GRUPPOIMPERIALI

Regolamento UE sulla protezione dei dati personali

Gli impatti per le aziende

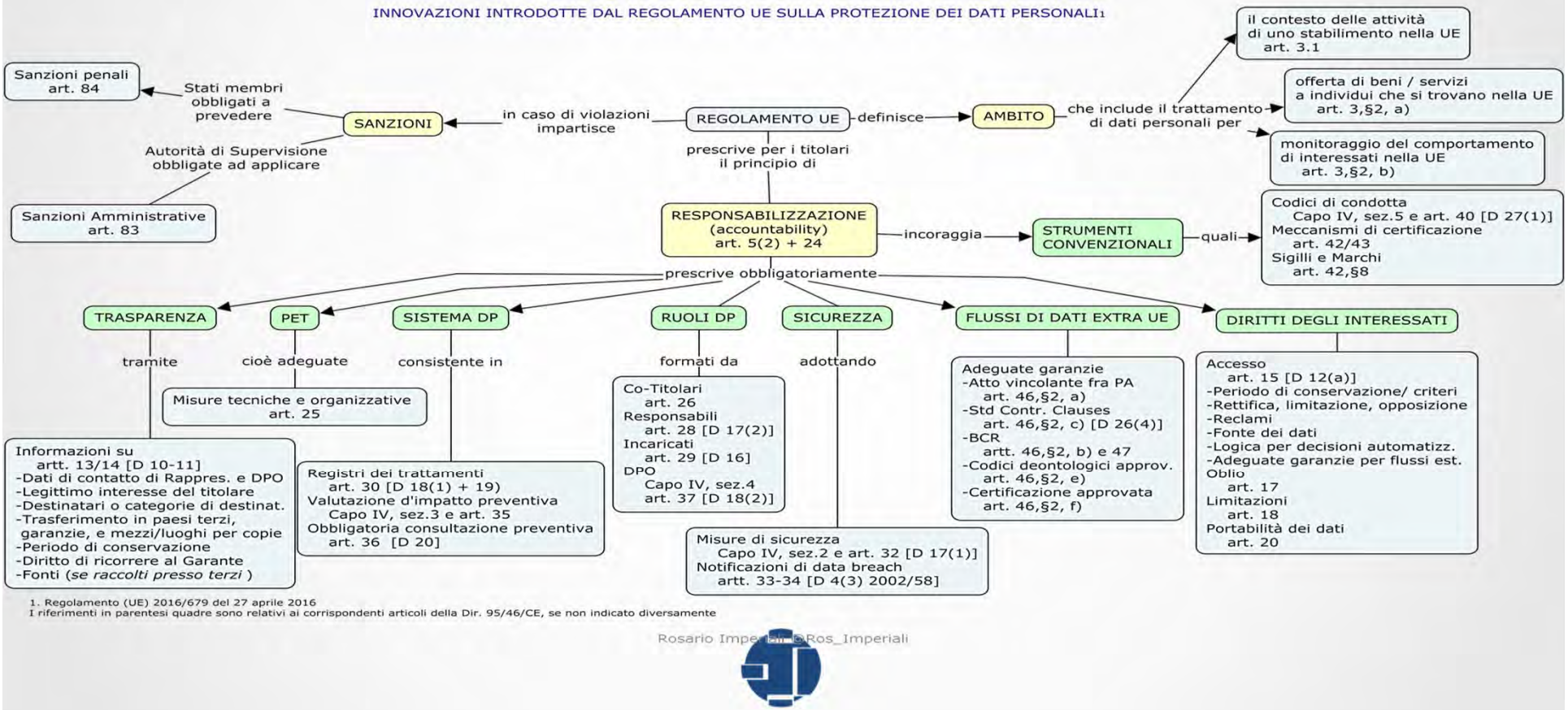
Indice dei temi – I parte

“Avv. Riccardo Imperiali di Francavilla - Partner Gruppo Imperiali

- Il nuovo Regolamento per la protezione dei dati personali (Reg. UE n. 679/2016)
- Evoluzione della Normativa
- Il Principio di Accountability
- Privacy by design e by default
- Trasparenza: Informativa e Consenso

GRUPPOIMPERIALI

Quadro sinottico Regolamento n. 2016/679



Il nuovo Regolamento Ue

- La riforma della normativa UE sulla protezione dei dati personali consiste nella promulgazione di:
  - Regolamento Europeo n. 2016/679 sulle regole generali di protezione dei dati personali
  - Direttiva n. 2016/680 sul trattamento dei dati personali per scopi giudiziari e di prevenzione criminale
- La riforma introduce significative innovazioni operative nella gestione dei dati personali da parte delle aziende private soggette alla giurisdizione degli Stati Membri dell'Unione Europea
- Il Regolamento n. 2016/679, si articola in 3 pilastri
  1. **Ambito**
  2. **Accountability**
  3. **Sanzioni**

