Sicurezza del dato, come presupposto al trattamento

ASSOPRIVACY

Roberto Ballanti
AP & Partner Srl – Management Consulting
Consulente Ict e Privacy Officer – DPO

Sala Opera Don Guanella Como
Via Tommaso Grossi, 18
22100 Como

Lunedì, 18 novembre 2019

Agenda

1. Cambiamenti … l'ACCOUNTABILITY cambia il modo di agire

2. Le misure di sicurezza … in funzione dei rischi sul trattamento

3. Quali sono le misure per la gestione del rischio?

1

Cambiamenti … l'ACCOUNTABILITY cambia il modo di agire

Cambiamenti … l'ACCOUNTABILITY cambia il modo di agire

"**Non è la più forte** delle specie che sopravvive, **né la più intelligente**, ma **quella più reattiva ai cambiamenti.**"

Teoria dell'evoluzione

CHARLES ROBERT DARWIN

Cambiamenti … l'ACCOUNTABILITY cambia il modo di agire

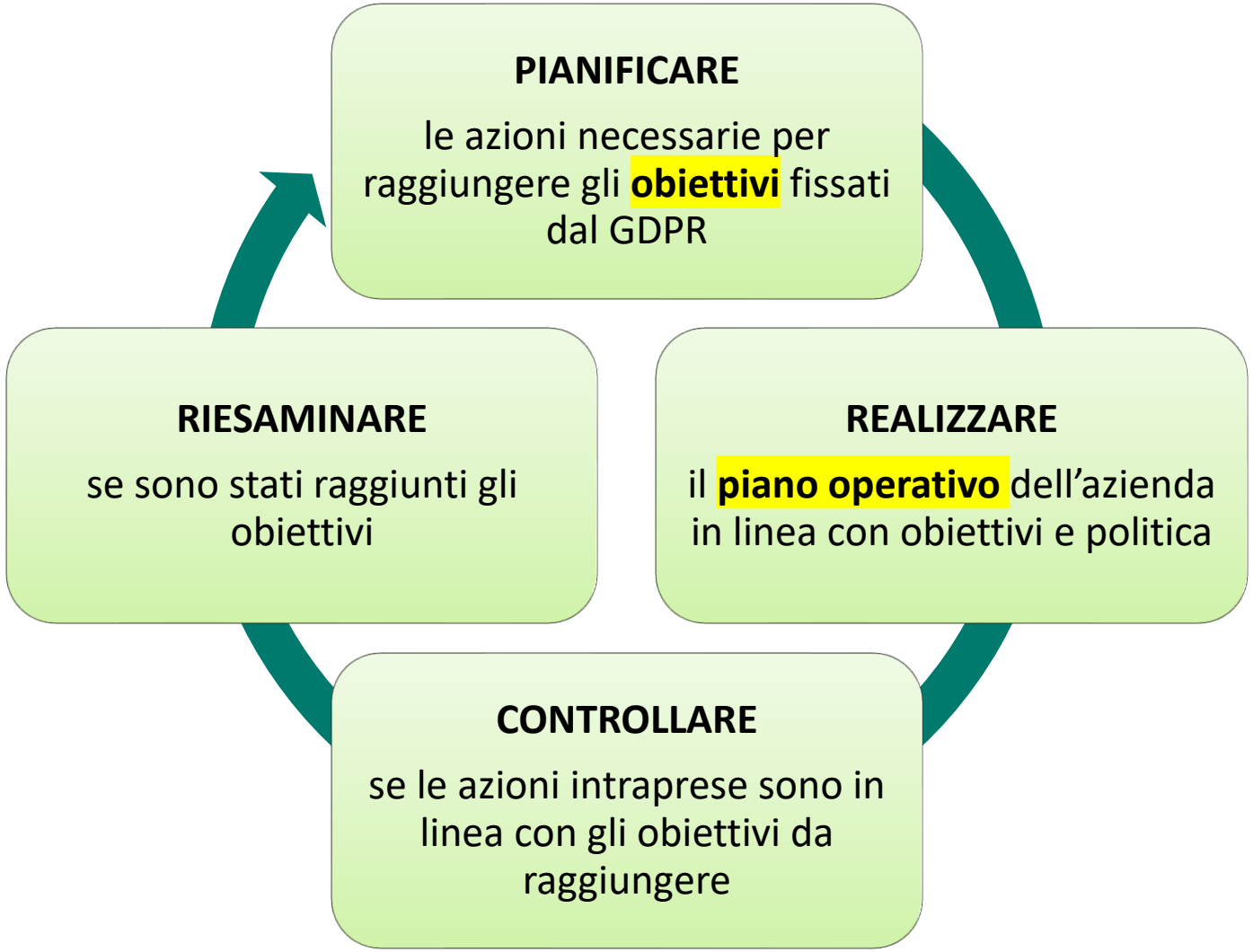
Cosa deve fare? Dalla forma alla sostanza

