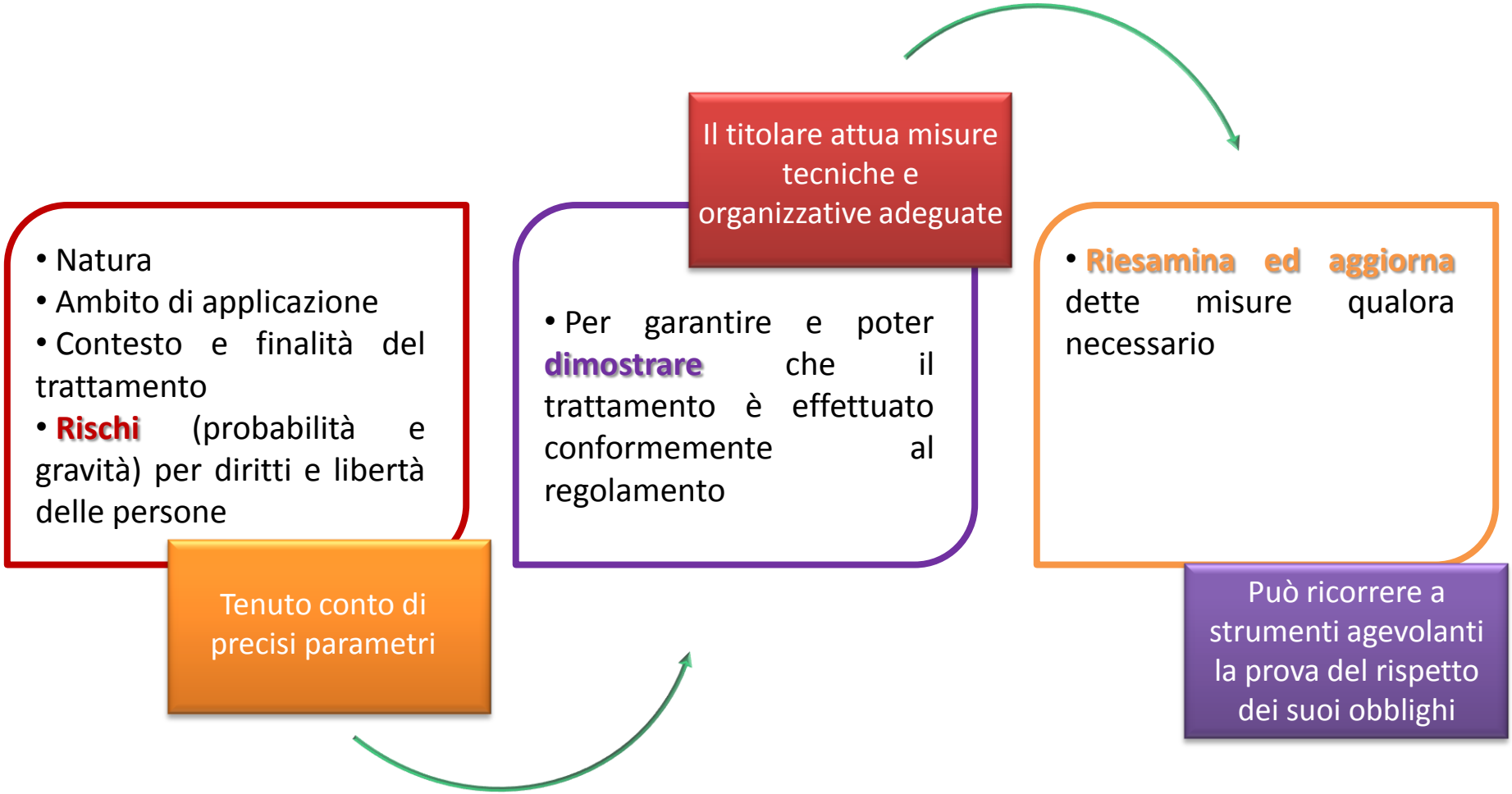
Regolamento UE 2016/679: le principali novità