- Ogni pilastro ha importanti implicazioni per la gestione della conformità alle prescrizioni sui dati personali, tali da dover aggiornare l'intero sistema aziendale di governo dei dati

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 <u>non</u> 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'utilizzi 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

Il concetto di «responsabilizzazione» o «accountability»

- 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»

Da FORMA a SOSTANZA mediante :

- l'attuazione del principio della protezione dei dati «by design» e «by default»
- valutazioni di impatto sulla protezione dei dati, talvolta obbligatorie

Principio di ACCOUNTABILITY → PRESCRIZIONI del Regolamento (obbligatorie/volontarie)

Profili innovativi di carattere obbligatorio

1. Trasparenza
2. Sicurezza
3. Sistema DP
4. Ruoli DP
5.. Diritti dell'interessato
6. Flussi Transfrontalieri

Focus su slide successive

Profili innovativi di carattere volontario

1. Codici di condotta
2. Meccanismi di certificazione
3. Segni e Sigilli

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: Trasparenza

Implicazioni per le imprese

- Il bisogno di stabilire delle **information policy adeguate**
- E' opportuno che i Titolari del Trattamento verifichino la rispondenza delle informative attualmente utilizzate a quanto richiesto dagli art. 12,13 e 14 del GDPR al fine di adeguarle entro il 25 maggio 2018 soprattutto con riferimento a titolo esemplificativo:

- Titolare
- Diritti degli interessati
- Finalità (Informativa Stratificata)
- Modalità di redazione (concisa, semplice e chiara)
- Tempi (al massimo entro un mese dalla raccolta e l'art. 14, par. 3 lett. A) …. cmq che il termine deve essere ragionevole)
- Dati DPO (se previsto)
- Periodo di conservazione dei dati o i criteri utilizzati per definire tale periodo
- Garanzie applicate in caso di trasferimento di dati a Paesi Terzi etc.

➢ Tutto ciò richiede uno **sforzo organizzativo continuo** in quanto dovranno essere adottate **misure organizzative interne** idonee a garantire il rispetto della tempistica. L'informativa deve essere fornita all'interessato prima di fare la raccolta e se i dati non sono raccolti presso l'interessato entro 1 mese dalla raccolta (termine max in quanto il termine deve essere «ragionevole).

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.

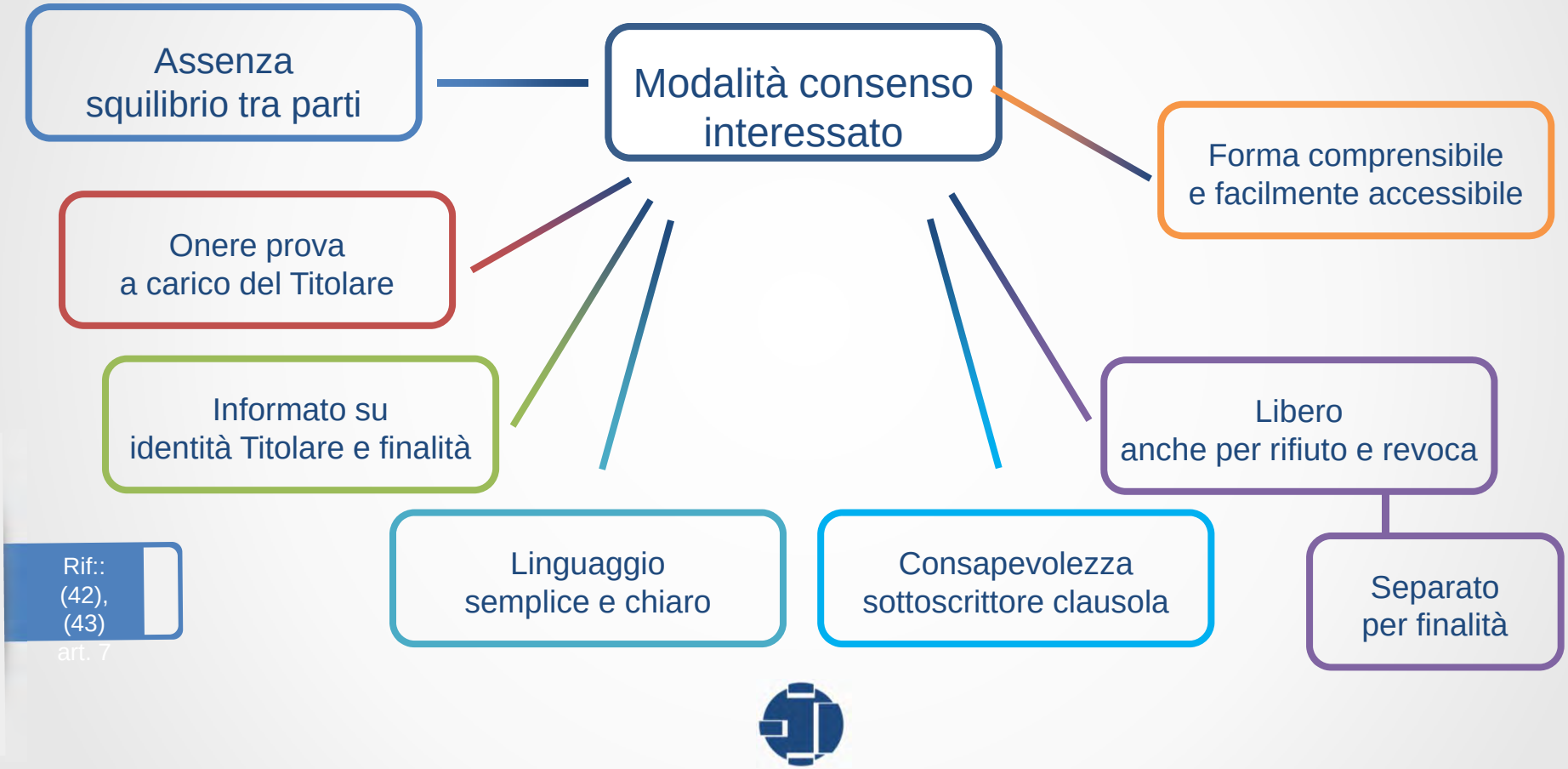
Ma quando il consenso non è liberamente espresso (considerando 43)?

