1 Il contesto

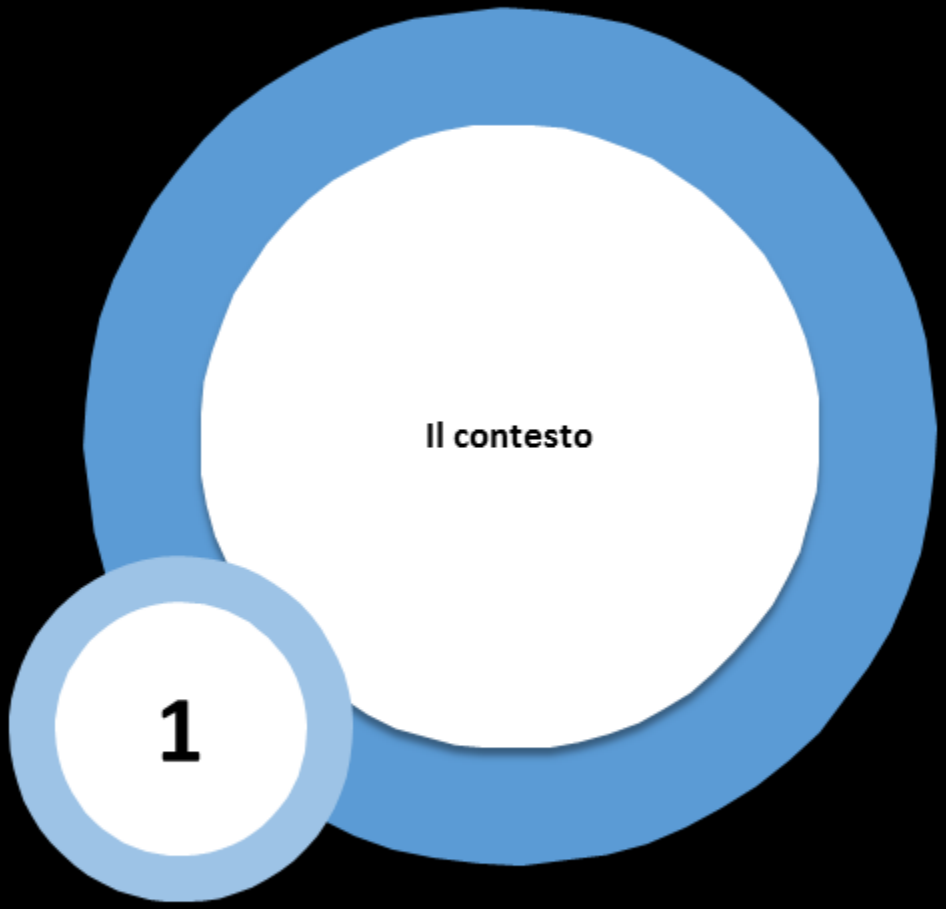
2 L'impatto del regolamento

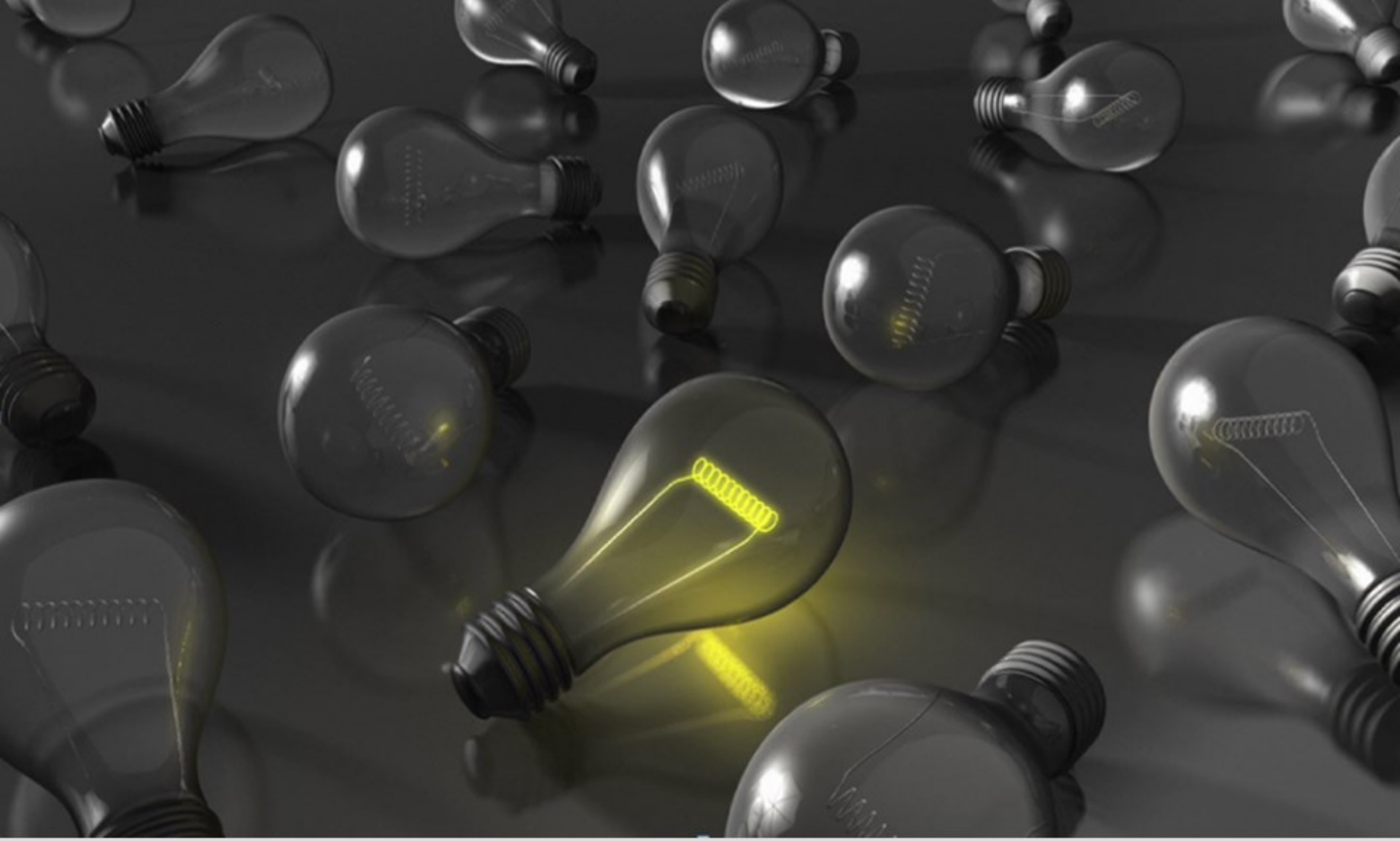
3 Il supporto del Garante alla PA

Il Regolamento UE 2016/679 e il ruolo del Responsabile dei dati personali per l'accountability

Dicembre 2017

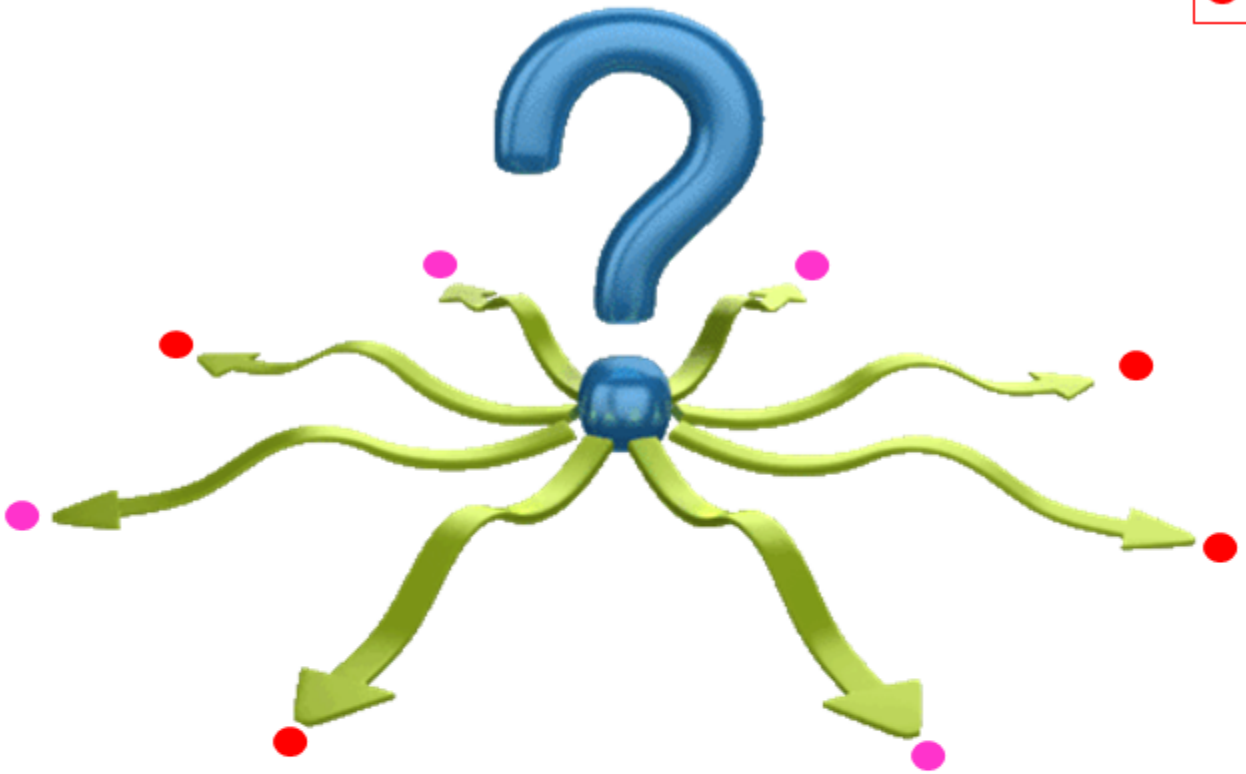
Francesco MODAFFERI


Il contesto
1



Qual’è l’impatto della protezione dei dati nel contesto del settore pubblico oggi?

