



Regolamento UE sulla protezione dei dati personali

Gli impatti per le aziende

Ambito di applicazione

Ambito Territoriale



Secondo l'articolo 3.2, le disposizioni del Regolamento riguardante il trattamento dei dati personali si applicano nel caso di:

- **Trattamento effettuato nel contesto delle attività di uno stabilimento nella UE** (art. 3.1)
- **Promozione o fornitura di beni e servizi ad individui che si trovano nell'Unione Europea** (art. 3.2(a))
- **Monitoraggio del comportamento nella UE di questi individui** (art. 3.2(b)).



Legge applicabile



- La **determinazione della legge applicabile** non è più solo decisa dal “principio di stabilimento”
- Le aziende che dirigono i loro servizi o offrono i loro prodotti a clienti UE saranno soggette al Regolamento, **a prescindere dal principio di territorialità** (art. 3.2)



Implicazioni per le imprese

- Le disposizioni del Regolamento possono essere applicate anche ad aziende che non hanno la propria sede in uno Stato Membro UE o che non utilizzano un prestatore di servizi che lavora per loro conto in uno Stato Membro UE ma che comunque:
 - Promuovono i propri prodotti o servizi a soggetti che si trovano nell'UE, anche solo mediante l'utilizzo di siti Internet
 - Monitorano il comportamento nell'Unione Europea di tali individui
- Di conseguenza, le disposizioni del Regolamento possono essere applicate ad aziende e situazioni differenti e più numerose di quelle che attualmente ricadono e sono gestite dal codice italiano della privacy

Le prescrizioni del Regolamento Ue

Protezione dei dati fin dalla progettazione («by Design»)



Sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, quindi già in fase di progettazione, il Titolare, al fine di tutelare i diritti degli interessati ed essere conforme ai principi del GDPR, deve porre in essere «adeguate misure tecniche organizzative (ad. es. pseudonimizzazione, minimizzazione dei dati, misure di sicurezza etc.) – art. 25

Protezione dei dati per impostazione predefinita («by Default»)



Secondo questo principio, devono essere adottati meccanismi che assicurino che per impostazione predefinita:

- Siano utilizzati solo i dati necessari a uno scopo specifico
- Non siano resi accessibili i dati personali ad un numero indefinito di persone
- I dati non siano archiviati oltre il tempo necessario alla soddisfazione dello scopo



Implicazioni per le imprese

- **È necessario implementare dispositivi di sicurezza il prima possibile** poiché ad uno stadio più avanzato essi si rivelerebbero insufficienti a garantire un'effettiva protezione dei diritti dell'interessato.

Le prescrizioni del Regolamento Ue: Il Consenso



Implicazioni per le imprese

E' opportuno che i Titolari del Trattamento **verifichino la rispondenza delle formule di consenso** attualmente utilizzate a quanto richiesto dal GDPR al fine di adeguarle entro il 25 maggio 2018 soprattutto con riferimento ai seguenti punti:

- Deve essere libero, specifico, informato e inequivocabile.
- Manifestato in modo non equivoco attraverso azioni positive
- - Per i dati sensibili (art. 9) il **consenso deve essere esplicito** e lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione art. 22)

Ma ciò non vuol dire che è richiesta la forma scritta oppure deve essere sempre documentato per iscritto.