- **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)

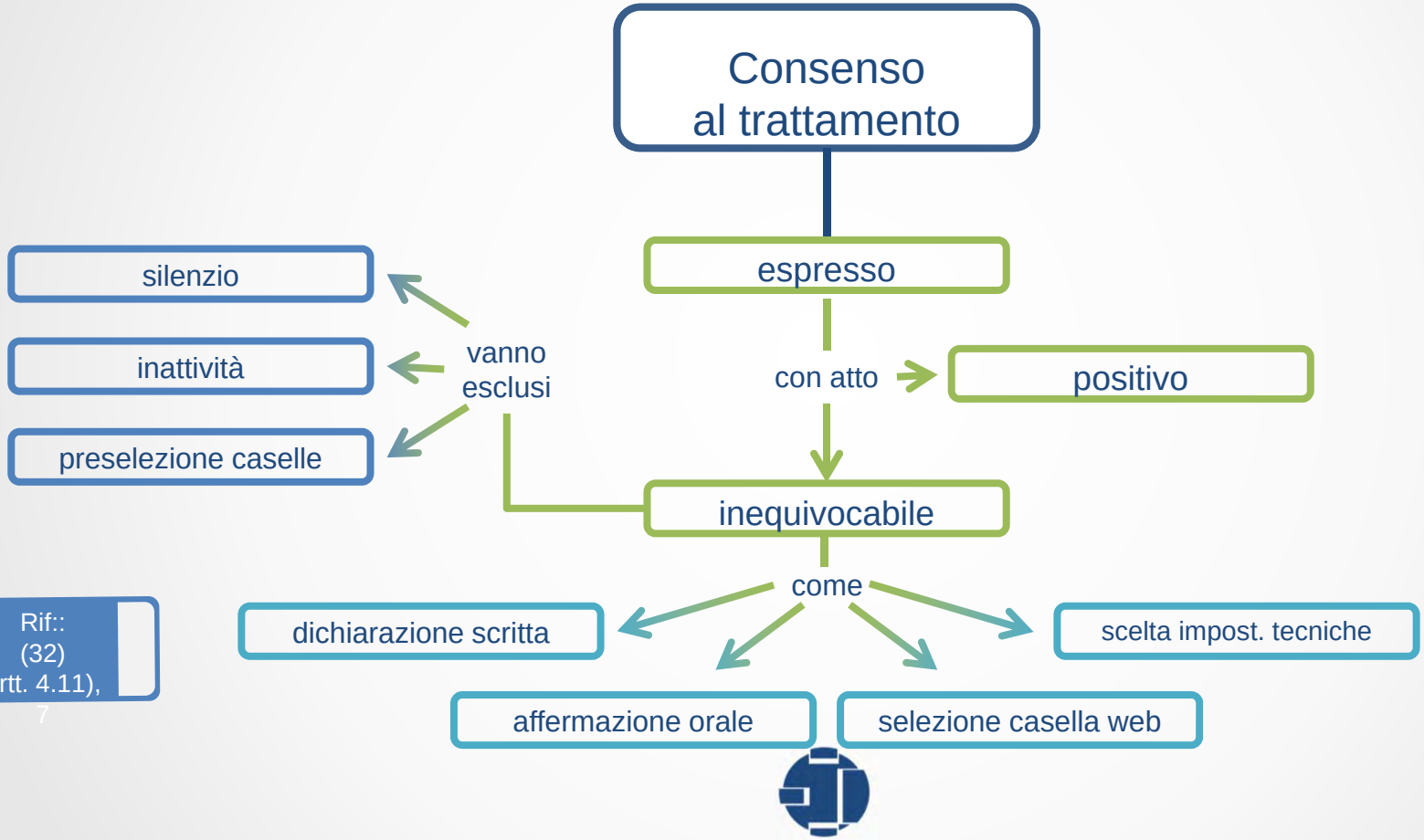
- Tutto ciò richiede uno sforzo organizzativo continuo in quanto dovranno essere **adottate misure organizzative interne** idonee a garantire che il Titolare (art. 71) sia sempre in grado di dimostrare che l'interessato ha prestato il consenso.
- .

