

Il Regolamento europeo UE n.
2016/679

L'applicazione alle istituzioni
scolastiche

Benvenuto.....

Il Regolamento Europeo privacy n. 2016/679
Prevede un'unica serie di norme direttamente
applicabili in tutti i Paesi dell'Unione

- Decreti legislativi attuativi dell'art. 13 della legge
- 163/2013

-Provvedimenti del Garante previsti dai
commi da 1021 a 1024 della l. 205/2017



La 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:

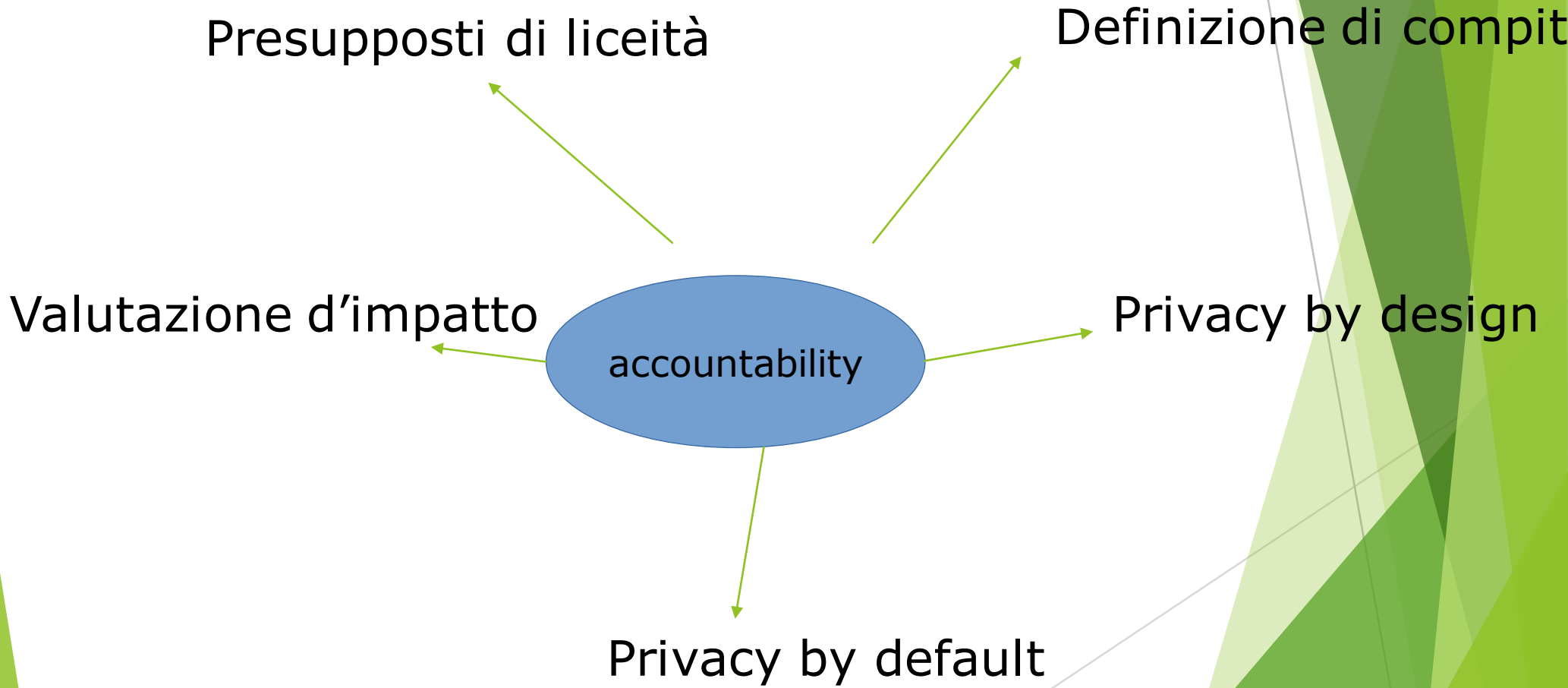
ABROGARE espressamente le disposizioni del Codice in materia di trattamento dei dati personali, decreto legislativo 30 giugno 2003, n. 196 (d'ora in poi Codice), incompatibili con le disposizioni contenute nel RGPD;

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.