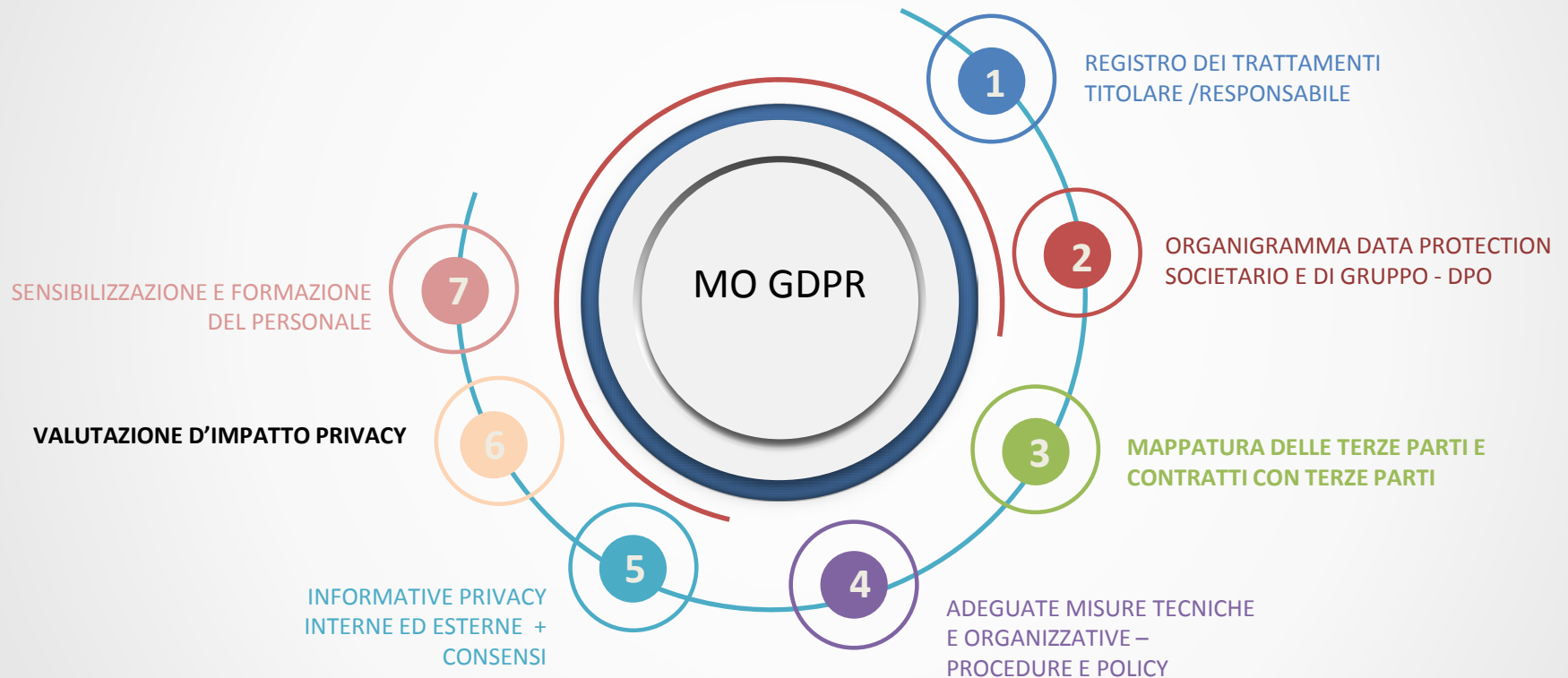
Ma quando il consenso non è liberamente espresso (considerando 43)?

- Se non è possibile esprimere un consenso separato a distinti trattamenti dei dati personali
- Se la prestazione di un servizio è subordinata ad un consenso sebbene esso non sia necessario per tale esecuzione

Non è ammesso il consenso presunto o tacito (no a caselle pre-spuntate sul modulo)

- Tutto ciò richiede uno sforzo organizzativo continuo in quanto dovranno essere **adottate misure organizzative interne** idonee a garantire che il Titolare (art. 71) sia sempre in grado di dimostrare che l'interessato ha prestato il consenso.

Modello GDPR



Il Registro dei Trattamenti

Titolare e **responsabile** devono mantenere un registro delle attività di trattamento, disponibile su richiesta del Garante (art. 30)