Consenso dell'Interessato



Rif::
(42),
(43)
art. 7

Consenso - Forma



Rif::
(32)
artt. 4.11),
7

Indice dei temi

- **Dott.ssa Anna Irace - Responsabile compliance Gruppo Imperiali**
- Il Modello Organizzativo Data Protection
- Registro dei Trattamenti
- Organigramma Privacy
- Data Protection Impact Assessment – (piano di valutazione di impatto sui dati personali)
- Procedure tecnico- organizzative e di sicurezza
- Data Breach
- Il DPO – Compiti e Responsabilità
- Sanzioni

GRUPPOIMPERIALI

Il Sistema di Gestione DP

Supervisione Indipendente
- ✓ DPO - Art. 37

Documentazione di Sistema
- ✓ Registro - Art. 30

Progettualità e struttura del Sistema
- ✓ Accountability - Art. 24
- ✓ Approccio basato sul rischio
- ✓ Misure tecnico-organizzative
- ✓ Valutazioni di adeguatezza - Art. 35

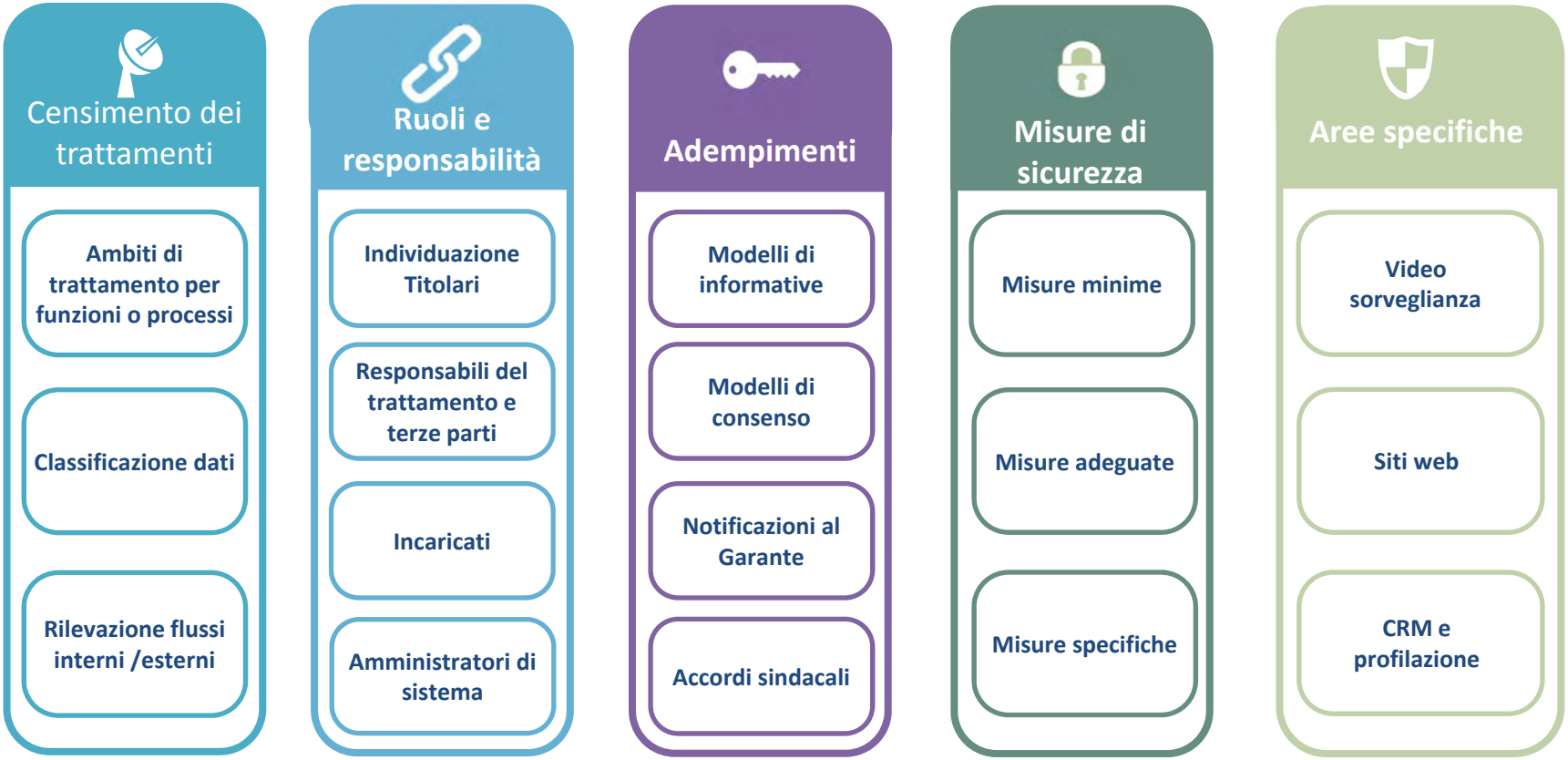
Modello organizzativo DP
- ✓ Relazioni infragruppo
- ✓ Outsourcer
- ✓ Implicazioni