Presupposto: un approccio sistemico



Ambito oggettivo di applicazione del Regolamento

Tipo di trattamento	RGPD
Trattamento completamente automatizzato	Si
Trattamento parzialmente automatizzato	SI
Trattamento non automatizzato di dati personali contenuti in un archivio	SI
Trattamenti effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico	No
Trattamenti effettuati dagli Stati membri nell'esercizio dell'attività applicative del TUE, tit V capo 2	No
Trattamenti effettuati dalle autorità competenti a fini giudiziari	NO

es. genitore che fa foto durante la recita;
docente che fa foto ricordo dei suoi alunni; studenti che scattano foto a coetanei

Le priorità da realizzare entro il 25 maggio 2018

Il Garante, già dal maggio 2017, ha individuato 3 priorità per le PPAA:

Il Responsabile Protezione Dati

Il Registro delle attività di trattamento

Data breach

Accountability.....principio di responsabilizzazione

Il Regolamento è in continuità con i principi già declinati nel Codice

Sono stati i Garanti europei a chiedere al legislatore europeo di inserire il principio di accountability

L'accountability integra una presunzione legale di conformità

Il nuovo regolamento UE in materia di protezione dei dati personali
Sviluppi e impatti per i soggetti pubblici

Dalla forma alla sostanza

1. Titolari del trattamento
2. Competente per il rispetto dei principi applicabili al trattamento di dati personali
3. In grado di comprovare («responsabilizzazione»)

Dimostrare provare una verità con un ragionamento logico con prove di fatto
Concetto chiave!

Dati personali e pubblica amministrazione
Il principio di responsabilizzazione e l'interazione con l'Autorità

Francesco Modafferi
Ufficiale del Dipartimento
Informatica pubblica che si occupa

Accountability

Essere accountable è un criterio di attenuazione della responsabilità

Approccio sistemico all'interno del titolare del trattamento.
Occorre legare i vari pezzi

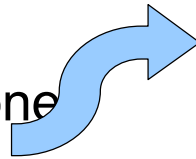
l'importanza di acquisire un metodo su come fare – Imparare a fare

L'accountability è una trama all'interno del Regolamento

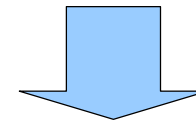
L'accountability e l'approccio basato sul rischio - il considerando 74

Le variabili:

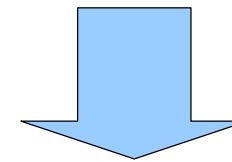
- la natura dell'ambito di applicazione
- del contesto
- le finalità del trattamento
- i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche



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 in conformità al Regolamento

L'accountability e l'approccio basato sul rischio - il considerando 74

Nell'uso della tecnologia non considerare solo la gratificazione immediatamente collegata all'innovazione

...ma anche le conseguenze future (che non sono sempre percepibili)

Dato personale «la sola evidenziazione visiva dello stato di minorità del soggetto costituisce condotta colpevole del reato in questione, così come avverrebbe se si mostrasse in un video una particolare preferenza sessuale di un soggetto»³⁸; potrebbe sostenersi, in contrario la non identificabilità del titolare di quei dati attraverso le informazioni diffuse con il video, ma il giudicante pare aver aderito all'opposta tesi che considera sufficiente ad integrare il requisito posto dall'art. 4, comma 1, lett. b), del Codice della privacy, l'identificabilità indiretta, attraverso la correlazione degli elementi diffusi con altre informazioni a disposizione del soggetto raggiunto dalla diffusione dei dati, circostanza questa probabile nel caso di specie, trattandosi di filmato molto popolare, che nel periodo successivo alla sua immissione, era stato visualizzato dagli utenti del sito almeno 5.500 volte ottenendo il primo posto nella classifica dei «video più divertenti» e il ventinovesimo in quella dei «video più scaricati».