Valutazione d'impatto:
sussistenza di rischio elevato



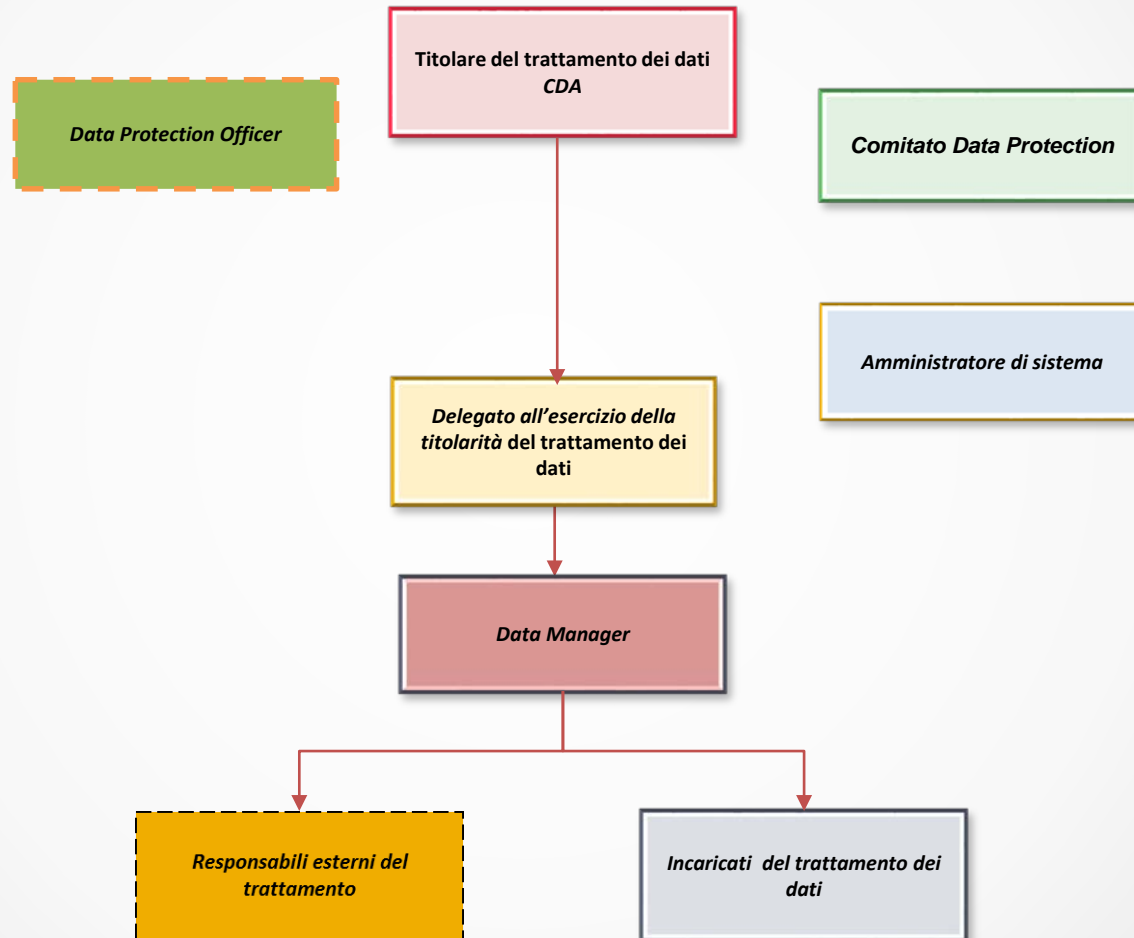
Registro dei Trattamenti punto di partenza per...

Il Registro dei Trattamenti rappresenta una parte fondamentale del Sistema di Gestione DP in quanto, se fatto bene, consente al Titolare di :

- ☐ **Definire un Organigramma DP**
- ☐ Mappatura delle Terze Parti (Contitolari e Responsabili Esterni)
- ☐ Individuare Trattamenti che potrebbero presentare rischi elevati per i diritti e libertà delle persone fisiche



Proposta di Modello Organizzativo Data Protection



Il concetto di «responsabilizzazione» o «accountability»

Le Responsabilità del Titolare del trattamento (art. 24)

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento **mette in atto misure tecniche e organizzative adeguate** per garantire, ed essere in **grado di dimostrare**, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono **riesaminate e aggiornate** qualora necessario.
2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono **l'attuazione di politiche adeguate** in materia di protezione dei dati da parte del titolare del trattamento.
3. L'adesione ai **codici di condotta** di cui all'articolo 40 o a un **meccanismo di certificazione** di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

Responsabili interni vigenti e data protection managers

1

Diversamente dal codice privacy vigente, il GDPR prevede la figura del Responsabile del trattamento solo riguardo a terze parti che effettuano operazioni di trattamento per conto del Titolare (**cd. Responsabili esterni**).

2

Sotto il profilo dei ruoli di legge, il Titolare è tenuto ad individuare le persone che hanno l'incarico di utilizzare i dati personali per lo svolgimento del proprio lavoro ed a fornire loro istruzioni formali d'uso (**cd. Incaricati**).

3

Nulla preclude, anzi è consigliabile che l'azienda Titolare, nell'ambito della propria **discrezionalità organizzativa**, preveda figure intermedie di governo della materia, per specifiche aree di competenza (**cd. Data Protection Managers**).

4

I Data Protection Managers sono soggetti incaricati del trattamento con speciali deleghe. Sostanzialmente essi sostituiscono la figura del responsabile del trattamento «interno» nota alla prassi italiana, nella vigenza del codice privacy.

Il Titolare del trattamento



Ai sensi del Regolamento UE 2016/679 in materia di protezione dei dati personali (“GDPR”) titolare del trattamento dei dati è «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, **determina le finalità e i mezzi del** trattamento di dati personali».

Il titolare del trattamento deve mettere in atto misure tecniche e organizzative **adeguate** per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR (ART.24).

Il Data Manager

Il Data Manager è individuato nel precedente responsabile interno del trattamento, ossia il capo dipartimento (es. capo marketing, capo HR, capo IT, ecc.)

Tramite nomina ottenuta dall'Azienda Titolare, anche per il tramite del Delegato, i Data Manager ricevono il potere di fornire istruzioni al personale della propria area di competenza (incaricati) sulle operazioni di trattamento da essi poste in essere.