Il Registro dei Trattamenti

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

Elementi da considerare nel Sistema di Gestione DP

DP Governance / DP Risk Management / Compliance / Policy, Guide Lines, Procedures / Monitoring



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

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.

Ruoli legali obbligatori e ruoli discrezionali

Codice privacy	
Ruoli obbligatori per legge	**Ruoli discrezionali**
Titolare del trattamento	Organo di coordinamento
Responsabile «interno» del trattamento (*se individuato dal Titolare*)	
Responsabile «esterno» del trattamento	
Incaricato del trattamento	Data Protection Managers o Referenti privacy

GDPR	
Ruoli obbligatori per legge	**Ruoli discrezionali**
Titolare del trattamento (art. 24)	Organo di coordinamento
DPO (*se sussistono le condizioni di legge*) (art. 37)	
Contitolare del Trattamento (art. 26) Responsabile «esterno» del trattamento (art.28)	
Incaricato del trattamento	Data Protection Managers o Referenti privacy

Il passaggio di regime dal codice privacy al GDPR ha comportato sotto il profilo organizzativo le seguenti innovazioni:

- La figura del responsabile del trattamento **(«processor») «interno»**, non è più un ruolo legale, cioè previsto dalla legge
- Il **Data Protection Officer** («responsabile della protezione dei dati») è un nuovo organo legale di supervisione e vigilanza previsto come obbligatorio in specifiche circostanze.

Sotto entrambi i regimi (codice e GDPR) l'azienda titolare del trattamento ha la facoltà, nell'ambito della propria discrezionalità organizzativa, di prevedere ulteriori figure cui assegnare compiti data protection. L'assetto organizzativo data protection che risponde in modo efficiente ed efficace alla realtà del contesto è un essenziale elemento a **testimonianza dell'accountability** dell'azienda e, quindi, del suo livello di responsabilizzazione, riducendo il rischio di non conformità e di conseguenti sanzioni.

Ruoli DP

Responsabilizzazione
(art. 24)

Norma richiede regolamentazione rapporti tra azienda titolare e altri ruoli DP

- ✓ Titolari e responsabili soggetti a principio responsabilizzazione
- ✓ Formalizzazione scritta
  - **tra co-Titolari** per reciproci obblighi
  - **verso il Responsabile** per obblighi relativi
  - **ad incaricati** per istruzioni
  - **al DPO** per assegnazione di competenze
- ✓ Titolari selezionano responsabili in base all'adozione di misure tecnico-organizzative
- ✓ Responsabile che decide su finalità e mezzi trattamento è considerato titolare