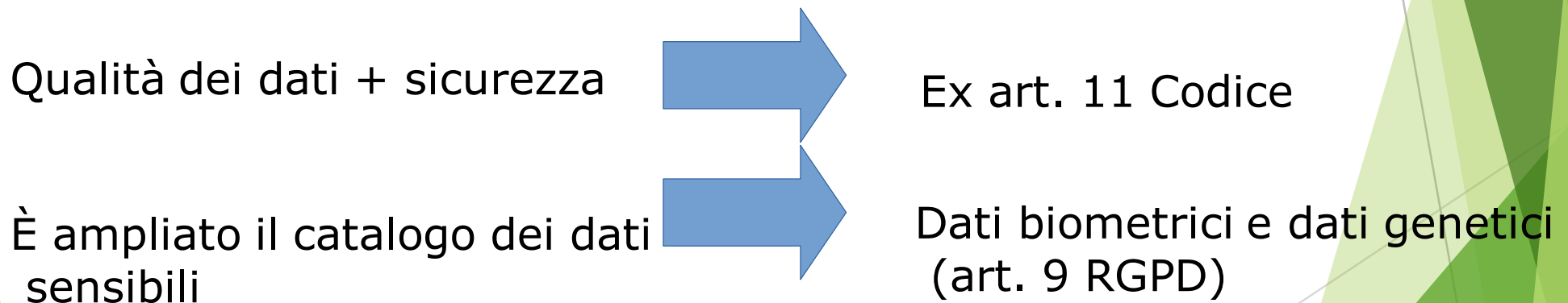
Principi generalissimi (artt. 5 del RGPD)

Principio	Significato
Liceità, correttezza e trasparenza	Dati trattati in modo lecito, corretto e trasparente nei confronti dell'interessato
Limitazione della finalità	Dati raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità oppure comunque a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici
Minimizzazione dei dati	Dati adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati
Esattezza	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
Limitazione della conservazione	Dati 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; i dati personali possono essere conservati per periodi più lunghi se trattati esclusivamente ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici
Integrità e riservatezza	Dati trattati in modo da garantire un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali

Disegno generale in continuità (art. 6)

In linea di principio il consenso non è idoneo fondamento del Trattamento dei dati da parte della PA perché la PA dovrebbe operare sulla base di altri presupposti, disposizioni di legge, interesse pubblico riconosciuto in specifiche disposizioni

Non cambiano i presupposti di liceità del trattamento: consenso, contratto, interesse vitale, obbligo di legge, **interesse pubblico**, interesse legittimo (art. 6)



Gruppo Art. 29 Linee guida sul consenso ai sensi del Regolamento 2016/679 WP259 rev.01

- Il considerando 43 indica chiaramente che è improbabile che le autorità pubbliche possano fare affidamento sul consenso. Ogni volta che il controller è un'autorità pubblica, c'è spesso un evidente squilibrio di potere nella relazione tra il responsabile del trattamento e l'interessato. È anche chiaro nella maggior parte dei casi che l'interessato non avrà alternative realistiche all'accettazione del trattamento da parte dell'Autorità pubblica.
- Il WP29 ritiene che ci siano altre basi legali che sono, in linea di principio, più appropriate per il attività delle autorità pubbliche.

Gruppo Art. 29 Linee guida sul consenso ai sensi del Regolamento 2016/679 WP259 rev.01

- Fermo restando queste considerazioni generali, l'uso del consenso come base legale per i dati l'elaborazione da parte delle autorità pubbliche non è totalmente esclusa dal quadro giuridico del GDPR.

Esempio: Un comune locale sta pianificando lavori di manutenzione stradale che potrebbero disturbare il traffico per lungo tempo.