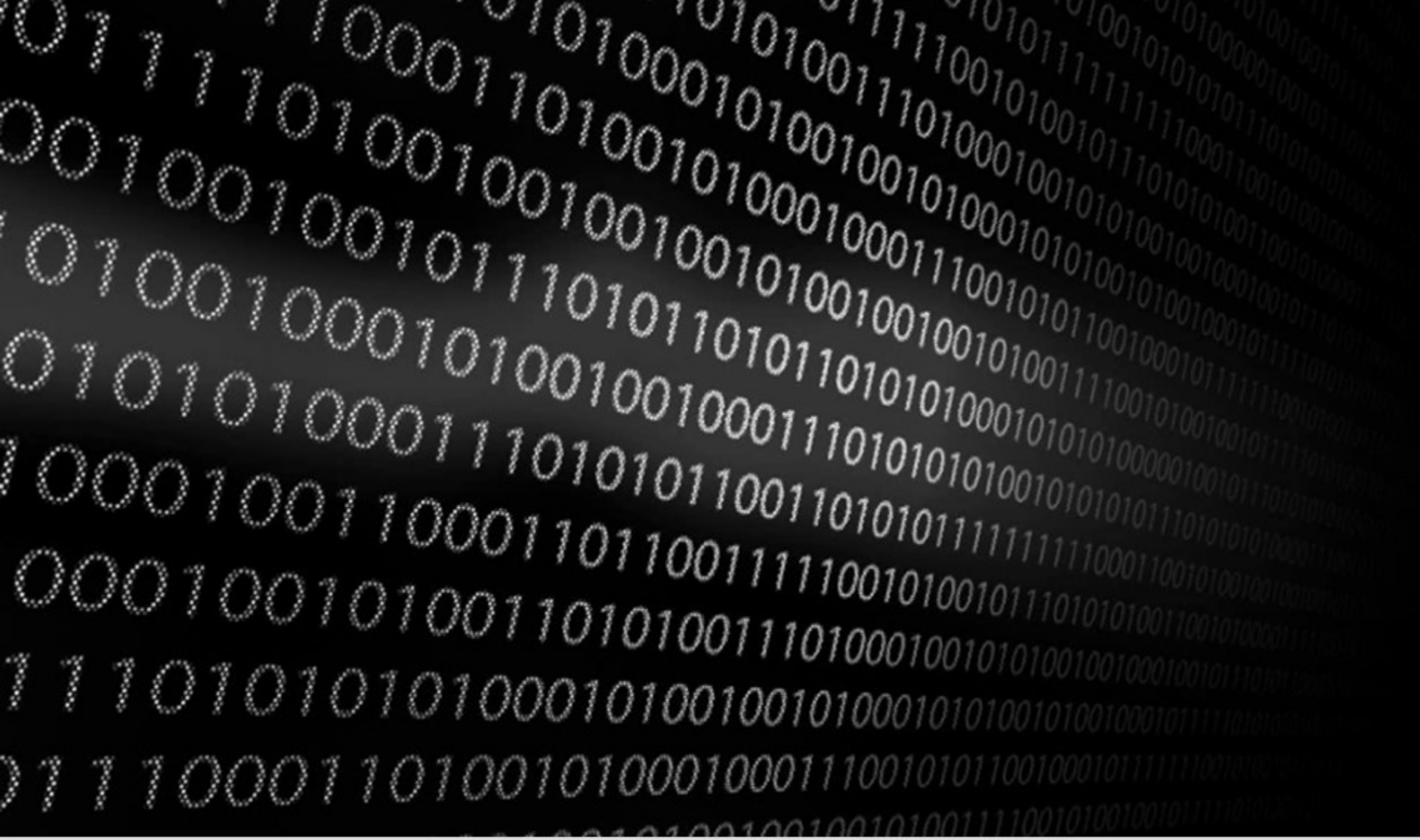
Outsourcer



Società in house

Quando un trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento

Cosa intendiamo per trattamento dei dati nel settore pubblico?



La pubblica amministrazione oggi e la sua dimensione digitale…

…opportunità tra mille contraddizioni

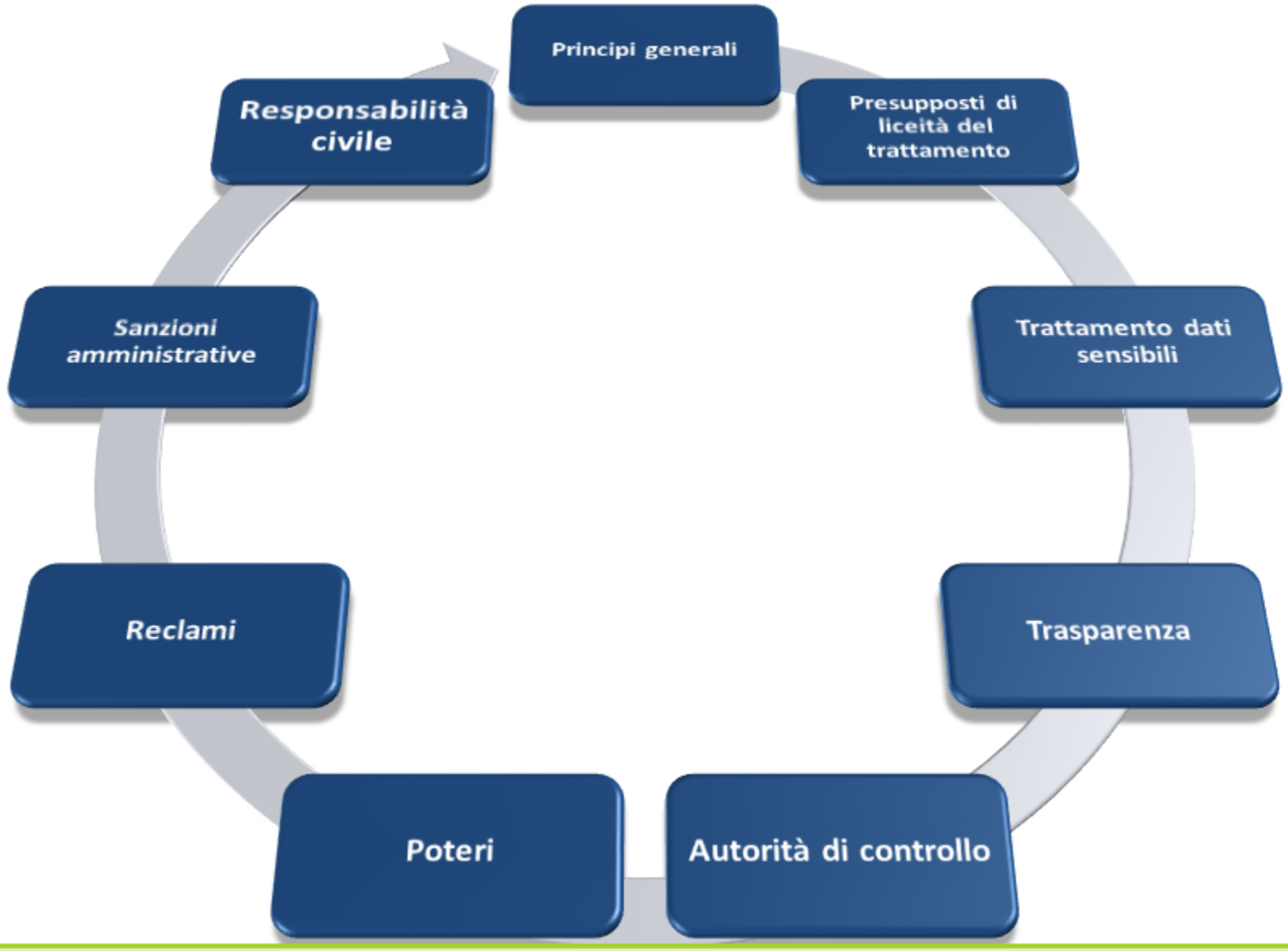
Il vero cambiamento non è dovuto alle nuove regole di protezione dei dati !!