- Art. 5 § 2: «Il **titolare del trattamento è competente** per il rispetto (…) dei principi applicabili al trattamento e **in grado di comprovarlo**.»
- Cons. 74: (…) il titolare del trattamento dovrebbe mettere in atto **misure adeguate** ed efficaci ed essere **in grado di dimostrare la conformità** delle attività di trattamento con il presente

Il principio di «**responsabilizzazione o accountability**» si concretizza nel **rispetto dei principi applicabili al trattamento** (art. 5), delle **condizioni di liceità del trattamento** (art. 6), nella capacità del titolare di **dimostrare di averli osservati**, di aver rispettato il Regolamento e di **aver attuato misure efficaci** (art. 24). **Dette misure sono riesaminate e aggiornate qualora necessario**

Cambiamenti … l'ACCOUNTABILITY cambia il modo di agire

Implementare un sistema di gestione come supporto alla conformità al GDPR



Cambiamenti … l'ACCOUNTABILITY cambia il modo di agire

Aree d'intervento

Approccio interdisciplinare e integrato

Cambiamenti … l'ACCOUNTABILITY cambia il modo di agire

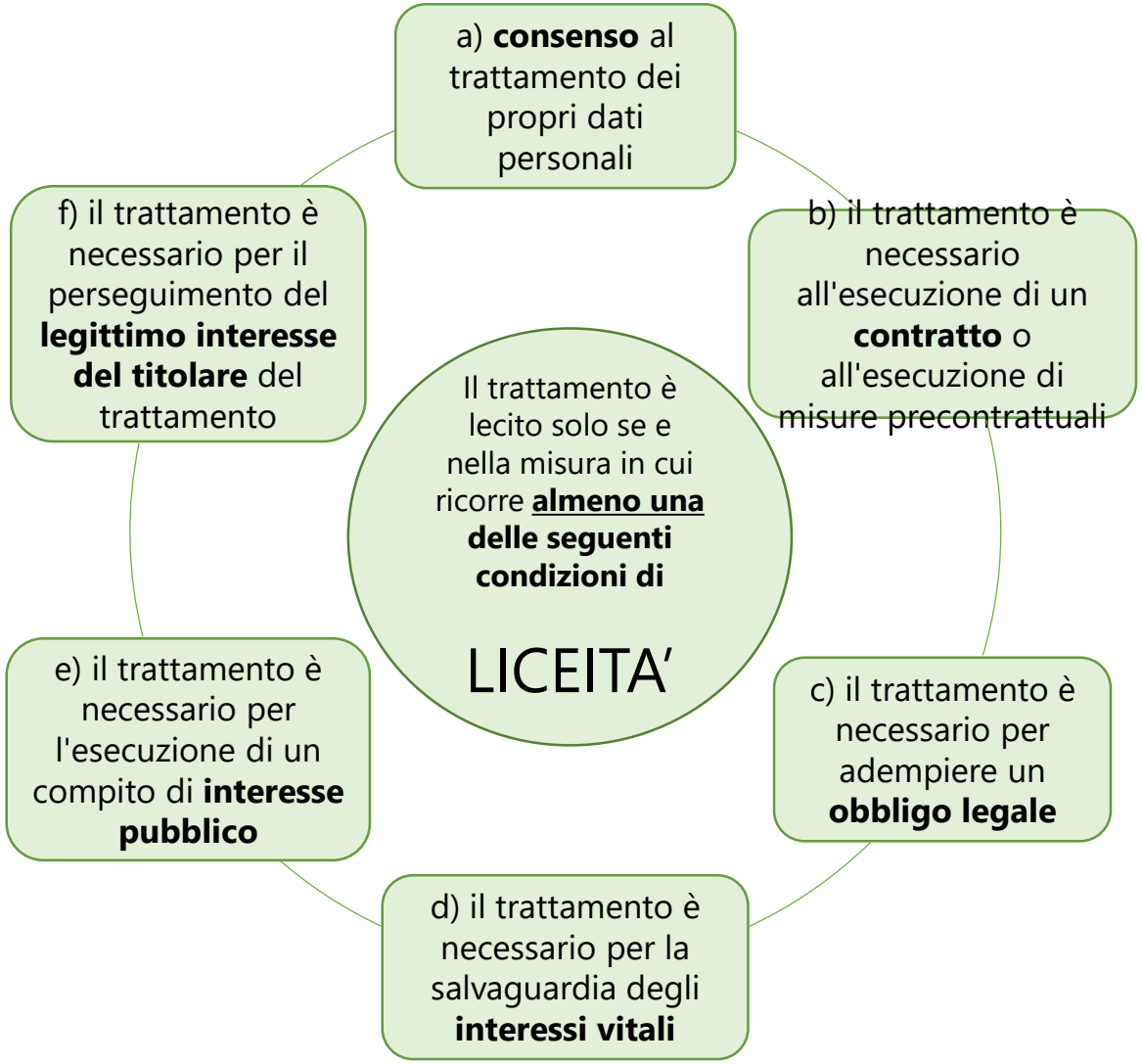
OBIETTIVI GIURIDICI DEL GDPR: Art. 5

I principi applicabili al trattamento dei dati personali

Cambiamenti … l'ACCOUNTABILITY cambia il modo di agire

OBIETTIVI GIURIDICI DEL GDPR: Art. 6 § 1

Condizioni di liceità del trattamento



Cambiamenti … l'ACCOUNTABILITY cambia il modo di agire

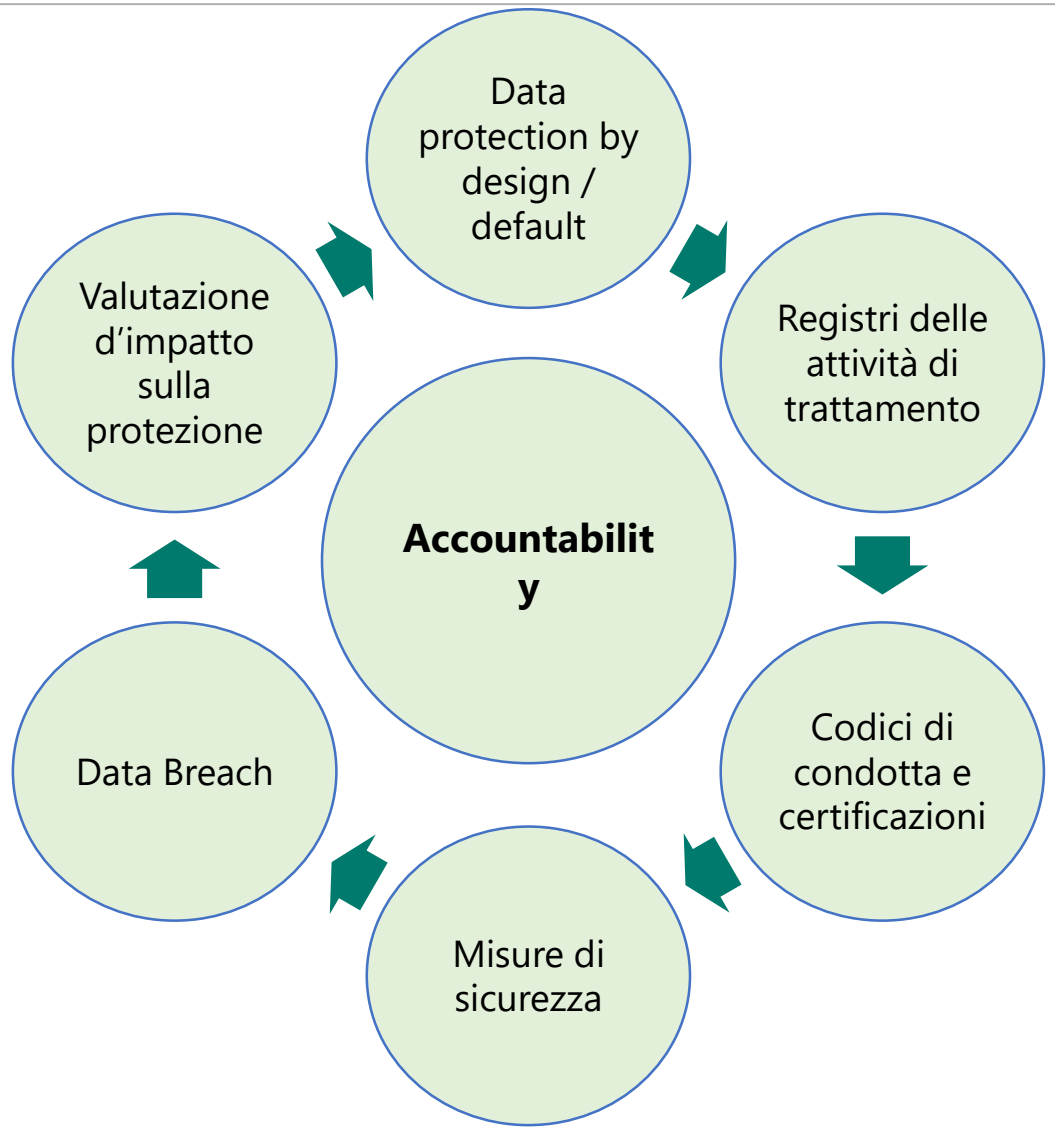
OBIETTIVI ORGANIZZATIVI DEL GDPR:

le conseguenze della Responsabilizzazione

Cambiamenti … l'ACCOUNTABILITY cambia il modo di agire

OBIETTIVI TECNICI DEL GDPR:

le conseguenze della Responsabilizzazione



2

Le misure di sicurezza, in funzione dei rischi sul trattamento

Le misure di sicurezza, in funzione dei rischi sul trattamento

Definizione di Rischio

Per "**rischio**" si intende uno scenario descrittivo di un evento e delle relative conseguenze, **per i diritti e le libertà,** che sono stimate in termini di **gravità** e **probabilità**»

(Linee guida del Gruppo di lavoro Articolo 29 WP248rev.1)

Le misure di sicurezza, in funzione dei rischi sul trattamento

Art. 32 del GDPR – Sicurezza del trattamento

Le misure di sicurezza devono garantire un livello di sicurezza **adeguato** **al rischio** sul **trattamento**.