Il comune offre ai suoi cittadini l'opportunità di iscriversi a una mailing list per ricevere aggiornamenti sullo stato di avanzamento dei lavori e sui ritardi previsti. Il comune chiarisce che non c'è obbligo di partecipazione e chiede il consenso a utilizzare indirizzi e-mail per questo scopo (esclusivo). I cittadini che non perdono alcun servizio di base del comune o l'esercizio di qualsiasi diritto, sono in grado di dare o rifiutare il loro consenso a questo uso dei dati liberamente.

Comunque tutte le informazioni sui lavori stradali saranno disponibili sul sito web del comune

Uniformizzazione in tutta la UE

Questo obiettivo è raggiunto attraverso:

Responsabilizzazione

Diritti degli interessati

Ruolo dell'Autorità di controllo

Europeizzazione di standard e prassi

I diritti degli interessati

Nel nuovo Regolamento europeo ci sono molti elementi di continuità con il Codice, in particolare per la PA

Cambia l'approccio che diviene più proattivo nell'ottica della responsabilizzazione

Rafforzamento e disciplina dettagliata dei diritti dell'interessato

I diritti degli interessati (artt. 12 e 23 RGPD)

Artt. 15-22 RGPD

Il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando idonee misure tecniche e organizzative

Significa che la struttura deve essere in grado di rispondere alle esigenze dell'interessato

La risposta alle richieste dell'interessato deve essere data entro un mese, anche nel caso di diniego.

Non esiste silenzio concludente

Nel caso di richieste infondate o eccessive può essere chiesto un contributo "ragionevole"

l'importanza e il ruolo del registro dei trattamenti

Le deroghe ai diritti

Sono ammesse deroghe agli obblighi e ai diritti se previste dalla normativa nazionale

Art. 23 RGPD

Art. 85 RGPD

Art. 89 RGPD

Il legislatore nazionale deve rispettare l'essenza del diritto alla protezione dei dati

L'informativa (artt. 12, 13 e 14 RGPD)

- ▶ Il regolamento CE interviene sulle modalità per informare il titolare dei dati personali sull'uso di questi ultimi che si fa più stringente (l'informativa deve essere concisa, trasparente, intelligibile e facilmente accessibile)
- ▶ Il titolare deve sempre specificare i dati di contatto del RPD-DPO (Responsabile Privacy (RDP) o Data Protection Officer (DPO),
- ▶ il periodo di conservazione dei dati (i dati personali possono essere conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti e trattati)o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'autorità di controllo
- ▶ Nel caso di dati personali non raccolti direttamente presso l'interessato (*art. 14 del regolamento*), l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione (NON della registrazione) dei dati (a terzi o all'interessato) (diversamente da quanto prevede attualmente l'art. 13, comma 4, del Codice)
- ▶ Se i dati personali possono essere legittimamente comunicati a un altro destinatario, l'interessato dovrebbe esserne informato nel momento in cui il destinatario riceve la prima comunicazione dei dati personali. Il titolare del trattamento, qualora intenda trattare i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, dovrebbe fornire all'interessato, prima di tale ulteriore trattamento, informazioni in merito a tale finalità diversa e altre informazioni necessarie.

Diritto di accesso (art. 15)

Il diritto di accesso comporta il diritto di ricevere una copia dei dati personali oggetto di trattamento

È possibile che il titolare preveda la possibilità di accesso da remoto ai propri dati

Diritto di rettifica (art. 16)

Possono essere rettificati i dati inesatti e possono essere

integrati dati incompleti

Il diritto di cancellazione (diritto all'oblio) (art. 17)

Il diritto all'oblio non si applica ai trattamenti necessari per adempiere ad obblighi di legge, quando si fondano su un interesse pubblico e in ambito sanitario

Diritto di limitazione del trattamento (art. 18)

Si tratta di un diritto più forte del blocco già previsto dal Codice

Si può esercitare



Nel caso di violazione dei presupposti di liceità del trattamento



In attesa della rettifica dei dati o durante la pronuncia del titolare a seguito di opposizione al trattamento

Diritto di limitazione del trattamento (art. 18 GDPR):

è un diritto diverso e più esteso rispetto all'attuale "blocco" del trattamento previsto dall'art. 7, comma 3, lett. a) del D. Lgs. n.196/2003.