Il Data Manager è tenuto a cooperare con gli altri Data Managers, il DPO e con tutti coloro che svolgono ruoli aziendali in materia di protezione dei dati personali ed a soddisfare le richieste avanzate da parte del Titolare, anche per il tramite del suo Delegato, per rendere effettive ed efficaci l'adozione delle misure tecniche ed organizzative predisposte dall'Azienda.

Gli Incaricati

Il GDPR conserva la figura dell'incaricato - anche senza attribuirgli uno specifico appellativo - al quale l'azienda Titolare dovrà **dare formali istruzioni** relative alle modalità di trattamento dei dati, previsione che per altro viene inquadrata come misura di sicurezza (Art. 32.4).

Tale requisito normativo, dovrebbe tradursi in **apposite modalità di incarico** ed eventuali **percorsi formativi**.

CHI SONO GLI INCARICATI

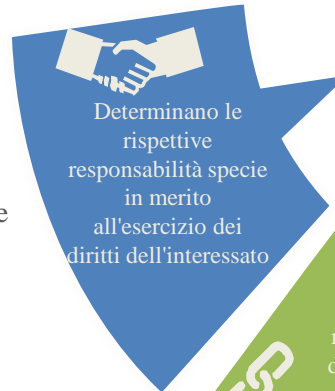
- Tutti i dipendenti dell'azienda che trattano dati personali verranno nominati incaricati con specifiche nomine
- Gli incaricati sono tutti i soggetti che accedono ai dati personali e li utilizzano secondo specifiche direttive impartite dal Titolare.

Contitolari e Responsabili

Contitolari e Responsabili del Trattamento

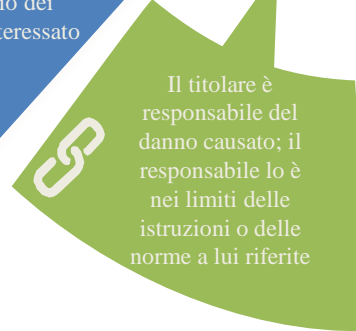


- Il Contitolare del Trattamento è l'azienda che condivide con un'altra entità **finalità e mezzi del trattamento** (art. 26)
- L'accordo è messo a disposizione dell'interessato e può designare un punto di contatto per gli interessati.
- Il Responsabile del trattamento che agisce al di là delle istruzioni ricevute dal Titolare o in assenza di queste è considerato un Titolare del Trattamento (art. 28.10)

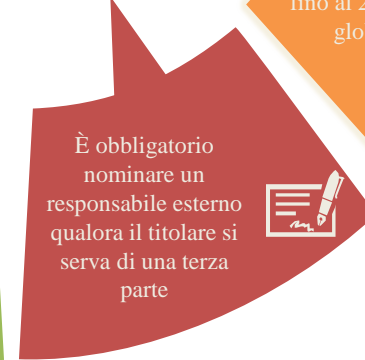


Determinano le rispettive responsabilità specie in merito all'esercizio dei diritti dell'interessato

Contitolari e Responsabili del Trattamento



Il titolare è responsabile del danno causato; il responsabile lo è nei limiti delle istruzioni o delle norme a lui riferite



È obbligatorio nominare un responsabile esterno qualora il titolare si serva di una terza parte



La non determinazione delle responsabilità è punita con sanzione fino al 2% del fatturato globale annuo



Implicazioni per le aziende



- Gli obblighi normativi relativi ai Responsabili contenuti nel regolamento (sicurezza dei dati, misure tecniche e organizzative appropriate, protezione dei dati fin dalla progettazione, valutazione d'impatto sulla protezione dei dati) hanno più peso delle obbligazioni contrattuali in essere tra le parti. Queste circostanze implicano:
 - Possibili **dispute inerenti la responsabilità** per violazioni della legge o del contratto e per danni, specialmente tra l'azienda cliente e il contractor
 - Necessità che la nomina fatta agli outsourcer sia efficace ed effettiva, cosa che richiede l'implementazione di una **attività di audit periodica**
 - Responsabilità del Titolare di scegliere un Responsabile che fornisca garanzie sufficienti per il trattamento

Obblighi del Responsabile del Trattamento dei dati (art. 28)



Sono responsabili del trattamento tutti coloro che effettuano un trattamento dati per conto del titolare.