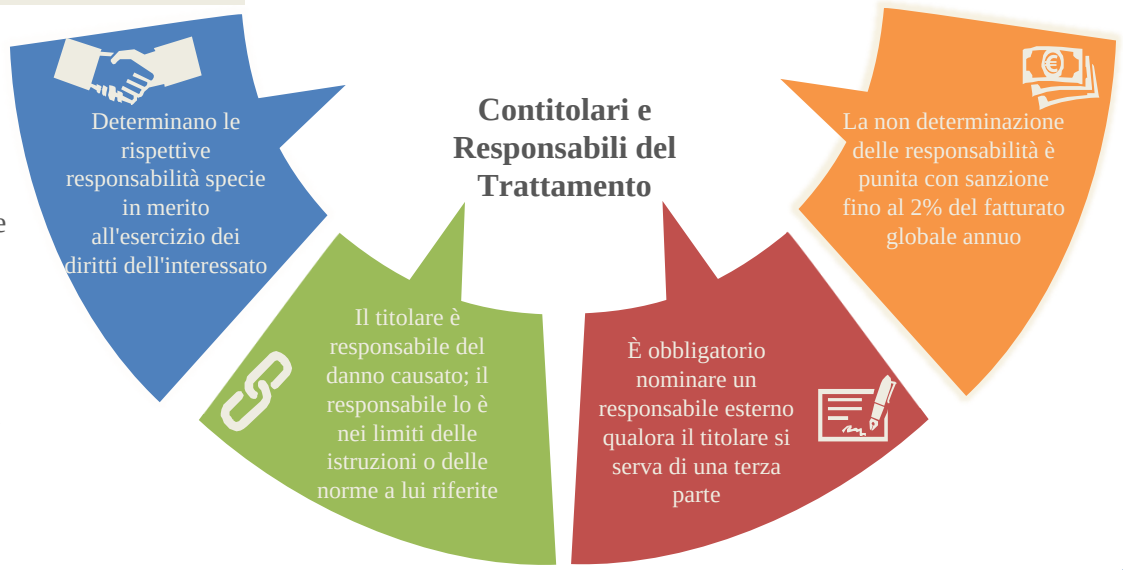
Ruoli DP
(artt. 26, 28/29, 37)

Ruoli DP richiedono effettività di mansioni
Corretto assetto organizzativo ruoli DP incide su adeguatezza MO DP
Il MO o Sistema DP è la cartina di tornasole livello responsabilizzazione azienda

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)



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

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

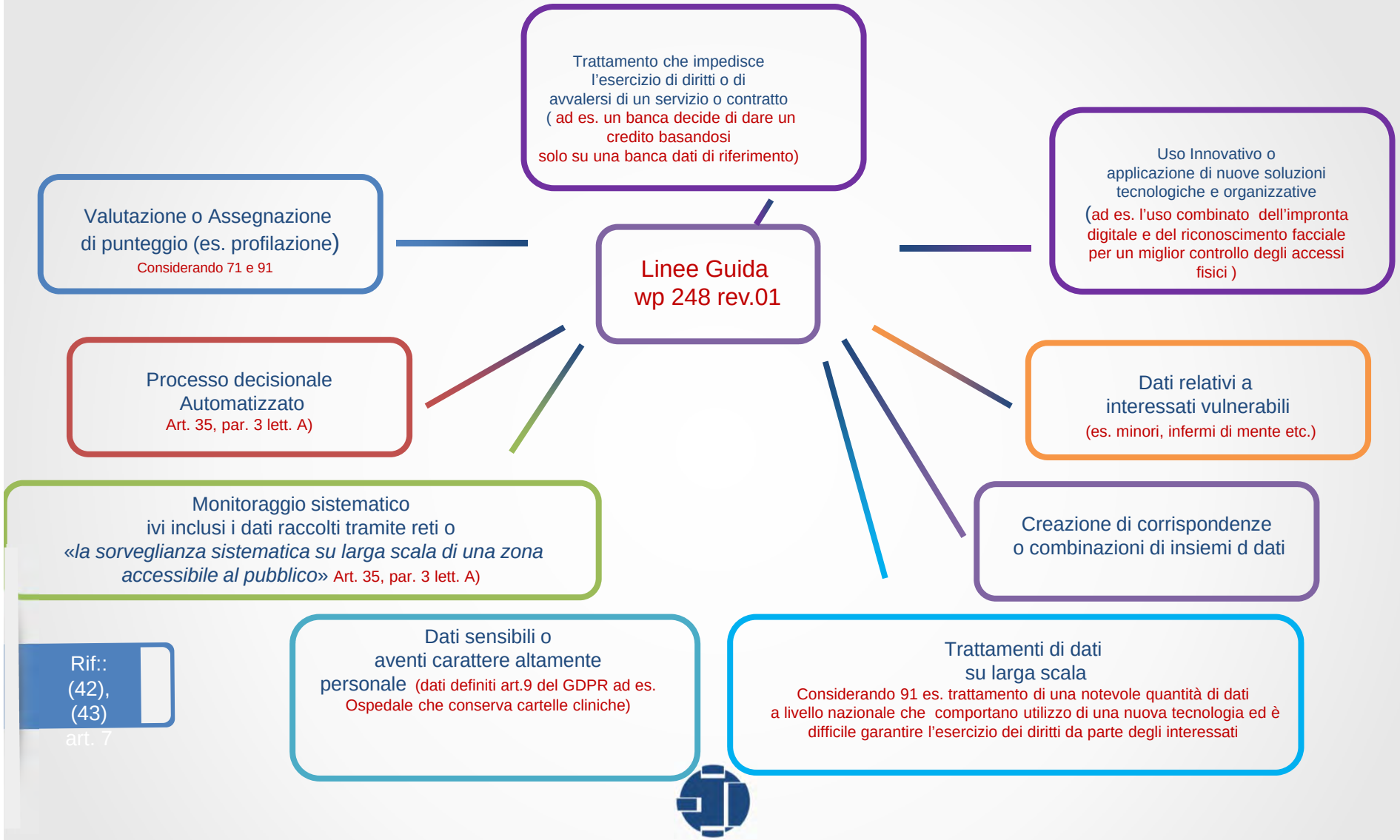
Quando fare la Valutazione d'impatto ?