Connessione tra l'elaborazione giuridica del concetto di privacy e il progresso tecnologico

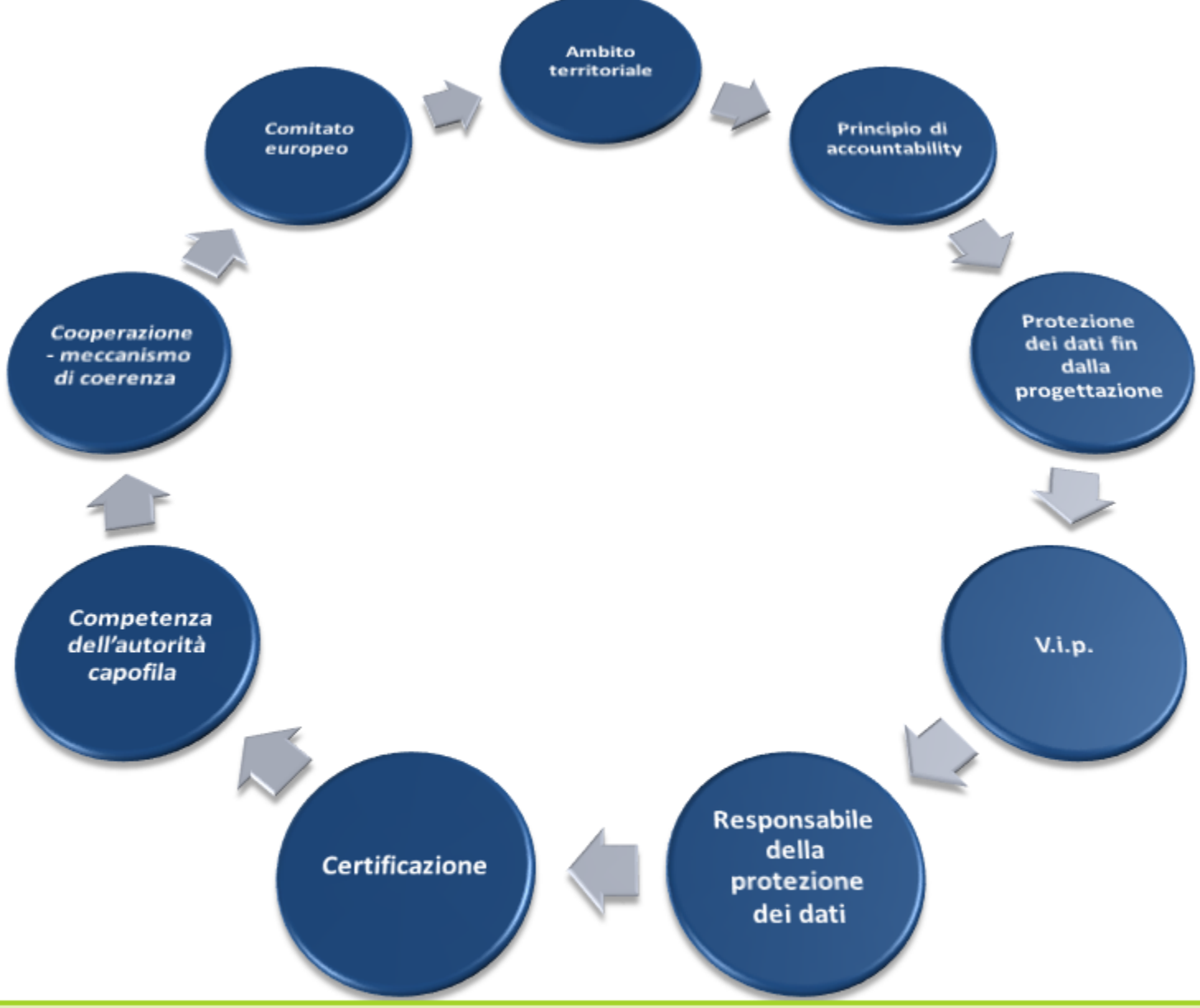
2

L’impatto del regolamento


La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività
La rapidità dell'evoluzione tecnologica comporta nuove sfide per la protezione dei dati personali.
È opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche
Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno


Principi generali
Presupposti di liceità del trattamento
Trattamento dati sensibili
Trasparenza
Autorità di controllo
Poteri
Reclami
Sanzioni amministrative
Responsabilità civile

Continuità


Ambito territoriale
Principio di accountability
Protezione dei dati fin dalla progettazione
V.i.p.
Responsabile della protezione dei dati
Certificazione
Competenza dell'autorità capofila
Cooperazione - meccanismo di coerenza
Comitato europeo

Novità


Trattati in modo lecito, corretto e trasparente nei confronti dell'interessato
(«liceità, correttezza e trasparenza»)
Raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità
(«limitazione della finalità»)
Adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati
(«minimizzazione dei dati»)
Esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati
(«esattezza»)
Conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati
(«limitazione della conservazione»)
Trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali
(«integrità e riservatezza»)
Accountability

Principi

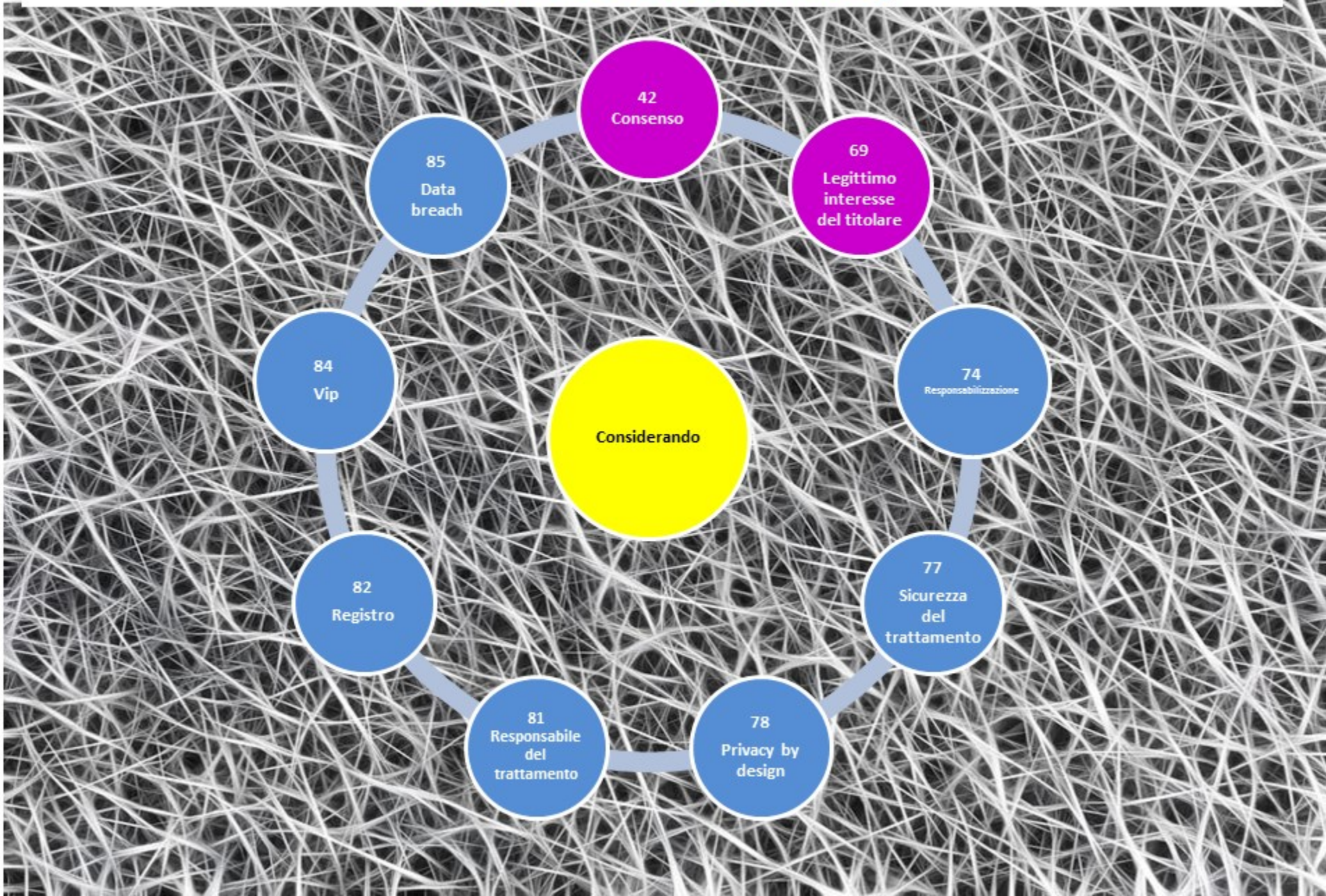
Accountability voce del verbo dimostrare

Il titolare del trattamento è:

competente per il rispetto dei principi applicabili al trattamento di dati personali

in grado di comprovarlo («responsabilizzazione»)

La trama dell'accountability



Sicurezza del trattamento - considerando 77 (art. 32)

Gli orientamenti per la messa in atto di opportune misure e per DIMOSTRARE la conformità da parte del titolare o del responsabile del trattamento in particolare per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità, e l'individuazione di migliori prassi per attenuare il rischio, potrebbero essere forniti mediante:

CODICI DI CONDOTTA

CERTIFICAZIONI

LINEE GUIDA DEL COMITATO

INDICAZIONI DEL RPD

Privacy by design e by default - Considerando 78 (art. 25)

La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento.