Accountability ed approccio *risk based*



Registri dei trattamenti

Responsabile della Protezione dei Dati (RPD)

Nell'eseguire i suoi compiti il RPD considera

I rischi inerenti al trattamento

Tenuto conto

- Della natura
- Dell'ambito di applicazione
- Del contesto
- Delle finalità

Privacy by design e by default

Il titolare del trattamento, tenendo conto di precisi parametri

Stato dell'arte	Costi di attuazione	Natura, ambito , finalità trattamento	Rischi (prob. e gravità)

Mette in atto misure tecniche e organizzative adeguate

Come la pseudonimizzazione

Volte ad attuare in modo efficace i principi di protezione dei dati

Quali la minimizzazione

Ed a integrare nel trattamento le necessarie garanzie

Al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati

Contitolarità (Contratto)

Quando due o più titolari determinano congiuntamente le finalità ed i mezzi del trattamento sono contitolari del trattamento

I contitolari devono definire in modo trasparente, mediante un accordo interno, le rispettive responsabilità:

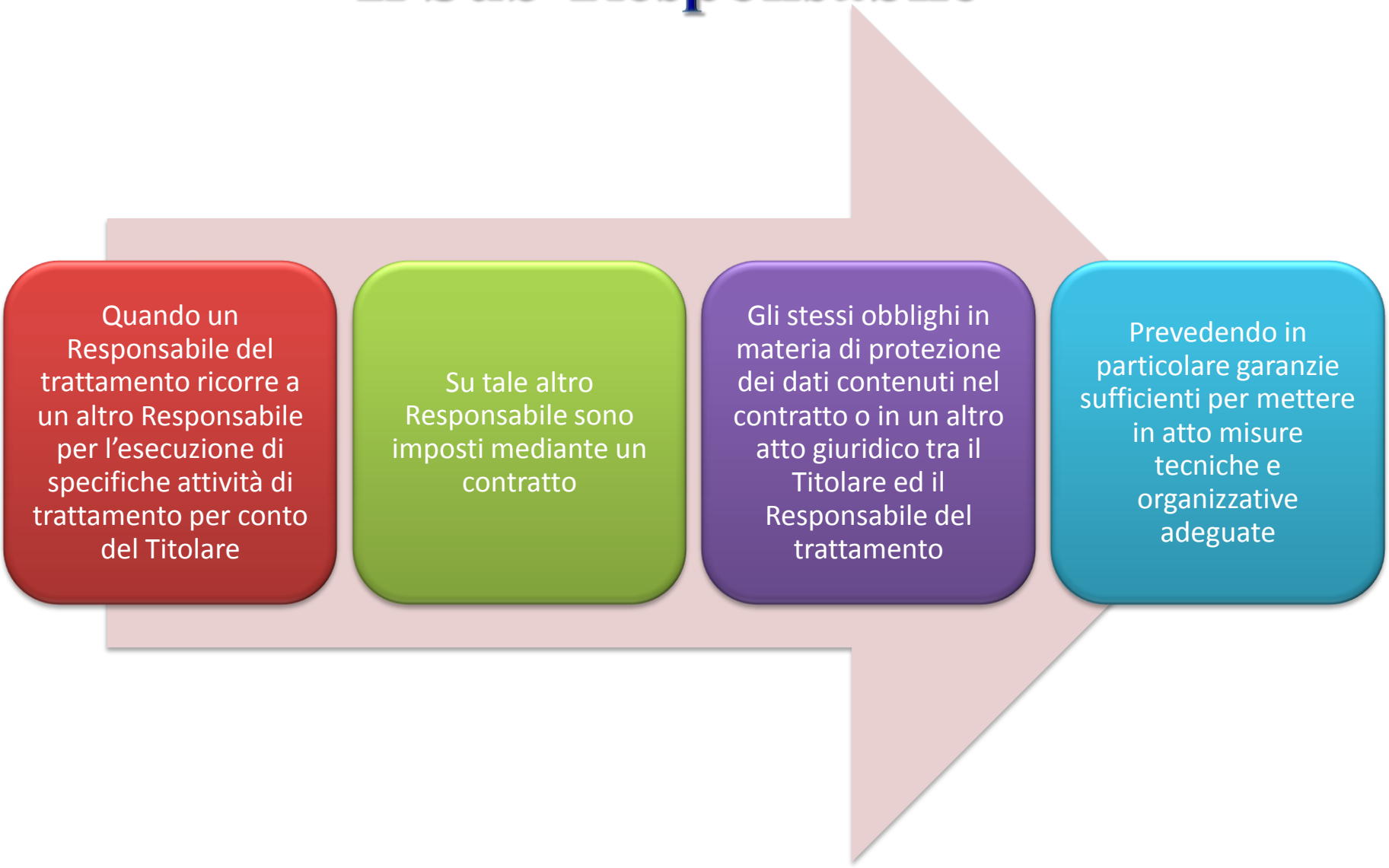
- **Gestione dei diritti dell'interessato**
- **Rispettive funzioni di rilascio dell'informativa**