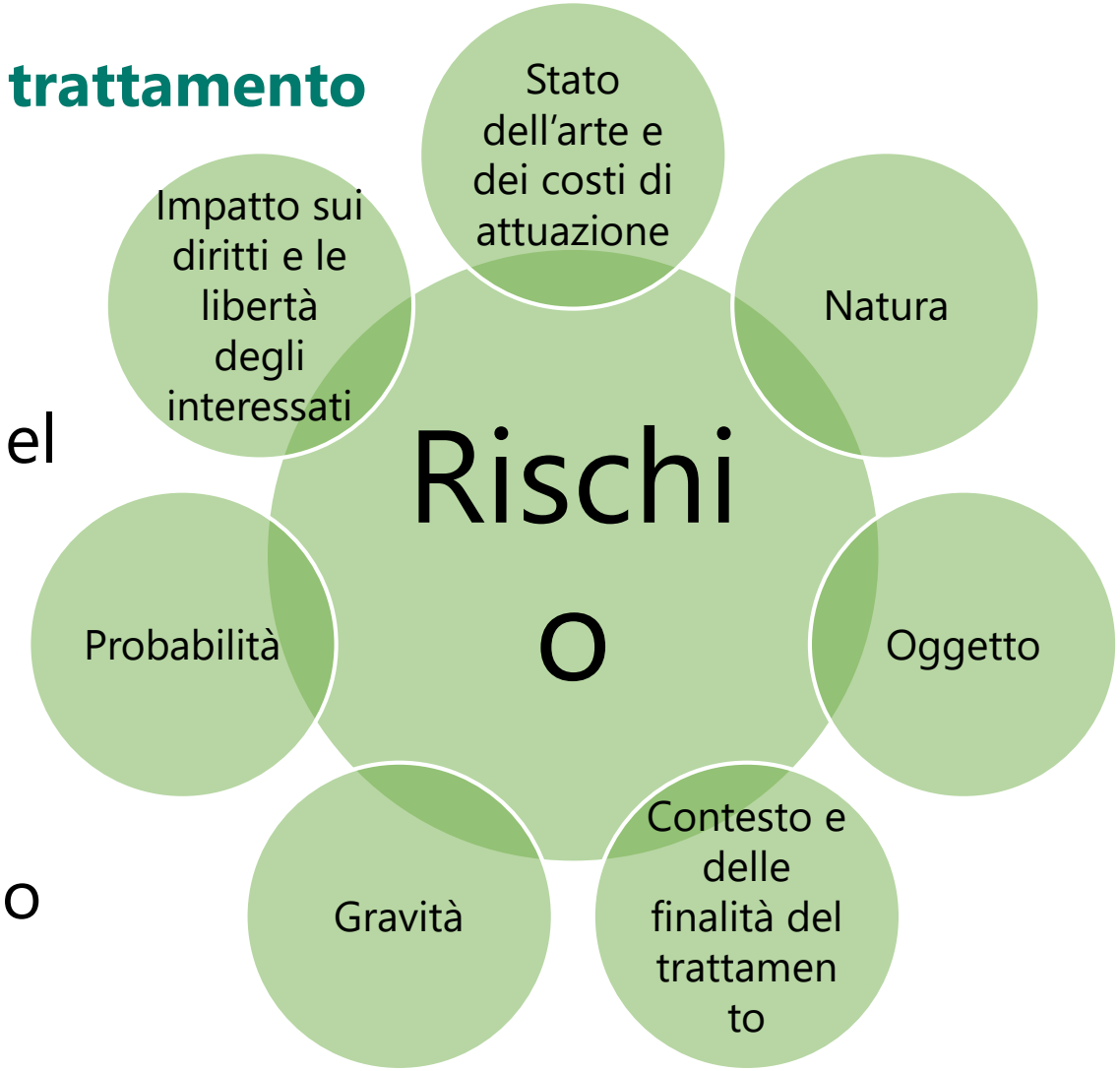
Quindi, **non potranno sussistere obblighi generalizzati di adozione di misure "minime" di sicurezza** (ex art. 33 del D.Lgs. 196/03) poiché tale **valutazione sarà decisa**, caso per caso, dal titolare e dal responsabile in rapporto **ai rischi specificamente individuati**.