I responsabili del trattamento dei dati devono:

- Trattare i dati soltanto su **istruzione documentata** del titolare del trattamento
- Garantire che le persone autorizzate al trattamento dei dati personali siano impegnate alla riservatezza o abbiano un obbligo legale di riservatezza.
- Adottare tutte le misure di sicurezza adeguate al rischio ai sensi dell'art. 32 (pseudonimizzazione, capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico.)
- **Assistere il Titolare** per dare seguito alle richieste per l'esercizio dei diritti dell'interessato

Obblighi del Responsabile del Trattamento dei dati (art. 28)



- **Assistere il Titolare** nel garantire il rispetto degli obblighi di cui all'art. 32 (sicurezza) e 36 (Consultazione Preventiva) e il rispetto del Regolamento
- **Consentire e contribuire alle attività di revisione** comprese le ispezioni, realizzate dal titolare o da un altro soggetto da questi incaricato.
- **Cancellare o restituire, su scelta del titolare** tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti.

La figura del Sub- Responsabile(art. 28.2)



Il RE non ricorre ad **altro responsabile** (per l'esecuzione di specifiche attività di trattamento per conto del titolare) senza **previa autorizzazione scritta**, specifica o generale, del Titolare del trattamento. Nel caso di autorizzazione scritta generale, il RE informa il TI di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili al trattamento, dando così l'opportunità al titolare di opporsi a tali modifiche.

Al sub-responsabile e/o responsabile di II livello, con contratto sono imposti gli stessi obblighi in materia DP, contenuti nel contratto tra TI e RE.

Qualora il sub-responsabile ometta di adempiere agli obblighi del trattamento **il RE iniziale conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi del sub- responsabile**

Valutazione d'impatto:
sussistenza di rischio elevato



Registro dei Trattamenti punto di partenza per...

Il Registro dei Trattamenti rappresenta una parte fondamentale del Sistema di Gestione DP in quanto, se fatto bene, consente al Titolare di :

- ☐ Definire un Organigramma DP
- ☐ Mappatura delle Terze Parti (Contitolari e Responsabili Esterni)
- ☐ Individuare Trattamenti che potrebbero presentare rischi elevati per i diritti e libertà delle persone fisiche



*Quindi è un valido strumento per il Titolare per iniziare a individuare se ci sono trattamenti per i quali è necessario **procedere con una DPIA.***



Valutazione d'impatto:
sussistenza di rischio elevato



Quando fare la Valutazione d'impatto ?



Altra novità del GDPR è la DPIA che il Titolare deve fare soltanto **quando** il trattamento «**può** presentare un rischio elevato per i diritti e le libertà delle persone fisiche» (art. 35 par. 1). Essa è particolarmente importante quando viene introdotta una nuova tecnologia di trattamento dei dati.