L'accordo deve riflettere adeguatamente

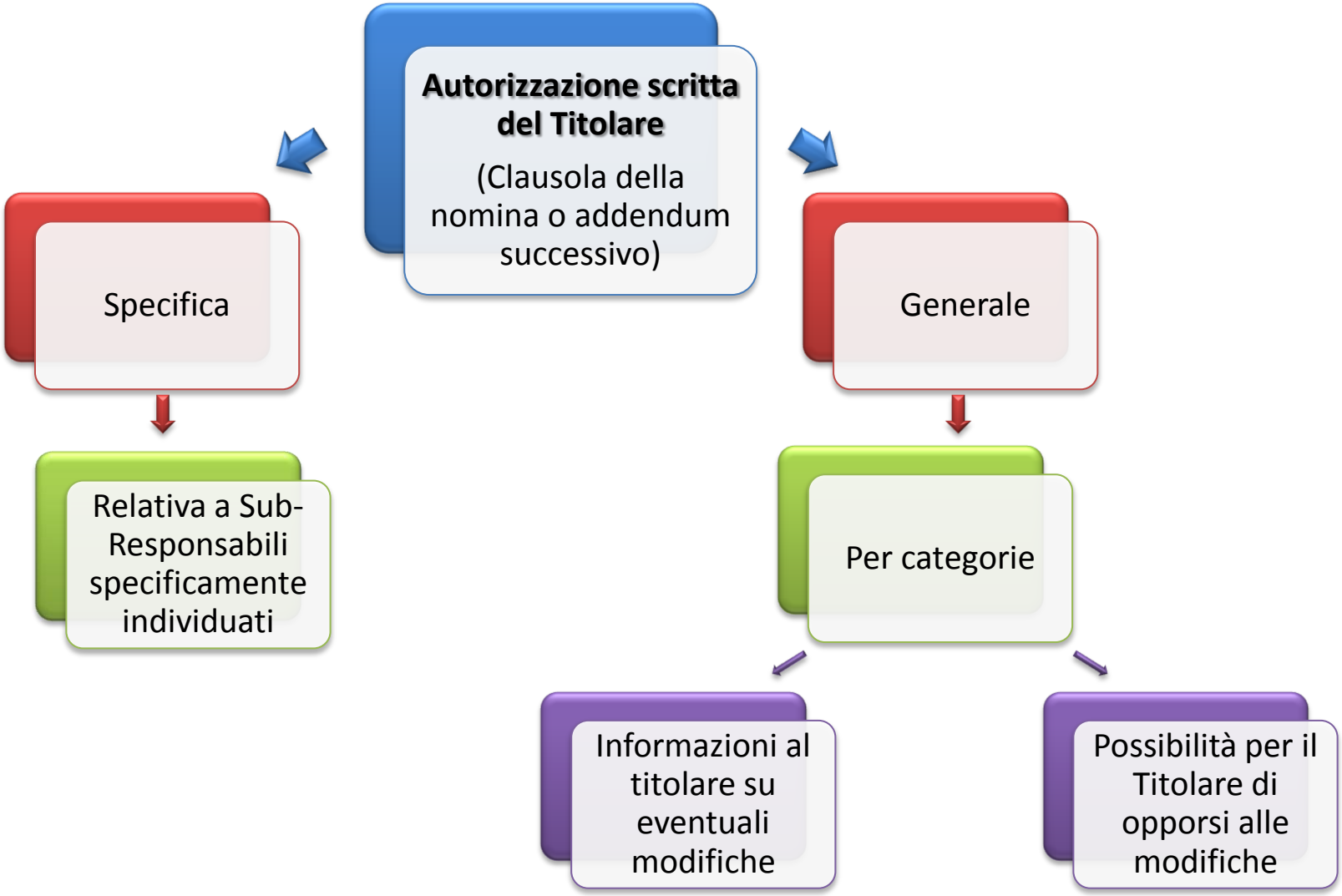
- **I rapporti con gli interessati**
- **I rispettivi ruoli**

Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato che può esercitare i propri diritti nei confronti di e contro ciascun Titolare

Il Sub-Responsabile



Disciplina del Sub-Responsabile

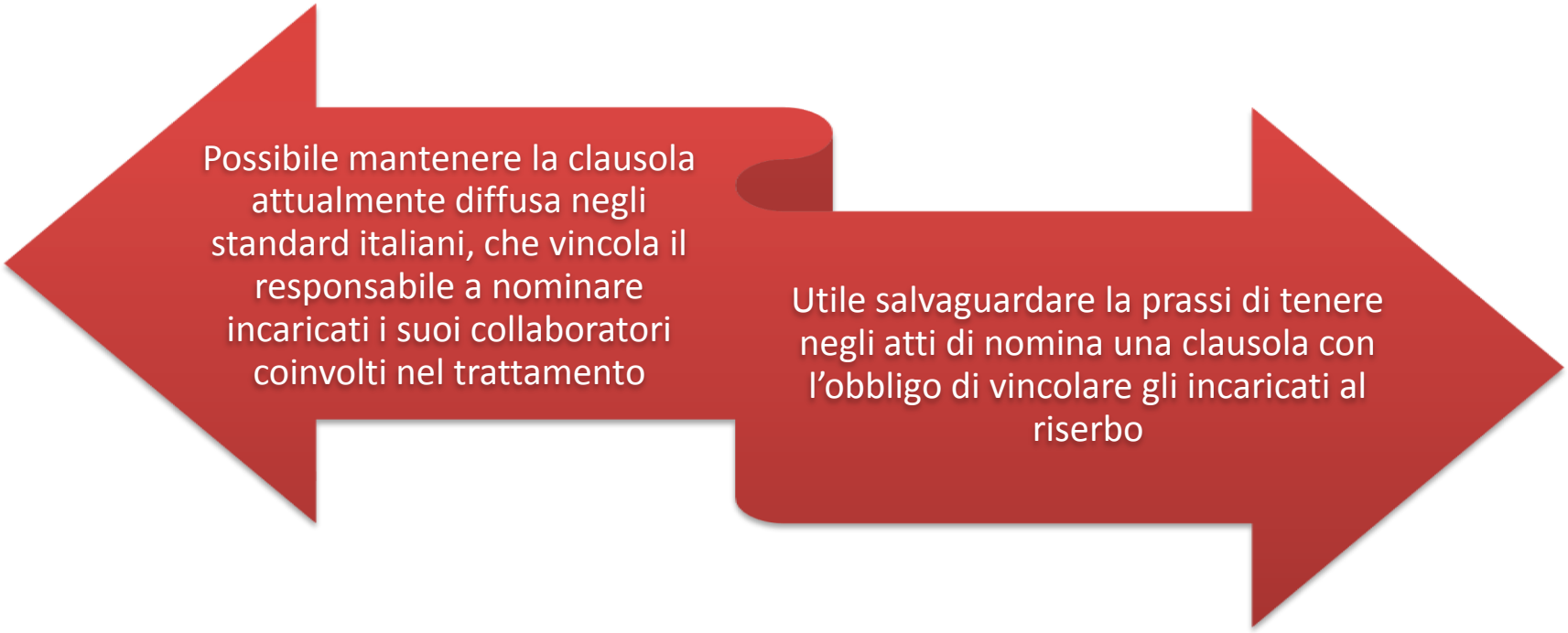


Trattamento dietro istruzione documentale del Titolare

Il responsabile deve trattare i dati personali soltanto su istruzione documentale del Titolare