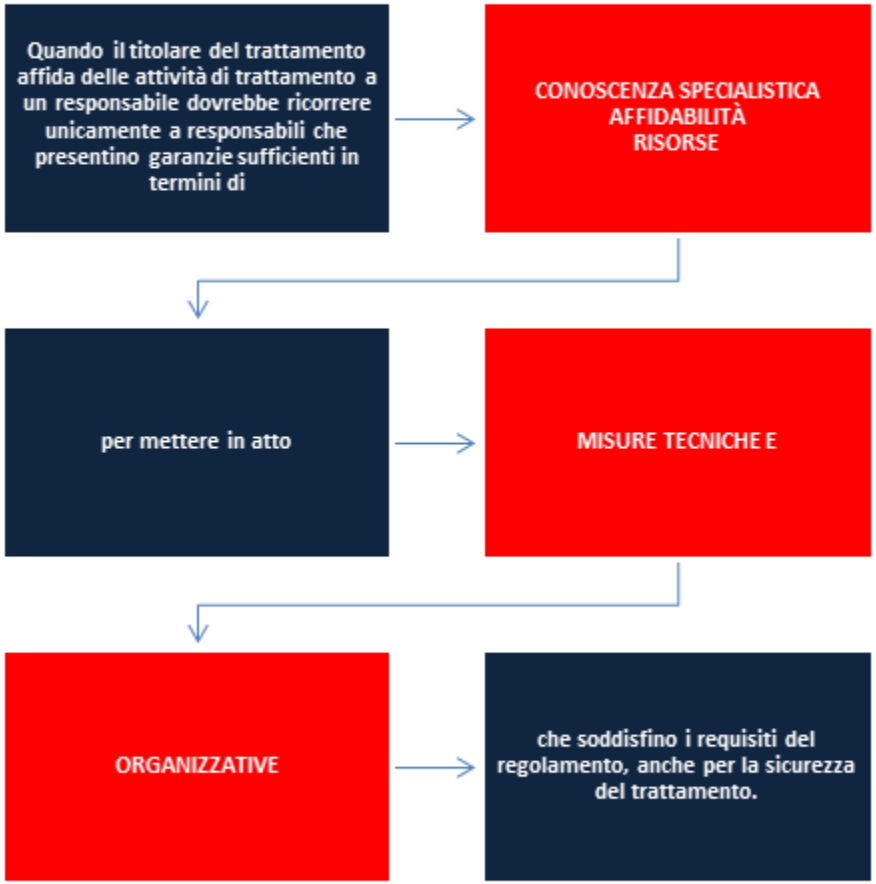
Al fine di poter DIMOSTRARE la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default.

Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza.

In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati.

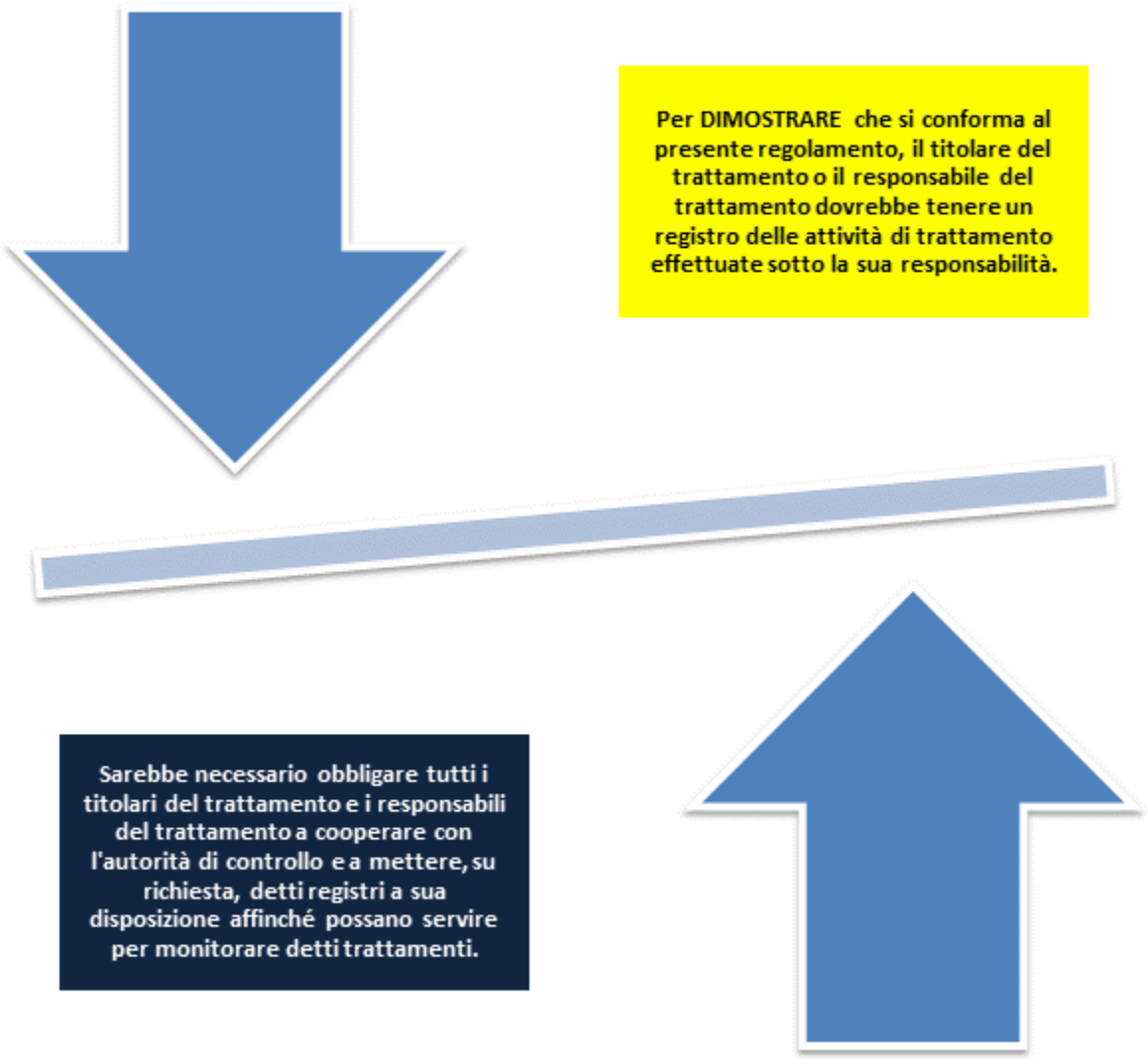
I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici.

Responsabile del trattamento - Considerando 81 (art. 28)



L'applicazione da parte del responsabile del trattamento di un codice di condotta approvato o di un meccanismo di certificazione approvato può essere utilizzata come elemento per DIMOSTRARE il rispetto degli obblighi da parte del titolare del trattamento.