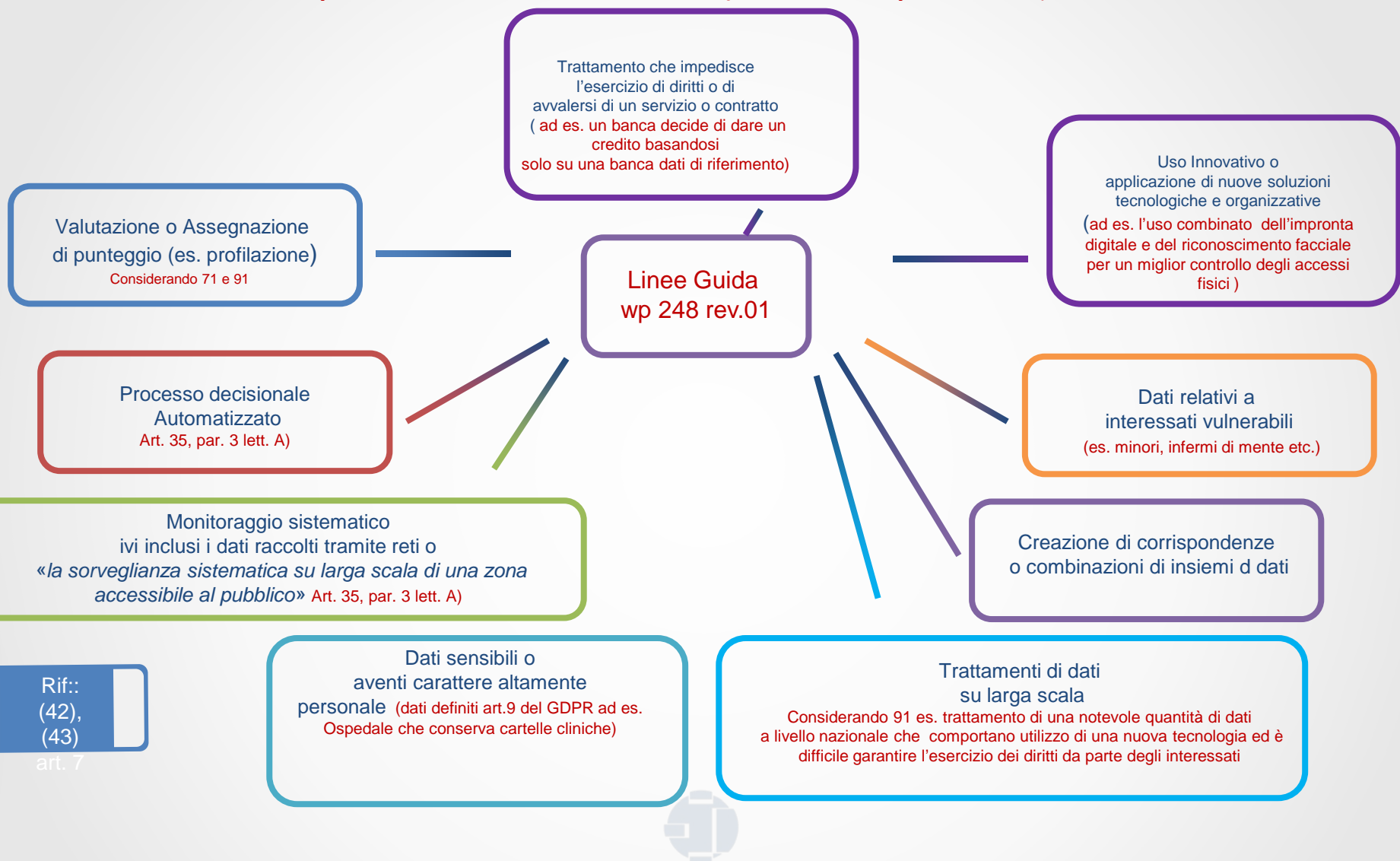


Il **Gruppo di Lavoro articolo 29** – (Organo Consultivo dell'UE per la protezione dei dati personali) ha adottato le **Linee Guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento «possa presentare un rischio elevato» ai fini del Regolamento (UE) 2016/679.**

Linee Guida WP 248 rev.01



9 Criteri per determinare il rischio elevato (Linee Guida wp 248 rev.01)



Rif.:
(42),
(43)

art. 7

Quando fare la Valutazione d'impatto ?



In generale, il WP 29 ritiene che maggiore è il numero di criteri soddisfatti dal trattamento, più è probabile che sia presente un rischio elevato per i diritti e le libertà degli interessati e, di conseguenza, che sia necessario realizzare una valutazione d'impatto sulla protezione dei dati, indipendentemente dalle misure che il titolare del trattamento ha previsto di adottare.

La decisione di non procedere con la DPIA, pur in presenza di almeno 2 dei suddetti criteri, deve essere giustificata e documentata dal Titolare.

Alcuni Esempi	Possibili Criteri Pertinenti	Richiesta DPIA?
Un ospedale che tratta i dati genetici e sanitari dei propri pazienti (Sistema informativo ospedaliero)	<ul style="list-style-type: none"><input type="checkbox"/> Dati sensibili o dati aventi carattere estremamente personale<input type="checkbox"/> Dati riguardanti soggetti interessati vulnerabili<input type="checkbox"/> Trattamento dei dati su larga scala	Si
Un'istituzione che crea una banca dati antifrode e di gestione del rating del credito a livello nazionale	<ul style="list-style-type: none"><input type="checkbox"/> Valutazione o assegnazione di un punteggio<input type="checkbox"/> Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente<input type="checkbox"/> Impedisce agli interessati di esercitare un diritto o utilizzare un servizio o un contratto<input type="checkbox"/> Dati sensibili o dati avente carattere estremamente personale	Si

Valutazione d'impatto: Consultazione preventiva



TITOLARE

- ✓ Se DPIA attesta che, in assenza di misure, meccanismi, garanzie di riduzione del rischio, **permangono rischi elevati**, ragionevolmente non mitigabili



Assistito su richiesta dal Responsabile

**Consultazione
preventiva**



GARANTE

- ✓ **Risponde entro 8+6 settimane** al Titolare o Responsabile per iscritto

Rif.:
(94)
Art. 36



Gli elementi della Valutazione d'Impatto

La valutazione deve contenere almeno:

- a) una descrizione sistematica dei trattamenti previsti (C, P o G) e delle finalità del trattamento;
- b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- c) una valutazione dei rischi per i diritti e le libertà degli interessati
- d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al regolamento
- e) le **responsabilità interne ed esterne** coinvolte nel trattamento dei dati

Misure tecnico-organizzative: Esempi e utilità



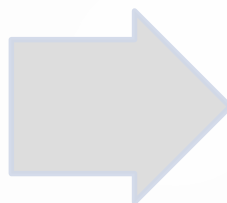
Misure Tecniche

Credenziali, Sistema
autorizzazione,
Cifratura, Antivirus, etc.