MISURE MINIME DI SICUREZZA ≠ MISURE DI SICUREZZA ADEGUATE

Le misure di sicurezza, in funzione dei rischi sul trattamento

Art. 32 del GDPR – Sicurezza del trattamento

Elementi che compongono **l'entità del rischio,** il quale deve essere mitigato, da parte del titolare o del Responsabile, mettendo in atto **misure tecniche e organizzative adeguate** a garantire un livello di **sicurezza del**



Le misure di sicurezza, in funzione dei rischi sul trattamento

ATTENZIONE! LA VALUTAZIONE DEL RISCHIO DEVE ESAMINARE

Aspetti riguardanti la sicurezza del trattamento

Aspetti attinenti le conseguenze negative del trattamento

Le misure di sicurezza, in funzione dei rischi sul trattamento

Art. 32 del GDPR – Sicurezza del trattamento

Nel **valutare l'adeguato livello di sicurezza**, si deve tenere conto in special modo dei rischi presentati dal trattamento che derivano in particolare:

- dalla **distruzione,**
- dalla **perdita,**
- dalla **modifica**,
- dalla **divulgazione non autorizzata** o **dall'accesso**,

in modo **accidentale o illegale**, a dati personali trasmessi, conservati o comunque trattati.

Le misure di sicurezza, in funzione dei rischi sul trattamento

Aspetti riguardanti la sicurezza del trattamento – Modello R.I.D.

R **Riservatezza**

Protezione dei dati trasmessi o conservati per evitarne l'intercettazione e la visione da parte di soggetti terzi non autorizzate.
Rientra in questo ambito la problematica dell'autenticazione sicura ovvero dell'identificazione certa ed univoca del soggetto che accede al sistema ed ai dati.

I **Integrità**

Veridicità che i dati trasmessi, ricevuti o conservati siano completi e non alterati

D **Disponibilità**

Esigenza che i dati siano sempre accessibili e che i servizi funzionino anche nel caso di interruzioni dovute, ad esempio, alla cessazione dell'energia elettrica, a eventi disastrosi naturali, eventi imprevisti e/o ad attacchi di pirateria informatica

Le misure di sicurezza, in funzione dei rischi sul trattamento

Che cosa è una violazione dei dati personali (Data breach)?

È un evento che comporta, in modo **accidentale** o in modo **illecito**:

- la **distruzione**;
- la **perdita**;
- la **modifica**;
- la **divulgazione non autorizzata**;
- l'accesso ai dati personali **trasmessi**, **conservati** o comunque trattatati

LA VIOLAZIONE DEI DATI PERSONALI PUO' COMPROMETTERE LA RISERVATEZZA, L'INTEGRITA' O LA DISPONIBILITA' DEI DATI

Le misure di sicurezza, in funzione dei rischi sul trattamento

Conseguenze negative del trattamento

Una **violazione dei dati personali**, se non affrontata in modo adeguato e tempestivo, può **comportare danni fisici, materiali o immateriali** alle persone fisiche quali …

Considerando 85 del GDPR

3

Quali sono le misure per la gestione del rischio?

Quali sono le misure per la gestione del rischio?

- Qualità dei dati ***(pertinenti, necessari, completi, esatti, aggiornati, etc.)***
- Minimizzazione
- Conservazione adeguata
- Cifratura e Pseudonimizzazione dei dati
- Anonimizzazione dei dati

Quali sono le misure per la gestione del rischio?

- **Misure tecnologiche**
  - policy di sicurezza logiche e fisiche, aggiornamenti servizi e software, test, controllo accessi e tracciamento operazioni
- **Misure organizzative**
  - ruoli, governance, istruzioni, formazione, procedure, audit, strumenti di controllo per gli interessati, contatti

Alcune riflessioni conclusive

- Il GDPR vuole **tutelare i diritti e le libertà** delle persone fisiche e la **libera circolazione dei dati**
- Cambiamento culturale: necessità di un **approccio proattivo** nel considerare i doveri in materia di protezione dei dati
- La sicurezza informatica è **necessaria ma non sufficiente**
- Il GDPR non è una norma **prescrittiva**, ma si basa sul principio della «**Responsabilizzazione**» del Titolare o del Responsabile del trattamento

Il dato personale è la traslazione delle persone fisiche nella realtà virtuale, e la protezione dei dati personali è lo strumento di difesa

GRAZIE PER L'ATTENZIONE!

Roberto Ballanti

Per informazioni e approfondimenti:

Cell. 338 62 60 144
r.ballanti@assoprivacy.eu