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)



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)	❑ Dati sensibili o dati aventi carattere estremamente personale ❑ Dati riguardanti soggetti interessati vulnerabili ❑ 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	❑ 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 avente carattere estremamente personale	**Si**

Valutazione d'impatto:
sussistenza di rischio elevato

Soggetti esposti al Rischio

E' interessante notare che il rischio oggetto della DPIA **non** è valutato in relazione all'azienda (cioè non si tratta di accertare un rischio della realizzazione di un evento che possa recare danno all'azienda), piuttosto del verificarsi di un potenziale danno a detrimento di terzi «persone fisiche»

N.B. E' interessante notare come la locuzione utilizzata dal legislatore non faccia riferimento ai diretti «interessati» (vale a dire ai soggetti cui si riferiscono i dati personali oggetto del trattamento in questione) bensì menzioni la più generale categoria delle «persone fisiche»: ciò potrebbe dire che la valutazione del rischio debba tener in conto il potenziale nocumento a danno dell'individuo in generale e non solo della più ristretta categoria dei soggetti cui si riferiscono i dati personali rientranti nel tratta[illegible] parola.

Questa diversa prospettiva di analisi è il fondamento giust[illegible] della prescrizione del GDPR secondo cui: *« se del caso, il Titolare del Trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto», senza che ciò vada a scapito degli interessi commerciali, pubblici o di sicurezza (art. 35 (g)).*

Valutazione d'impatto: Tracciabilità e modalità operative

Fase 1

Si determina se sia necessaria la DPIA:

- ✓ Raccolta di informazioni sul progetto
- ✓ Decisione su ingaggio di stakeholder
- ✓ Identificazione e valutazione del rischio
- ✓ Identificazione opzioni per evitare o mitigare il rischio

Fase 2

- ✓ **Preparazione** del DPIA report
- ✓ **Stesura** delle raccomandazioni
- ✓ **Monitoraggio** raccomandazioni

Principali benefici della DPIA

- ✓ La pronta **identificazione e la gestione dei rischi** relativi alla protezione dei dati
- ✓ **Risoluzione gap potenziali in termini di compliance e sicurezza** evitando, quindi, perdita di fiducia e danni reputazionali