Il GDPR prevede, infatti, che tale diritto possa essere esercitato non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati), bensì anche se l'interessato chiede la rettifica dei suoi dati o si oppone al trattamento, in attesa della valutazione di tale opposizione da parte del titolare.

Diritto alla portabilità (art. 20)

Si applica ai trattamenti automatizzati

Sono portabili solo i dati conferiti con il consenso dell'interessato o su base contrattuale.

Non si applica la portabilità ai dati che vengono trattati sulla base dell'interesse pubblico o sull'adempimento di obblighi di legge del titolare o per scopi di archiviazione nel pubblico interesse

Diritto di opposizione (art. 21)

- ▶ L'interessato può opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare al trattamento dei dati che lo riguardano



Ex art. 7 Codice

Il responsabile della protezione dati

Figura già presente nella prassi di altri Stati membri e anche in Italia (settore della grande industria e nella PA Agenzie fiscali, alcuni enti previdenziali, alcune regioni)

Titolare

Nella Governance dei dati è il riferimento per

Personale che tratta dati

Interessati

Autorità di controllo

Il responsabile della protezione dati

Artt- 37-38-39 del RGPD

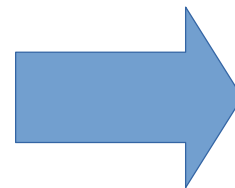
Cons. 97

Linee guida 13 dicembre 2016 Gr. Art. 29

Nell'ambito della PA l'obbligatorietà della figura del RPD è dovuto allo scarsissimo margine di discrezionalità dell'interessato.

Non essendo il consenso un requisito di legittimità del trattamento dei dati, la scelta del legislatore appare pienamente giustificata (anche per la mole di dati trattati dalla PA)

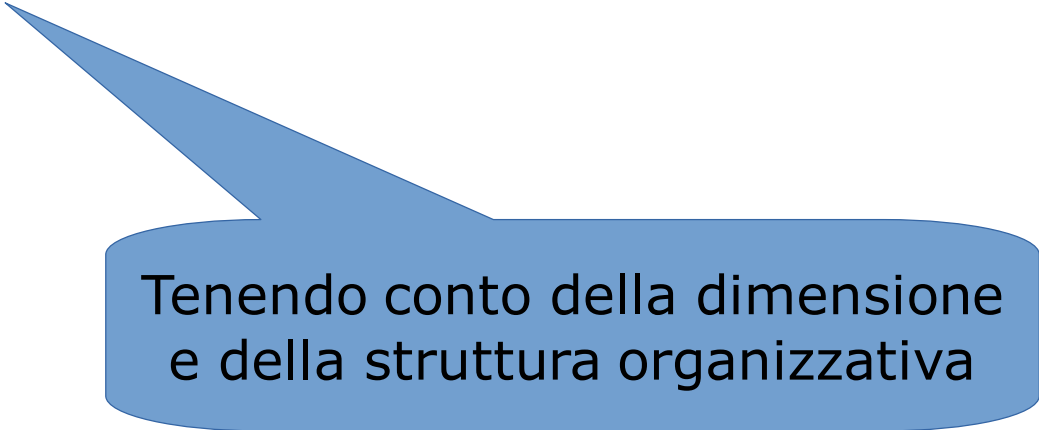
Chi sono le "Autorità pubbliche"
e gli "Organismi pubblici"



Riferimento artt 18-22
del Codice

Designazione per più titolari

Più autorità pubbliche possono designare un Unico RPD



Tenendo conto della dimensione
e della struttura organizzativa

I requisiti che deve possedere il RPD

Determinante la conoscenza della normativa di settore,
dell'organizzazione e dei sistemi
informatici utilizzati