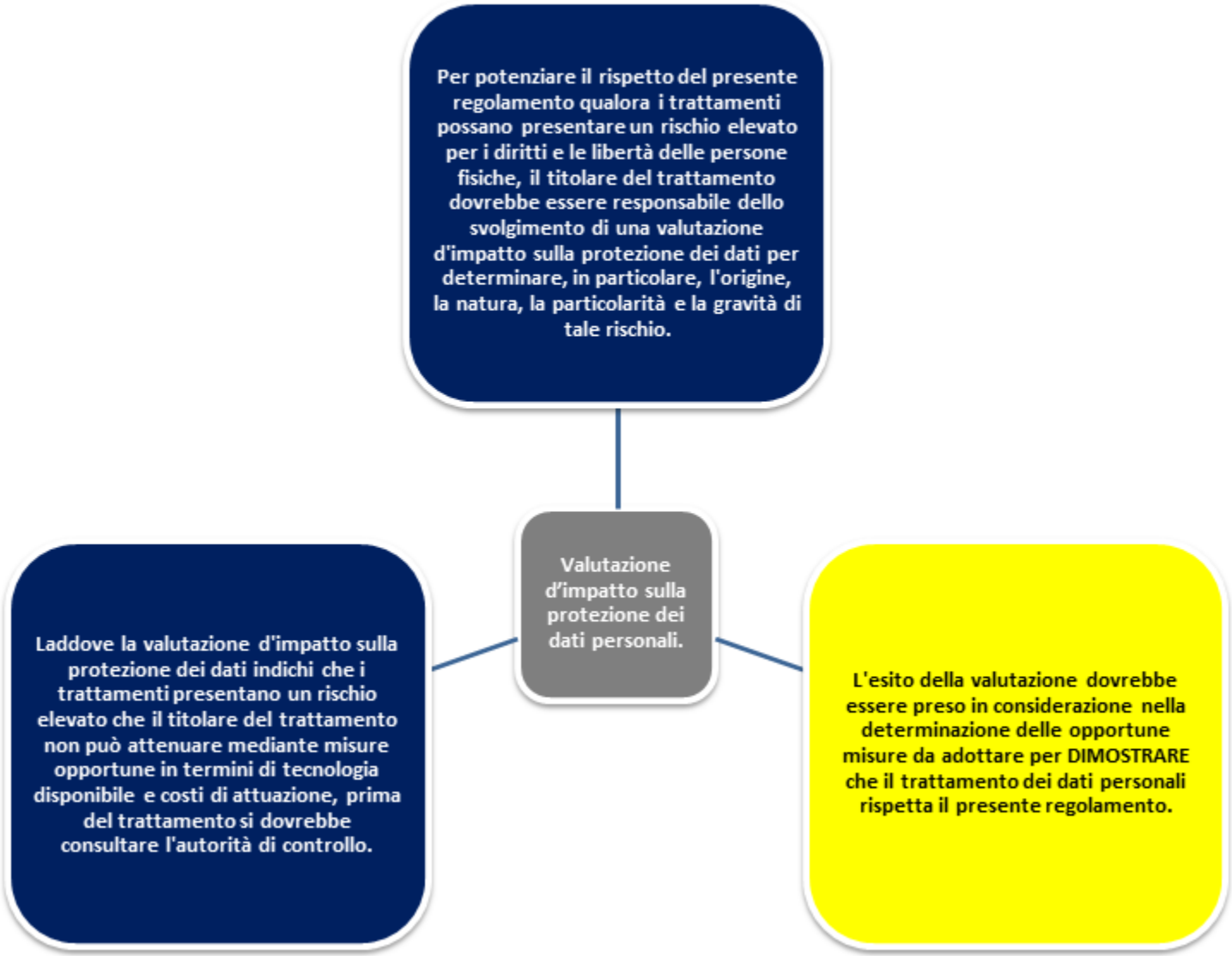
Registro delle attività di trattamento - Considerando 82 (art. 30)



Per DIMOSTRARE che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità.

Sarebbe necessario obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per monitorare detti trattamenti.

Valutazione di impatto privacy considerando 78 (art. 25)

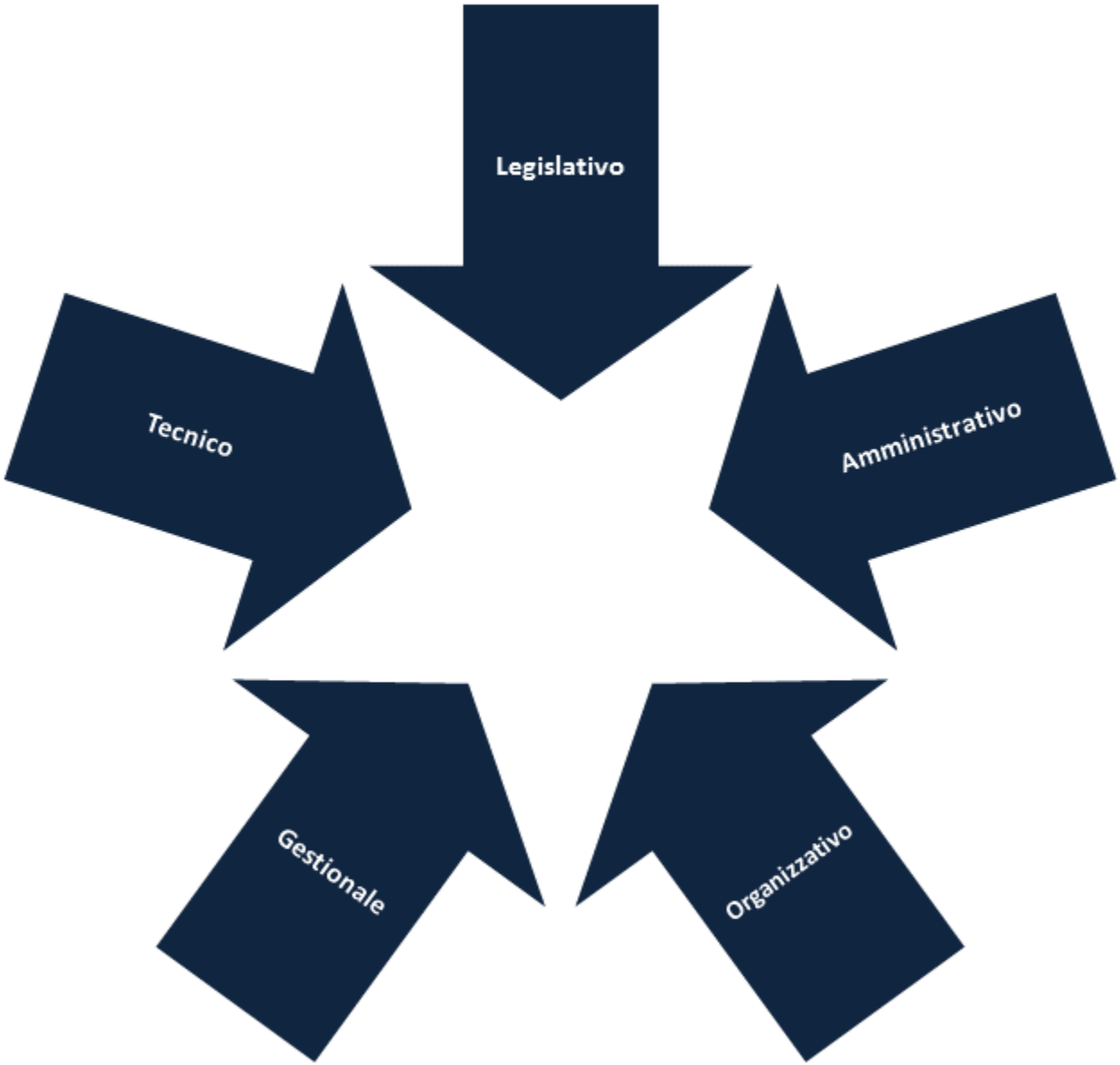


Data breach - considerando 85 (art. 33)

Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di DIMOSTRARE che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