Misure Organizzative

Clausole DP, Contratti con
Responsabili,
Vincoli riservatezza, Istruzioni,
Registro



Sistema di **protezione e**
reazione alle violazioni (*data breach*)



Strumento di
verifica e dimostrazione di conformità



Strumento di
riduzione e valutazione del rischio



Modello organizzativo



Supporto e facilitazione
all'esercizio dei diritti



Responsabile della protezione dei dati (DPO)



- Il DPO deve essere prontamente coinvolto in tutte le questioni che interferiscono con la protezione dei dati personali (art. 38.1)
- Il DPO è indipendente e deve ricevere adeguato supporto in termini di risorse e accessibilità (art. 38.2)
- La nomina del DPO è obbligatoria (art. 37.1) per:
 - **Enti pubblici** eccetto le autorità giudiziarie per le funzioni giurisdizionali
 - Quando le «attività principali» «consistono in trattamenti» «che richiedono» (a) **monitoraggio di interessati** (b) regolare e sistematico (c) su larga scala
 - Quando l'attività principale consiste nel trattamento «su larga scala» di **dati sensibili e giudiziari**
- Un gruppo imprenditoriale può nominare anche un solo DPO purché «sia facilmente raggiungibile da ciascuno stabilimento» (art. 37.2)



Implicazioni per le aziende

- La nomina, la posizione nell'organizzazione e le attività del DPO richiedono l'utilizzo di valutazioni innovative per l'ambiente della protezione dei dati

D

P

O

Responsabilità e accountability dei Titolari

Per assicurare i doveri e le responsabilità previsti per il DPO, i Titolari possono:

- Fare uso dello staff esistente, con training appositi
- Utilizzare contractor esterni
- Assumere nuovo staff

Benefici nel nominare un DPO

- Fornire un collegamento tra il Titolare del trattamento, l'interessato e l'Autorità di Controllo
- Implementare un Sistema di governo dei dati personali, coordinando i doveri e le responsabilità dei diversi ruoli coinvolti nella protezione dei dati personali
- Ridurre i costi amministrativi e di compliance

Compiti e Requisiti del DPO

- Deve possedere competenze giuridiche, informatiche, di *risk management* e di analisi dei processi;
- Si relaziona direttamente con i vertici gerarchici Titolare o Responsabile;
- Deve svolgere i propri compiti in modo autonomo ed indipendente;
- Non deve essere individuato tra soggetti che per funzioni o ruoli potrebbero determinare un conflitto d'interesse.



Informare e
fornire consulenza



Sorvegliare l'applicazione del GDPR



Formazione e
sensibilizzazione



Fornire parere su DPIA
e vigilarne lo svolgimento



Cooperare col Garante Privacy
e fungere da punto di contatto

Il Data Protection Officer



Ai sensi dell'art.39 del GDPR, il DPO è tenuto a:

1. **informare e fornire consulenza** al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
2. **sorvegliare l'osservanza del regolamento**, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati **nonché delle politiche** del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi **l'attribuzione delle responsabilità**, la **sensibilizzazione** e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
3. fornire, se richiesto, **un parere in merito alla valutazione d'impatto** sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
4. cooperare con l'autorità di controllo; e
5. fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Il DPO nei Gruppi



Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento.

Importante implementare:

- Procedura Flussi Informativi al DPO
- Integrazione con altri Organi di Controllo

Flussi informativi tra DPO e altri ruoli DP



Il ruolo centrale del DPO si ravvisa anche nell'emanazione di politiche e linee guida, nonché come riferimento terminale di evidenze da parte di responsabili, incaricati, referenti e Amministratori di Sistema.