Può essere un soggetto interno



Dipendente del titolare



Può essere un soggetto esterno



Contratto di servizio

27

Il Responsabile protezione dati

Risorse necessarie allo svolgimento della funzione

Non può rivestire ruoli che determinano le finalità e modalità di trattamento



Compiti - 1

(art. 39)

Informazione, consulenza e indirizzo al titolare e ai dipendenti

Sorveglianza sull'osservanza della normativa sulla protezione dei dati (Regolamento, norme nazionali e politiche adottate dal titolare)

- Raccolta di informazioni per individuare i trattamenti svolti
- Analisi e verifica della conformità dei trattamenti

Formazione e sensibilizzazione dei dipendenti

Compiti - 2

(art. 39)

Ruolo nella valutazione d'impatto (DPIA)

- Consultazione da parte del titolare: necessità di effettuare o meno DPIA, metodologia, garanzie da applicare, valutazione anche sulla conformità alla normativa (art. 35, par. 2)
- Parere sulla DPIA e sorveglianza sul suo svolgimento (39, par.1, lett.c)

Approccio basato sul rischio

- Definizione di un ordine di priorità



Compiti - 3

(art. 39)

Coopera con il Garante per la protezione dei dati personali

Funge da referente del Garante per la protezione dei dati

- Per la procedura di consultazione preventiva (art. 36)
- *Data breach*, anche nei confronti degli interessati (artt. 33-34)
- Per effettuare consultazioni relativamente a qualunque altra questione sul trattamento dei dati

Altri compiti

(es. tenuta del registro delle attività del trattamento)

La responsabilità del RPD

La responsabilità di garantire e dimostrare l'osservanza della normativa ricade sul titolare/responsabile

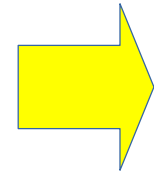
Il RPD deve manifestare il proprio dissenso sulle decisioni che non ritiene corrette

Obbligo di riservatezza sulle attività svolte

I soggetti: Il titolare del trattamento

Chi è il titolare...

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 (art. 4, § 7);



Istituzione scolastica

La disciplina della **contitolarità del trattamento** impone ai titolari di definire specificamente il rispettivo ambito di responsabilità e i compiti **con particolare riguardo all'esercizio dei diritti degli interessati**, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari che operano congiuntamente

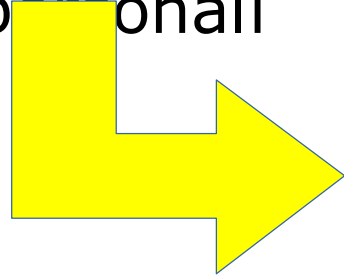
I contitolari determinano con **accordo interno**, le rispettive responsabilità in merito all'osservanza degli obblighi, all'esercizio dei diritti dell'interessato e all'informativa

L'accordo interno (nel contenuto essenziale) è messo a disposizione degli interessati



La responsabilizzazione del titolare

Il principio di responsabilizzazione attribuisce direttamente ai titolari del trattamento il compito di assicurare ed essere in grado di comprovare il rispetto dei principi applicabili al trattamento dei dati personali



I PRINCIPI POSTI ALLA BASE DELLA RESPONSABILIZZAZIONE

I dati devono essere:

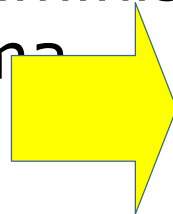
- trattati secondo "liceità, correttezza e trasparenza";
- raccolti per "finalità determinate, esplicite e legittime";
- adeguati, pertinenti e limitati rispetto alle finalità;
- esatti
- limitati nella conservazione;
- trattati garantendo sicurezza e integrità.