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

Consultazione preventiva

GARANTE

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

Assistito su richiesta dal Responsabile

Rif::
(94)
Art. 36

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)*

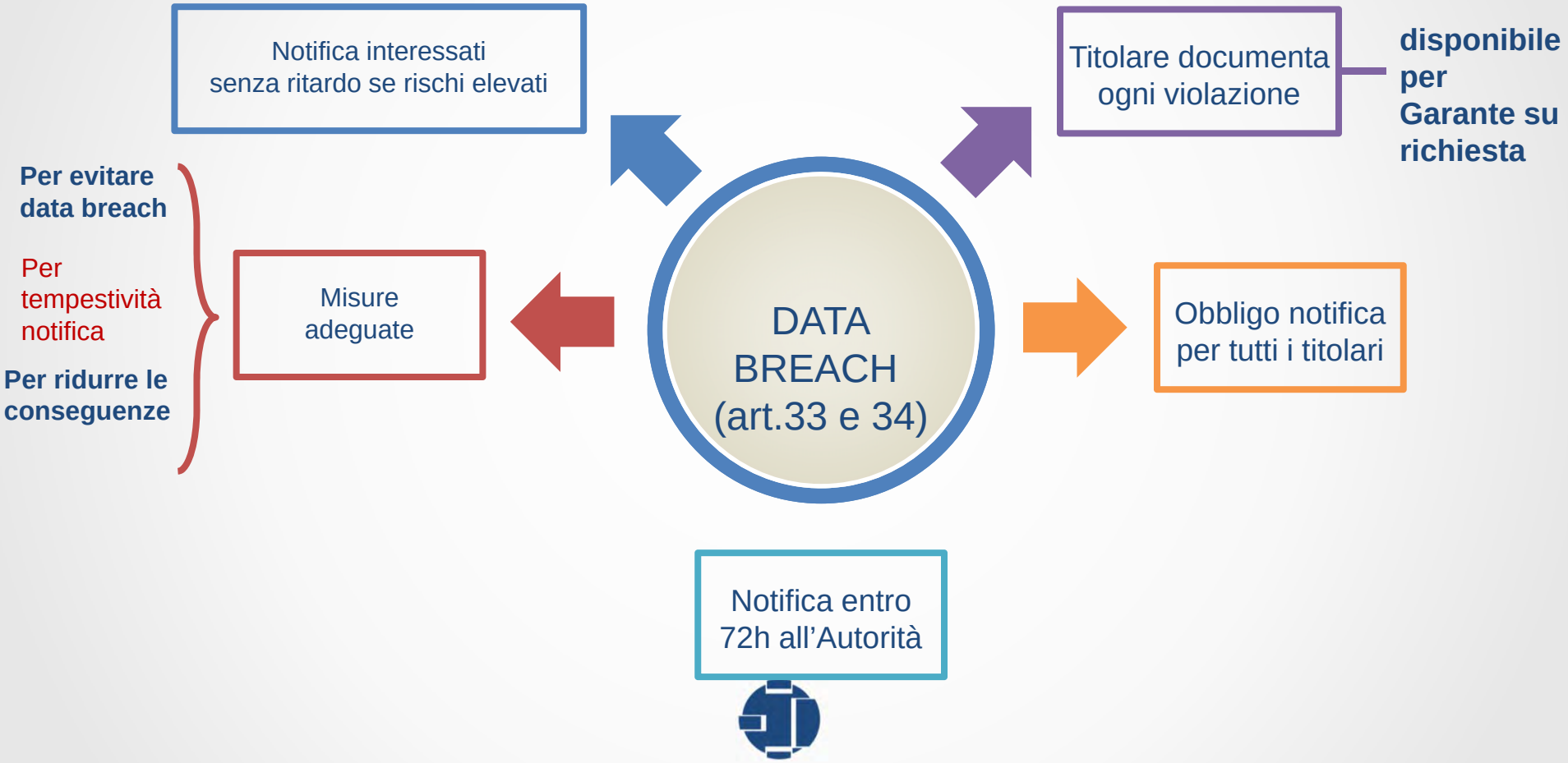
Strumento di **verifica e dimostrazione di conformità**

Strumento di **riduzione e valutazione del risc**

Modello organizzativo

Supporto e facilitazione **all'esercizio del diritti**

Data Breach: in sintesi



DPO

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 purchè «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

Flussi informativi tra DPO e altri ruoli DP

TITOLARE

Coinvolge la figura del DPO:

- ✓ In caso di **verifica ispettiva o richiesta da parte di organismi di controllo o Authority** sul tema della protezione dei dati,
- ✓ in tutte le **questioni data protection**

DPO

Riferisce al Titolare:

- ✓ circa lo stato di **conformità del sistema** aziendale data protection
- ✓ Sul livello di **sensibilizzazione** degli addetti
- ✓ **Fornisce consulenza ed informa** Titolari e responsabili
- ✓ **Interagisce con gli interessati**

RESPONSABILI/REFERENTI/ INTERESSATI

- ✓ Richieste di **informazioni** e **consulenza** da responsabili/referenti
- ✓ **Esercizio dei diritti** da parte degli interessati

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.

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

GRUPPOIMPERIALI

Grazie

Avv. Riccardo Imperiali

riccardo.imperiali@imperiali.com

Dott.ssa Anna Irace

anna.irace@imperiali.com

Aggiungici su

gruppoimperiali