)*

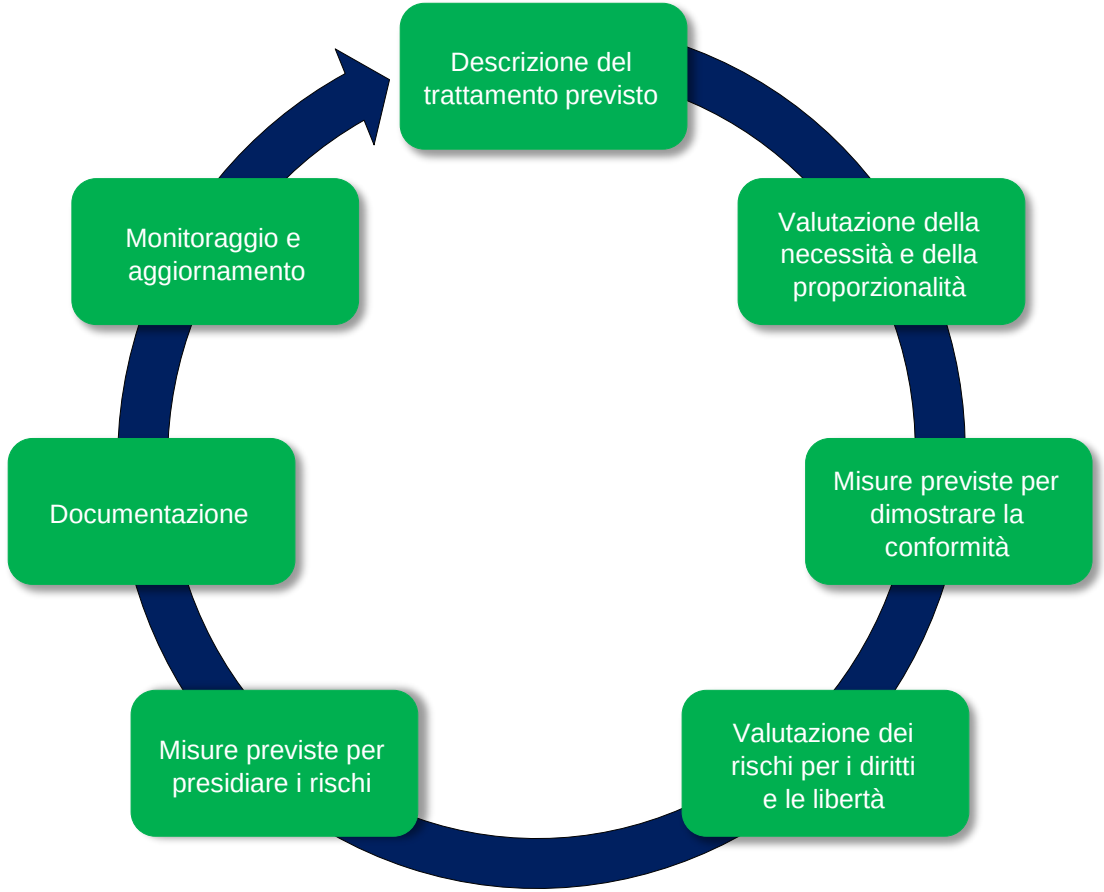
RESPONSABILI
Per la scelta appropriata dei responsabili *(art. 28).*

BY DESIGN & BY DEFAULT
Per conformità a prescrizioni in fase di progettazione e per protezione dati come impostazione predefinita *(art. 25).*

Dalla valutazione dei rischi alle misure di sicurezza adeguate
DPIA in action (wp 248)

Le Linee Guida del Gruppo ex. art. 29 forniscono delle indicazioni operative su come realizzare una DPIA





Dalla valutazione dei rischi alle misure di sicurezza adeguate
Alcune indicazioni sui trattamenti che richiedono la DPIA (wp 248)

Il Gruppo ex art. 29 ha emanato il 4 aprile delle Linee Guida che forniscono indicazioni e criteri di di maggiore dettaglio sui trattamenti che richiedono una valutazione di impatto

ref	Ambito	esempio
1	Valutazione o scoring	Credit scoring, test genetici, profilazione online
2	Decisioni automatizzate	Profilazione dei clienti
3	Monitoraggio sistematico	Videosorveglianza nei luoghi di lavoro
4	Trattamento di dati sensibili	Cartelle sanitarie, comunicazioni elettroniche, geolocalizzazione, transazioni con carta di credito, servizi cloud
5	Trattamenti a larga scala	Big Data
6	Combinazioni di banche dati	Dati provenienti da diversi titolari con diverse finalità
7	Dati inerenti soggetti vulnerabili	Minori, alcuni trattamenti HR
8	Tecnologie innovative	Biometria, riconoscimento facciale, IoT
9	Flussi di dati trans bordalieri	Flussi di dati extra EU
10	Trattamenti che limitano l'interessato nell'esercizio di un diritto o nel accedere a un servizio	Videosorveglianza, credit scoring