Contitolari del trattamento

- ▶ La figura del contitolare del trattamento è prevista all'art. 26 'Contitolari del trattamento' GDPR, il quale articolo precisa che i contitolari possono anche essere più di due, che devono determinare congiuntamente le finalità e mezzi del trattamento. Si ipotizza quindi la necessità della sussistenza di una codecisione in merito alle finalità (perché) e a i mezzi (come) di un determinato trattamento.
- ▶ Tramite accordo interno i contitolari hanno l'obbligo di determinare, in modo trasparente, le rispettive responsabilità e compiti sull'osservanza degli obblighi derivanti dal GDPR con particolare riferimento ai diritti dell'interessato e gli obblighi di fornire le informazioni previste al momento della raccolta (Art.13 – Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato; Art.14 – Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato).

Il responsabile

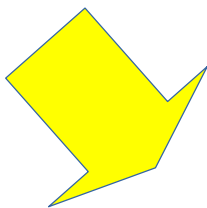
Trattamento di dati di cui l'amministrazione non si occupa direttamente ma che affida all'esterno



Il responsabile

la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (artt. 4, § 8 - 28);

Attività di outsourcing trova qui la propria legittimazione



Il responsabile **può nominare sub-responsabili** per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e «responsabile primario».

ATTENZIONE

Il «responsabile primario» **risponde dinanzi al titolare dell'inadempimento del sub-responsabile**, anche ai fini del **risarcimento** di eventuali danni causati dal trattamento.

Le responsabilità del responsabile in outsourcing

UN RESPONSABILE CON TANTE «RESPONSABILITÀ»

ESCLUSIVAMENTE CON UN CONTRATTO (o altro atto giuridico) E' DISCIPLINATA:

- materia e durata del trattamento;
- natura e finalità del trattamento;
- tipo di dati personali e categorie di interessati;
- obblighi e diritti del titolare del trattamento.

IN BASE AL CONTRATTO IL RESPONSABILE SI IMPEGNA A:

- trattare dati soltanto su istruzione documentata del titolare;
- consentire i trattamenti solo a persone autorizzate con impegno alla riservatezza o che abbiano un adeguato obbligo legale di riservatezza;
- adottare tutte le misure di sicurezza (es. cifratura; pseudonimizzazione; recupero da backup);
- rispettare le condizioni per ricorrere a un sub-responsabile del trattamento;
- assistere il titolare per dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- cancellare o restituire tutti i dati e cancellare le copie esistenti;
- mettere a disposizione del titolare le informazioni per dimostrare il rispetto dei suddetti obblighi e consentire le ispezioni.

- ▶ Art. 29 Codice Privacy
- ▶ Responsabile del trattamento
- ▶ 1. Il responsabile è designato dal titolare facoltativamente.
- ▶ 2. Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
- ▶ 3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.
- ▶ 4. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.
- ▶ **4-bis. Fermo restando quanto previsto ai commi 1, 2, 3 e 4, il titolare può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie di cui al comma 2. I titolari stipulano con i predetti responsabili atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento; i predetti atti sono adottati in conformità a schemi tipo predisposti dal Garante (1).**
- ▶ **5. Il responsabile effettua il trattamento attenendosi alle condizioni stabilite ai sensi del comma 4-bis e alle istruzioni impartite dal titolare, il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2, delle proprie istruzioni e di quanto stabilito negli atti di cui al comma 4-bis (2).**

Referenti interni

- Il titolare può mantenere la nomina di “referenti interni” comunque denominati con eventuale integrazione degli atti di nomina precedenti al RGPD

Che fine ha fatto l'incaricato del trattamento?

La figura non è espressamente prevista dal regolamento, ma se ne evince la permanenza da diversi articoli dello stesso

È definito «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo **che non sia** (.....) la persona **autorizzata** al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile (art. 4, § 10);

Sicurezza del trattamento (art 32, § 4)

Il titolare del trattamento e il responsabile del trattamento fanno sì che **chiunque** agisca sotto la loro autorità e **abbia accesso** a dati personali non tratti tali dati **se non è istruito** in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento (art. 29)

Il responsabile del trattamento, o **chiunque** agisca sotto la sua autorità o sotto quella del titolare del trattamento, che **abbia accesso** a dati personali **non può** trattare tali dati **se non è istruito** in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Le sanzioni amministrative

- Registri delle attività di trattamento (art. 30);
- Valutazione di impatto e consultazione preventiva (artt. 35 -36);
- Responsabile della protezione dei dati (artt. 37-39);
- Sicurezza dei dati personali (artt. 32-34)

- es. obbligo comunicazione al Garante - data breach.