Istruzioni operative, eventualmente allegate all'atto di nomina	Verbalizzazione di indicazioni date dal Titolare durante il servizio, se hanno impatto sui trattamenti	Documentazione di indicazioni migliorative previste a seguito di attività ispettive

Vincolo di riserbo per le persone autorizzate (incaricati)



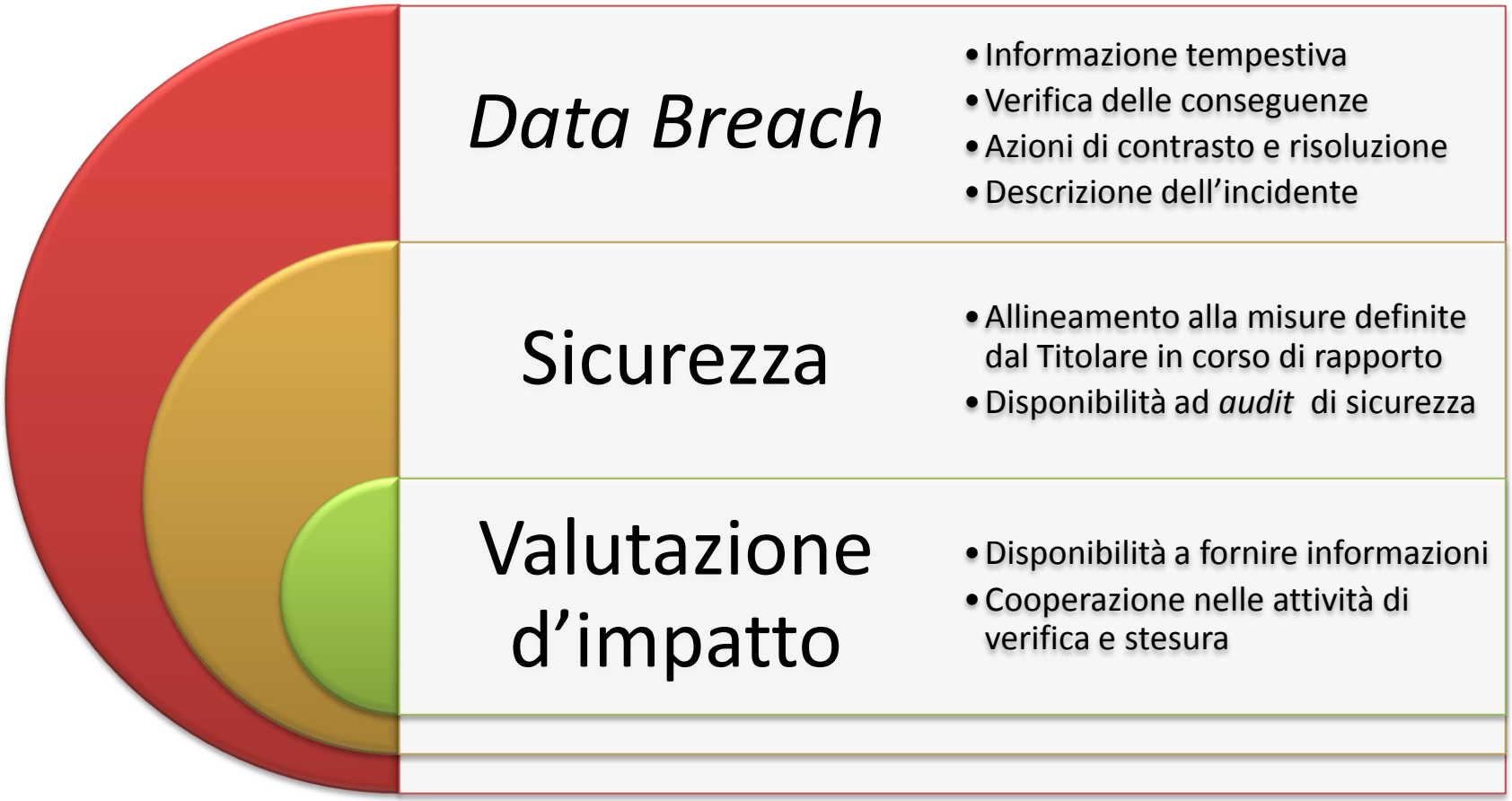
Oneri in materia di sicurezza a carico del Responsabile