Dalla valutazione dei rischi alle misure di sicurezza adeguate
La valutazione degli impatti, esemplificazione

Ogni minaccia deve essere valutata secondo le dimensioni della **probabilità** e della **gravità**, per ogni potenziale danno materiali o immateriale. Di seguito una tabella esemplificativa di valutazione degli impatti.

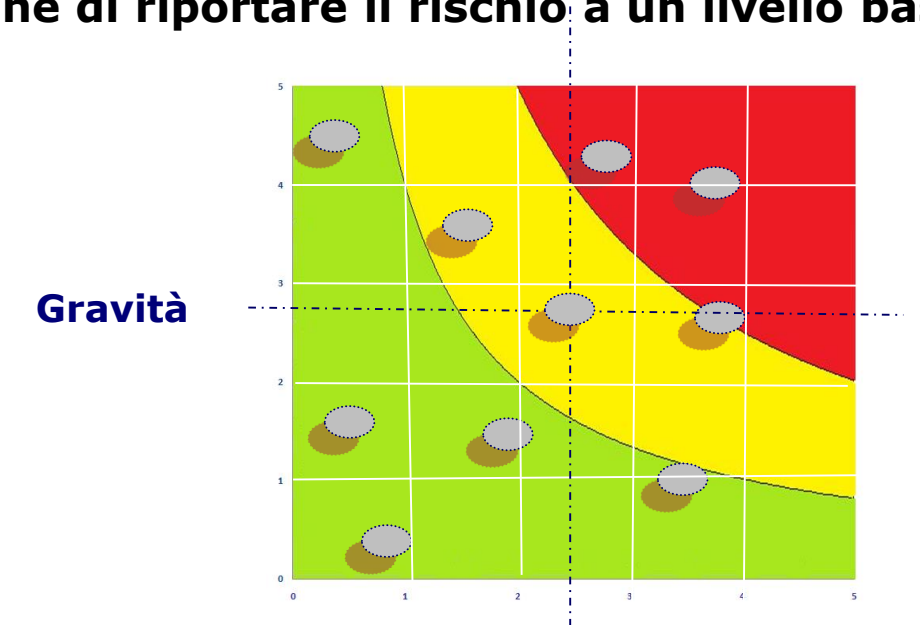
MINACCE / DANNI	Uso improprio					Violazione di dati (data breach)					
	Dati eccessivi e non proporzoinati	Trattamento non conforme con le finalità	Dati inesatti, incompleti o obsoleti	Utilizzi inattesi	Deduzioni o decisioni ingiustificate	Dati dispersi o rubati	Accessi non autorizzati	Trasferimenti non autorizzati	Divulgazione non autorizzata	Distruzione dei dati	De-anonimizzazione
MATERIALI											
Danni fisici	-	-	-	-	-	-	-	-	-		-
Danno emergente (frode, risoluzione contratto)											
Mancato guadagno (perdita opportunità)											
IMMATERIALI											
Discriminazione o stigmatizzazione											
Danni a identità (furto, omonimia)											
Reputazionali											
Ansia/paura											

Dalla valutazione dei rischi alle misure di sicurezza adeguate
La valutazione della probabilità e della gravità

La **valutazione delle probabilità** può essere fatta (a) su base **frequentista**, ovvero sulla base della frequenza con cui un determinato evento si è presentato in un periodo di riferimento, (b) oppure su base **soggettivista**, ovvero esprimendo un certo grado di fiducia che un determinato evento si realizzi

La **valutazione della gravità** è finalizzata a **quantificare la "*magnitudo*" delle conseguenze dell'evento indesiderato**, ovverosia del danno, materiale e immateriale, derivante dalla minaccia rappresentata.

La combinazione di probabilità e gravità consente di **stimare il rischio che una determinata minaccia generi un danno agli interessati del trattamento**. Il Titolare del trattamento deve **individuare adeguate misure di sicurezza al fine di riportare il rischio a un livello basso o accettabile**.



Dalla valutazione dei rischi alle misure di sicurezza adeguate
Una visione di insieme

- Le misure di sicurezza sono il risultato di un'analisi dei rischi che si sviluppa a diversi livelli, come rappresentato nella figura seguente.