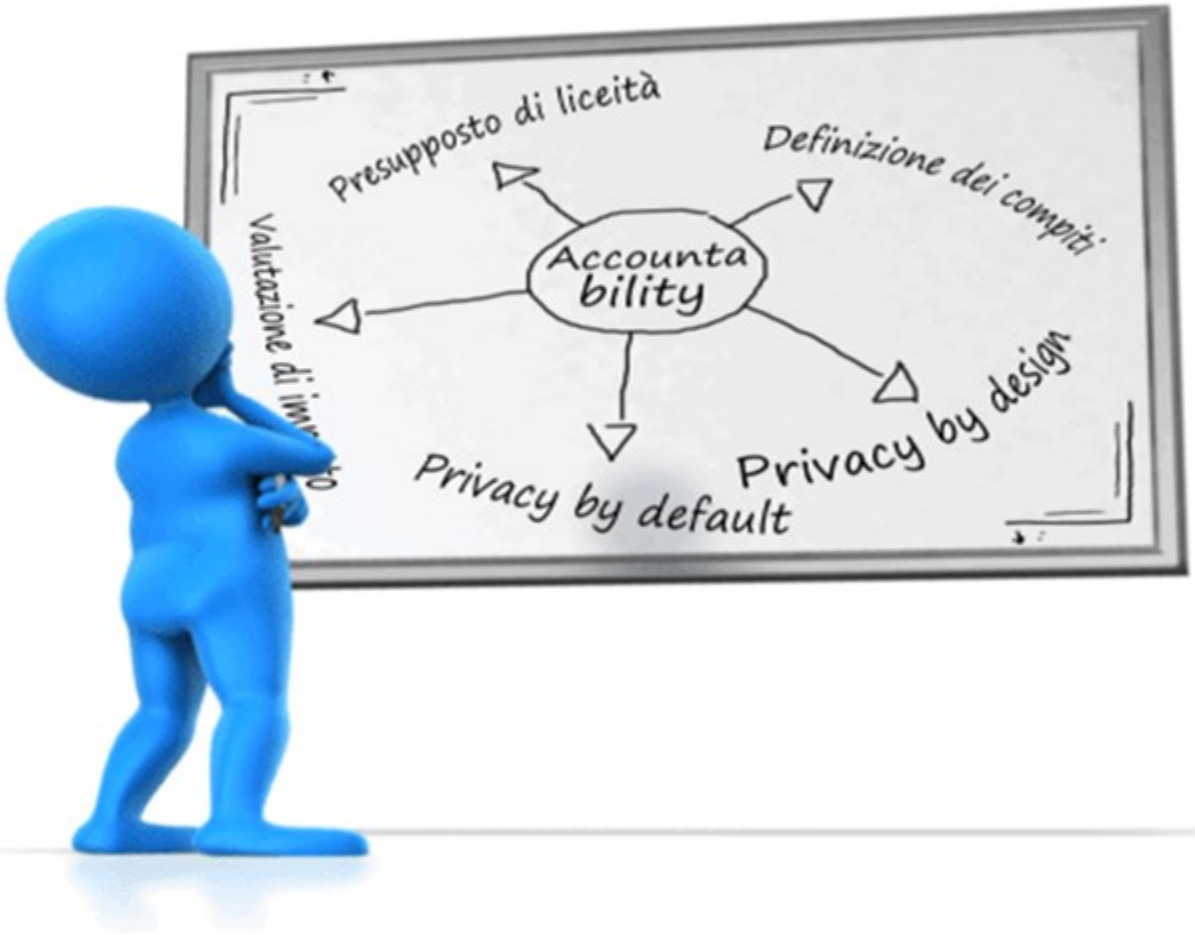

Legislativo
Tecnico
Amministrativo
Gestionale
Organizzativo

Vision

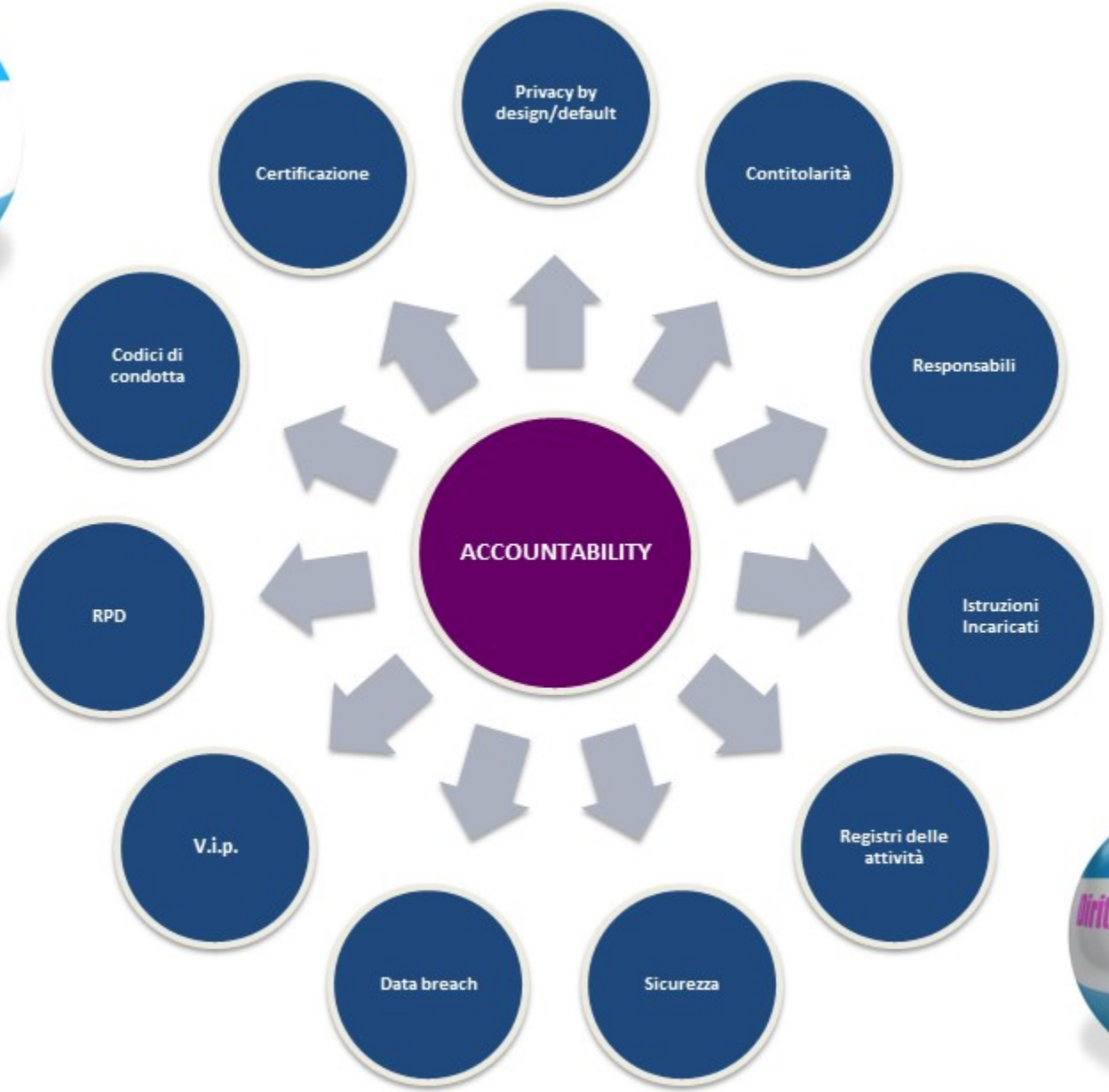
Non considerare solo la gratificazione immediata collegata all'innovazione…

…ma anche le conseguenze future (non sempre immediatamente percepibili)

Necessità di un approccio sistemico



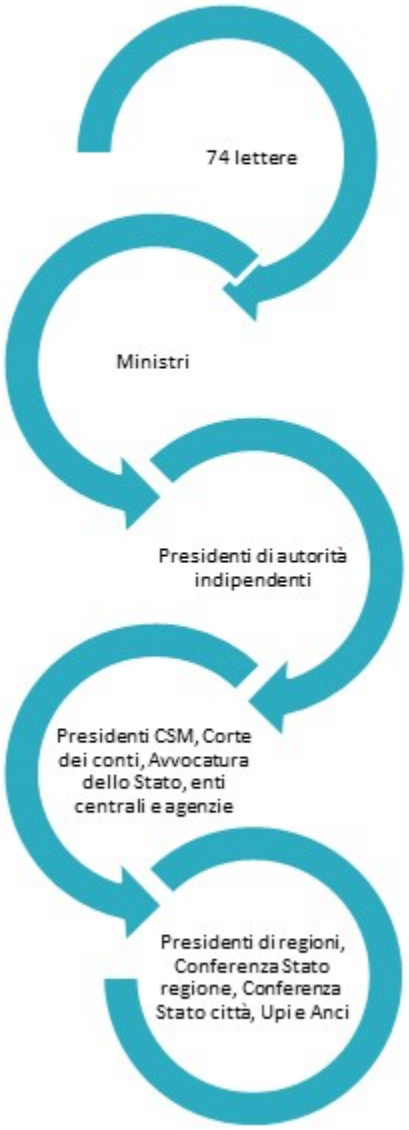
L'importanza di un metodo




Il supporto del Garante per la PA
3

Iniziativa del 24 maggio

"Il Regolamento n. 2016/679, costituisce la vera architrave del nuovo sistema di regole in materia di protezione dei dati personali e si applicherà esattamente tra 365 giorni, a partire dal 25 maggio 2018, in tutti i Paesi UE".



Ambito e limiti dei cc.dd. «margini di flessibilità»
Considerando 8, 9, 10 e 11

Ove il regolamento preveda specificazioni o limitazioni delle sue norme ad opera del diritto degli Stati membri, gli Stati membri possono, nella misura necessaria per la coerenza e per rendere le disposizioni nazionali comprensibili alle persone cui si applicano, integrare elementi del regolamento nel proprio diritto nazionale

Sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche

SI

Il regolamento prevede un margine di manovra degli Stati membri per precisarne le norme, con riguardo al trattamento dei «dati sensibili», per quanto riguarda il trattamento per l'adempimento di un obbligo legale e per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. In tal senso, il regolamento non esclude che il diritto degli Stati membri stabilisca con maggiore precisione le condizioni alle quali il trattamento è lecito.

Un'efficace protezione dei dati personali in tutta l'Unione presuppone il rafforzamento e la disciplina dettagliata dei diritti degli interessati e degli obblighi di coloro che effettuano e determinano il trattamento dei dati personali, nonché poteri equivalenti per controllare e assicurare il rispetto delle norme di protezione dei dati personali e sanzioni equivalenti per le violazioni negli Stati membri.

NO

DELEGA AL GOVERNO

Nell'ambito del disegno di legge per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea (Legge di delegazione europea 2016-2017) è stata prevista la delega al Governo per dare attuazione alla Direttiva (UE) 2016/680 (art. 11) e adeguare la normativa nazionale alle disposizioni del RGPD (art. 13), fissando i seguenti principi e criteri direttivi:

abrogare espressamente le disposizioni del Codice in materia di trattamento dei dati personali, decreto legislativo 30 giugno 2003, n. 196 (d'ora in poi Codice), incompatibili con le disposizioni contenute nel RGPD;

modificare il Codice limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel RGPD e coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni del RGPD;

prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali nell'ambito e per le finalità previsti dal RGPD;

adeguare il sistema sanzionatorio, penale e amministrativo, vigente alle disposizioni del RGPD, con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità delle violazioni commesse.