A
- Se possibile, pseudonimizzazione e cifratura dei dati personali

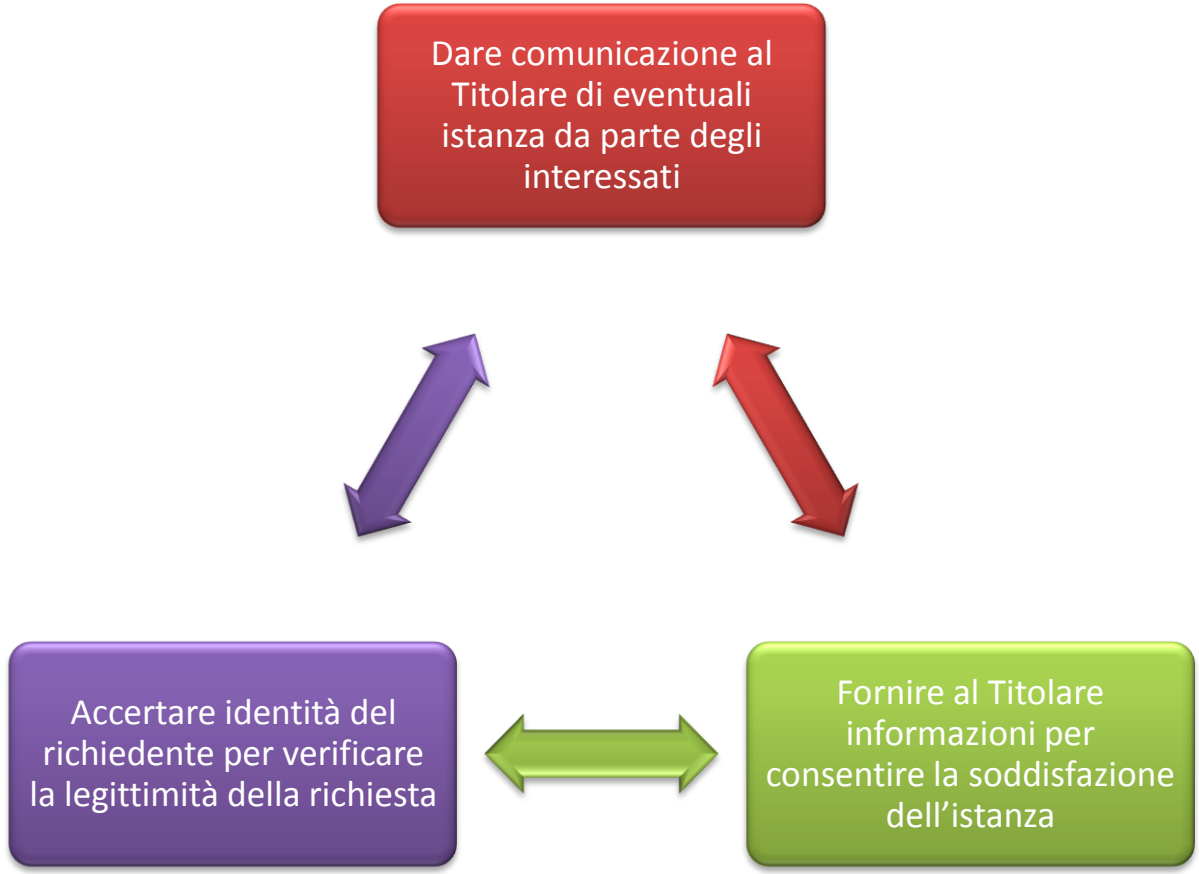
B
- Capacità di assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi

C
- Procedura per testare, verificare e valutare l'efficacia delle misure tecniche e organizzative per garantire la sicurezza del trattamento

Assistenza al Titolare sui temi di *compliance*



Assistenza nella gestione Delle richieste degli interessati



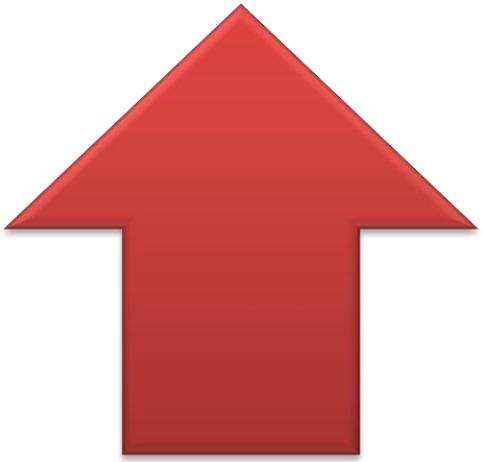
Cancellazione o restituzione dei dati
Alla fine del rapporto

Su scelta del Titolare

Cancellare o restituire tutti i dati personali	Cancellare le copie di *back up* esistenti

Suggerimento: chiedere la distruzione dei dati, con relativa attestazione di avvenuta distruzione, se il titolare preferisce la cancellazione.

Valutazione d'impatto (DPIA) : cos'è?



E' un processo **obbligatorio** di valutazione del rischio

Solo quando il trattamento abbia **rischio elevato** per i diritti e le libertà delle persone

Operazioni di trattamento soggette a DPIA

Trattamento che prevede l'uso di nuove tecnologie in considerazione di:

- Natura
- Oggetto
- Contesto
- Finalità del trattamento

Può presentare un rischio elevato

- Peri i diritti
- Per le libertà delle persone

Il Titolare effettua, prima di procedere al trattamento

- Una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali

Tre casi in cui la DPIA è necessaria

Valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone.

Trattamento, su larga scala, di categorie particolari di dati sensibili o relativi a condanne penali

Sorveglianza sistematica su larga scala di una zona accessibile al pubblico

In sintesi

1. • Trattamenti valutativi o di *scoring*
2. • Decisioni automatizzate che producono significativi effetti giuridici o di analoga natura
3. • Monitoraggio sistematico
4. • Dati sensibili o dati di natura estremamente personale
5. • Trattamenti di dati su larga scala
6. • Combinazione o raffronto di insieme di dati
7. • Dati relativi a categorie di interessati “vulnerabili”
8. • Utilizzi innovatiti o applicazioni di nuove soluzioni tecnologiche
9. • Trattamenti che “impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto”

La DPIA è necessaria per i trattamenti già in corso?

Contenuto della DPIA

Una **descrizione sistematica dei trattamenti previsti e delle finalità del trattamento**, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare

Le misure previste per affrontare i rischi includendo le **garanzie**, le **misure di sicurezza** ed i **meccanismi per garantire la protezione dei dati** personali e dimostrare la conformità al Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati

Una valutazione della **necessità e proporzionalità dei trattamenti** in relazione alle finalità

Valutazione dei **rischi per i diritti e le libertà** degli interessati