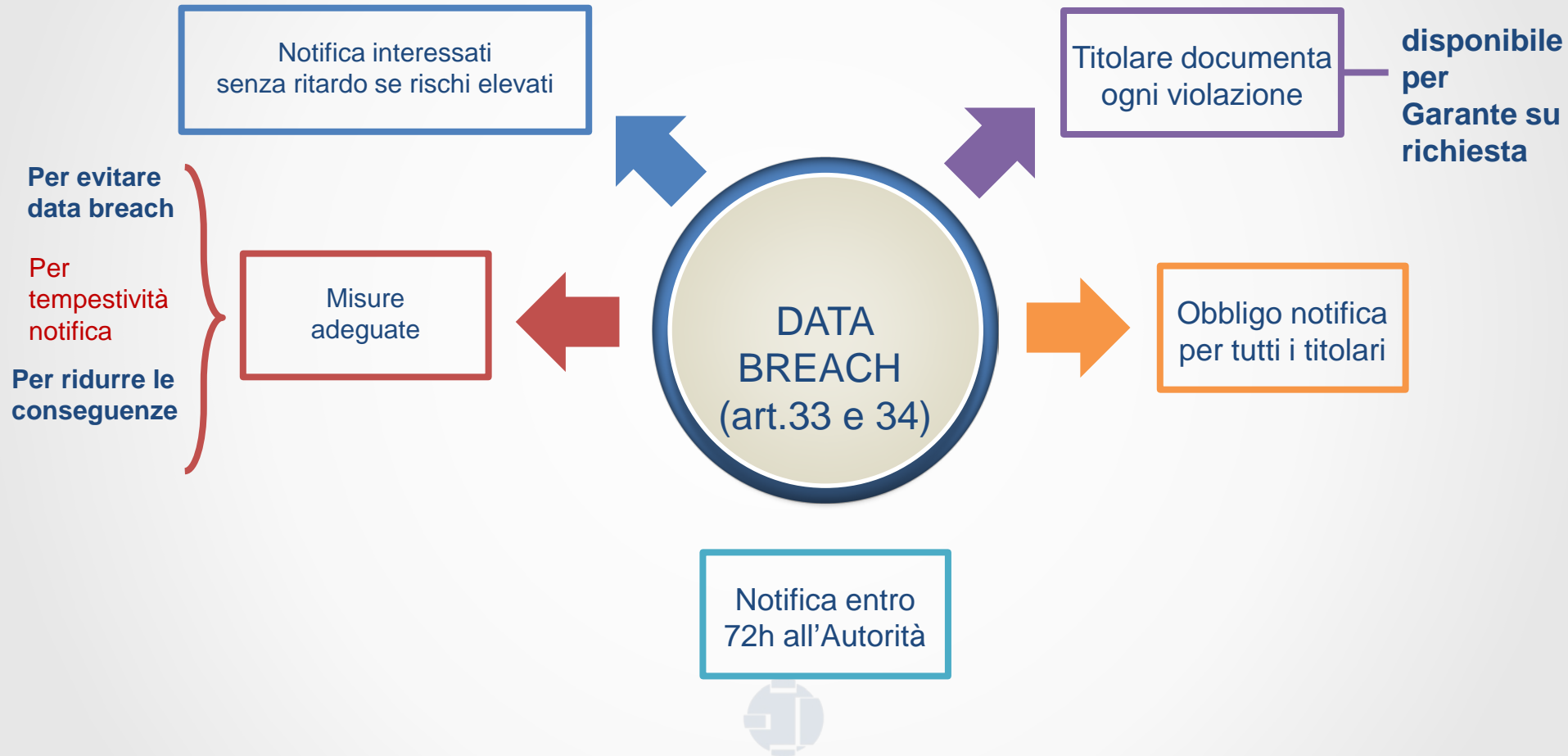
Il Comitato Data Protection

Il Comitato Data Protection contiene i capi funzione dei dipartimenti maggiormente impattati dalla normativa data protection (Legale, Commerciale/MKT, HR , Security e IT). Il ruolo del Comitato è quello della *longa manus* del Delegato.

Sarà il Comitato Data Protection, attraverso la stretta collaborazione con i Data Managers, ad accertarsi che i requisiti del GDPR siano effettivamente calati all'interno dei diversi dipartimenti aziendali. Inoltre, sarà il Comitato ad interfacciarsi con il DPO al fine di ricevere opportune linee guida e valutazioni circa la bontà dell'operato.

Il Comitato Data Protection, sotto la supervisione del Delegato, ha l'obiettivo di creare una pianificazione strategica, definire linee guida e concordare budget per gli interventi data protection, tutto ciò servendosi della supervisione e *expertise* del Data Protection Officer.

Data Breach: in sintesi



Sanzioni previste dal solo Regolamento



Organizzazione 2%

Mancata individuazione formale di ruoli e responsabilità nel trattamento dei dati personali



Sicurezza 2%

Mancata adozione di adeguate misure di sicurezza



Informativa e Consenso 4%

Non adempiere agli obblighi sul consenso



Accountability

Omessa DPIA quando richiesta, consultazione preliminare Autorità 2%

Violazione diritti interessati, regole su trasferimenti extra-UE, obblighi Stati Membri, prescrizioni dell'Autorità 4%

2%

Sanzione sino a 10 milioni di euro o, in caso di imprese, sino al 2% del fatturato globale annuo

4%

Sanzione sino a 20 milioni di euro o, in caso di imprese, sino al 4% del fatturato globale annuo





Grazie

Avv. Riccardo Imperiali



riccardo.imperiali@imperiali.com

Dott.ssa Anna Irace



anna.irace@imperiali.com

Aggiungici su



gruppoimperiali