Le norme relative all'adeguamento della disciplina al RGPD dovranno essere adottate entro sei mesi dall'entrata in vigore della legge di delegazione.


Priorità!
*RPD
*Registro
*Data breach

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
A TUTELA DI UN DIRITTO FONDAMENTALE

BANCA D'ITALIA
EUROSISTEMA

IL NUOVO REGOLAMENTO UE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

SVILUPPI E IMPATTI PER I SOGGETTI PUBBLICI

Il **Garante** incontra la pubblica amministrazione

Roma

7 novembre 2017

Centro Carlo Azeglio Ciampi per l'educazione monetaria e finanziaria
Banca d'Italia - via Nazionale, 190

ore 9,00-17,30

9:00 - Indirizzo di saluto dell'Autorità ospitante - *dott. Luigi Federico Signorini, Vice Direttore Generale e membro del Direttorio della Banca d'Italia*

9:15 - Il Garante per la protezione dei dati personali nel nuovo sistema di regole europee - *Augusta Iannini, Vice Presidente del Garante per la protezione dei dati personali*

9:45 - Dati personali e pubblica amministrazione. Il principio di responsabilizzazione e l'interazione con l'Autorità - *Francesco Modafferi, Dirigente del Dipartimento libertà pubbliche e sanità*

10.30 - Come cambiano i principi e i diritti degli interessati - *Luigi Montuori, Dirigente del Dipartimento relazioni internazionali*

11:15 - *Coffee break*

11:45 - Organizzazione privacy, ruoli e adempimenti - *Claudio Filippi, Dirigente del Dipartimento attività ispettive, sanzioni*

12:30 - Il Responsabile della Protezione dei dati (RPD) in ambito pubblico – *Irene Faganello, Dipartimento libertà pubbliche e sanità*

13:15 - Pausa

14:15 - Il Registro delle attività di trattamento - *Silvia Melchionna, Dipartimento libertà pubbliche e sanità*

15:00 - "Data protection by default and by design", valutazione di impatto e consultazione preventiva - *Miriam Viggiano, Dipartimento libertà pubbliche e sanità*

15:45 - Sicurezza, minimizzazione dei rischi e data breach - *Cosimo Comella, Dirigente del Dipartimento Tecnologie digitali e sicurezza informatica*

16:30 - *Risposte ai quesiti*

17:30 - *Chiusura dei lavori*

PER ULTERIORI INFORMAZIONI: www.garanteprivacy.it/regolamentoue

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
A TUTELA DI UN DIRITTO FONDAMENTALE

LOMBARDIA INFORMATICA

Regione Lombardia

Il **Garante** incontra la pubblica amministrazione

IL NUOVO REGOLAMENTO UE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

SVILUPPI E IMPATTI PER I SOGGETTI PUBBLICI

Milano, lunedì **4 dicembre 2017**, ore **9:00 - 17:30**

Palazzo Lombardia
Piazza Città di Lombardia, 1
Auditorium Testori

PROGRAMMA

8:00	Registrazione dei partecipanti
9:00	Saluti istituzionali Presidente, Roberto Maroni
9:15	Introduce il Privacy Officer di Regione Lombardia: **Maria Pia Redaelli**, Direttore Sistema dei Controlli Prevenzione della Corruzione Trasparenza e Privacy Officer **Il Garante per la protezione dei dati personali nel nuovo sistema di regole europee** **Giovanna Bianchi Clerici**, Garante per la protezione dei dati personali
9:45	**Dati personali e pubblica amministrazione. Il principio di responsabilizzazione e l'interazione con l'Autorità** **Francesco Modafferi**, Dirigente Dipartimento libertà pubbliche e sanità
10:30	**Come cambiano i principi e i diritti degli interessati** **Antonio Caselli**, Unità documentazione internazionale e revisione quadro normativo UE
11:15	Pausa
11:45	**Organizzazione *privacy*, ruoli e adempimenti** **Claudio Filippi**, Dirigente Dipartimento attività ispettive, sanzioni
12:30	**Il Responsabile della Protezione dei dati (RPD) in ambito pubblico** **Anna Carla Meloni**, Dipartimento libertà pubbliche e sanità
13:15	Sospensione dei lavori e pausa pranzo
14:15	Ripresa dei lavori. Introduce: **Giorgio Calelli**, Presidente di Lombardia informatica S.p.a. **Il Registro delle attività di trattamento** **Miriam Viggiano**, Dipartimento libertà pubbliche e sanità
15:00	***"Data protection by default and by design"* valutazione di impatto e consultazione preventiva** **Irene Faganello**, Dipartimento libertà pubbliche e sanità
15:45	**Sicurezza, minimizzazione dei rischi e data breach** **Cosimo Comella**, Dirigente Dipartimento Tecnologie digitali e sicurezza informatica
16:30	**Risposte ai quesiti dei partecipanti da parte dell'Autorità Garante per la protezione dei dati**
17:30	Chiusura dei lavori

In videoconferenza:

Palazzo Lombardia
Ingresso N4

Sala Marco Biagi
Sala Solesin
Sala 4
Sala Pari Opportunità

Lombardia Informatica
Auditorium
Via Taramelli, 26

www.regione.lombardia.it

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

A TUTELA DI UN DIRITTO FONDAMENTALE

REGIONE PUGLIA

anci

CITTÀ METROPOLITANA DI BARI

COMUNE DI BARI

IL NUOVO REGOLAMENTO UE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

SVILUPPI E IMPATTI PER I SOGGETTI PUBBLICI

Il **Garante** incontra

la pubblica amministrazione

Bari

15 gennaio 2018

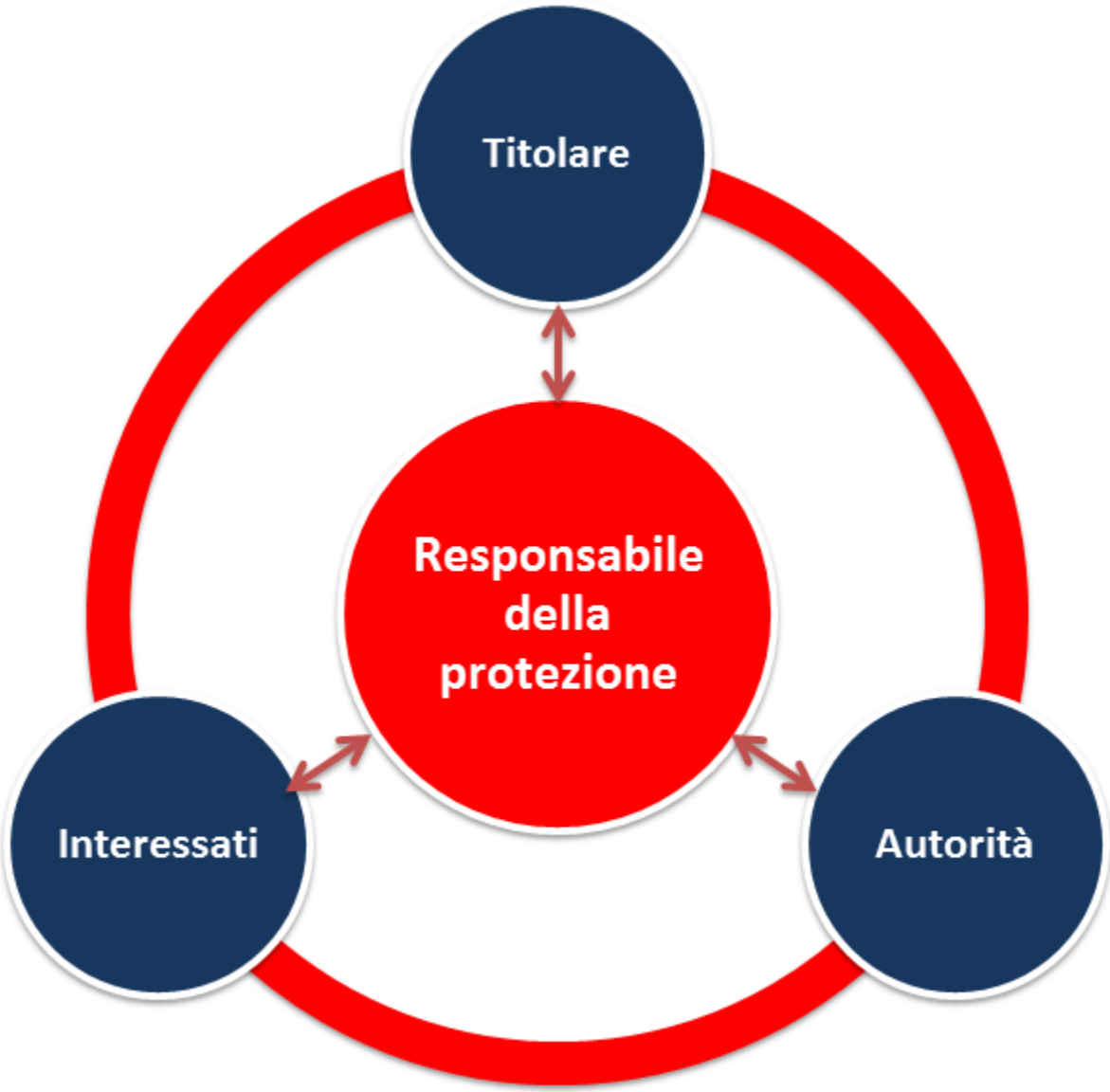
Teatro Petruzzelli

Corso Cavour, 12

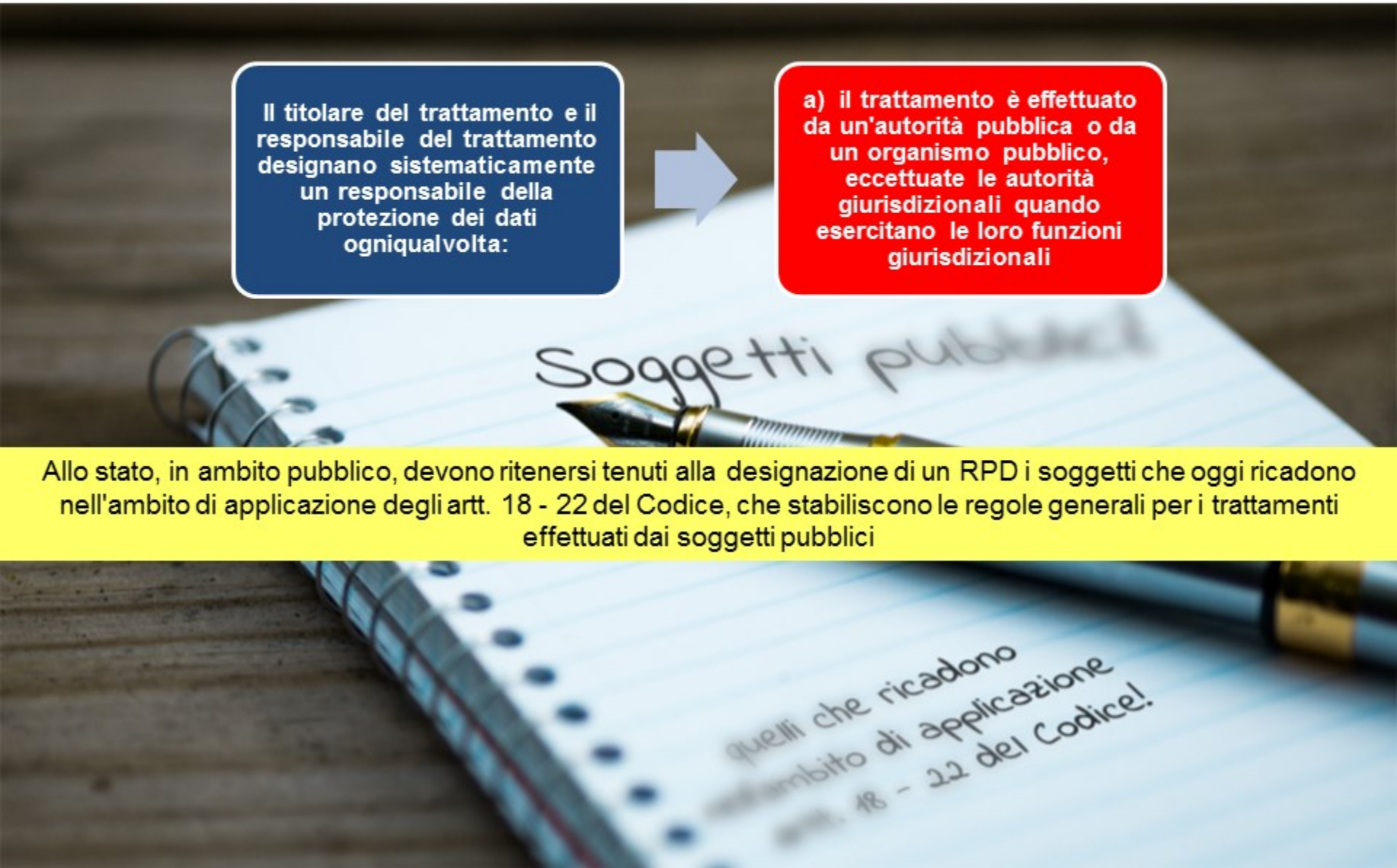
Le indicazioni del Garante

Sul responsabile della protezione dei dati

Il ruolo chiave



Quali sono i soggetti tenuti alla designazione del RPD, ai sensi dell'art. 37, par. 1, lett. a), del RGPD?



Allo stato, in ambito pubblico, devono ritenersi tenuti alla designazione di un RPD i soggetti che oggi ricadono nell'ambito di applicazione degli artt. 18 - 22 del Codice, che stabiliscono le regole generali per i trattamenti effettuati dai soggetti pubblici

Nel caso in cui il RPD sia un dipendente dell'autorità pubblica o dell'organismo pubblico, quale qualifica deve avere?

Nel caso in cui si opti per un RPD interno, sarebbe in linea di massima preferibile che, ove la struttura organizzativa lo consenta e tenendo conto della complessità dei trattamenti, la designazione sia conferita a un **DIRIGENTE OVVERO A UN FUNZIONARIO DI ALTA PROFESSIONALITÀ**, che possa svolgere le proprie funzioni in autonomia e indipendenza, nonché in collaborazione diretta con il vertice dell'organizzazione

Quali certificazioni risultano idonee a legittimare il RPD nell'esercizio delle sue funzioni, ai sensi degli artt. 42 e 43 del RGPD?

Si sono diffusi schemi proprietari di certificazione volontaria delle competenze professionali effettuate da appositi enti certificatori. Esse, pur rappresentando, al pari di altri titoli, un valido strumento ai fini della verifica del possesso di un livello minimo di conoscenza della disciplina, **non equivalgono, di per sé, a una "abilitazione" allo svolgimento del ruolo del RPD né, allo stato, sono idonee a sostituire il giudizio rimesso alle PP.AA**. nella valutazione dei requisiti necessari al RPD per svolgere i compiti previsti dall'art. 39 del RGPD

Con quale atto formale deve essere designato il RPD?

Nel caso in cui la scelta del RPD ricada su una professionalità interna all'ente, occorre formalizzare un apposito atto di designazione a "Responsabile per la protezione dei dati". In caso, invece, di ricorso a soggetti esterni all'ente, la designazione costituirà parte integrante dell'apposito contratto di servizi

La designazione di un RPD interno all'autorità pubblica o all'organismo pubblico richiede necessariamente anche la costituzione di un apposito ufficio?

In relazione alla complessità (amministrativa e tecnologica) dei trattamenti e dell'organizzazione, occorrerà valutare attentamente se una sola persona possa essere sufficiente a svolgere il complesso dei compiti affidati al RPD.
All'esito di questa analisi si potrà valutare l'opportunità/necessità di istituire un apposito ufficio al quale destinare le risorse necessarie allo svolgimento dei compiti stabiliti. Ove sia costituito un ufficio, è necessario che venga sempre individuata la persona fisica che riveste il ruolo di RPD

È ammissibile che uno stesso titolare/responsabile del trattamento abbia più di un RPD?

L'unicità della figura del RPD è una condizione necessaria per evitare il rischio di sovrapposizioni o incertezze sulle responsabilità, sia con riferimento all'ambito interno all'ente, sia con riferimento a quello esterno, e pertanto occorre che questa sia sempre assicurata.
Nulla osta, invece, all'individuazione di più figure di supporto, con riferimento a settori o ambiti territoriali diversi, anche dislocate presso diverse articolazioni organizzative dell'amministrazione, che facciano però riferimento a un unico soggetto responsabile

Quali sono gli ulteriori compiti e funzioni che possono essere assegnati a un RPD?

A seconda della natura dei trattamenti e delle attività e dimensioni della struttura del titolare o del responsabile, le eventuali **ulteriori incombenze attribuite al RPD non dovrebbero sottrarre allo stesso il tempo necessario per adempiere alle relative responsabilità**.
In linea di principio, è quindi ragionevole che **negli enti pubblici di grandi dimensioni** non vengano assegnate al RPD ulteriori responsabilità (si pensi, ad esempio, alle amministrazioni centrali, alle agenzie, agli istituti previdenziali, nonché alle regioni e alle asl).
Rispetto all'assenza di conflitto di interessi, occorre inoltre valutare se le eventuali ulteriori funzioni assegnate non comportino la definizione di finalità e modalità del trattamento dei dati. In ambito pubblico, oltre ai ruoli di vertice, possono sussistere situazioni di conflitto di interesse rispetto a figure quali, ad esempio, il responsabile dei Sistemi informativi (chiamato ad individuare le misure di sicurezza necessarie), ovvero quello dell'Ufficio di statistica (deputato a definire le caratteristiche e le metodologie del trattamento dei dati personali utilizzati a fini statistici).

Domande?