SANZIONI

La violazione delle disposizioni riguardanti gli **obblighi del titolare e del responsabile** previsti dagli **articoli da 25 a 39** è soggetta a sanzioni amministrative pecuniarie **fino a € 10 milioni**

(per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore).



Condizioni generali per infliggere sanzioni amministrative pecuniarie (art. 83)

- la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o la finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;
- il carattere doloso o colposo della violazione;
- le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
- **il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;**
- eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
- il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
- le categorie di dati personali interessate dalla violazione;
- **la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;**
- qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;
- l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e
- eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

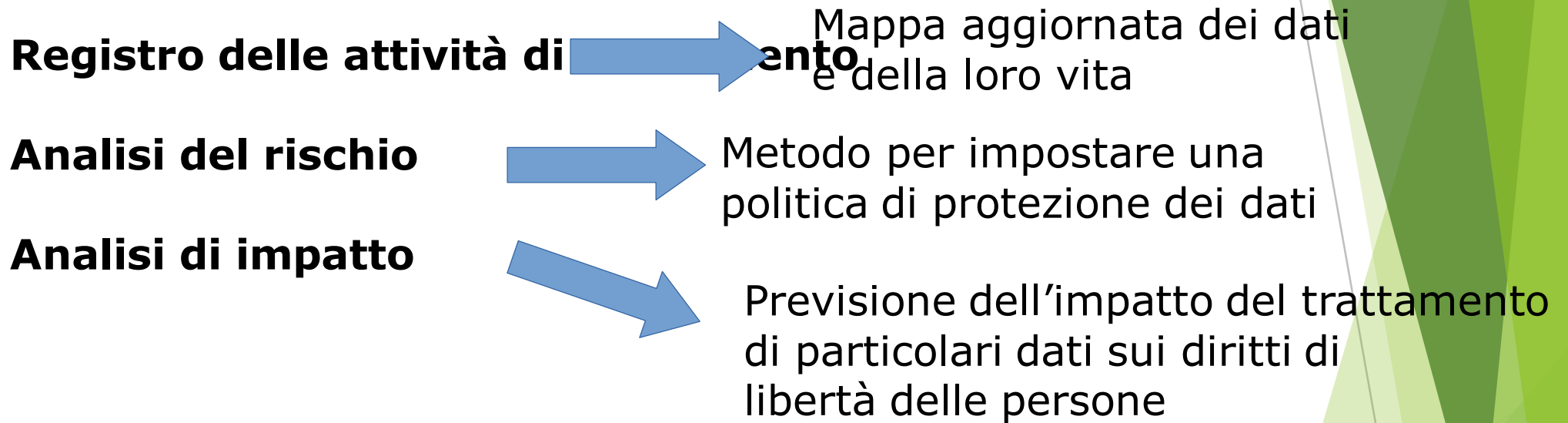
La tutela amministrativa e giudiziaria

L'art. 77 del Regolamento prevede la possibilità per i trattamenti svolti da soggetti pubblici di proporre reclamo al garante

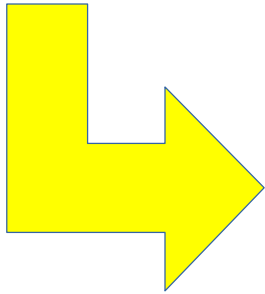
È risarcibile il danno materiale e immateriale

La responsabilità è di tipo solidale tra il titolare e il responsabile

Le tappe fondamentali nella gestione della Privacy



Data protection by design e data protection by default (art. 25)



Trattamenti che presentano rischi elevati

attenzione nella fase di lancio di un servizio o di programmazione di una app o di un software, ossia già nella fase costruttiva.

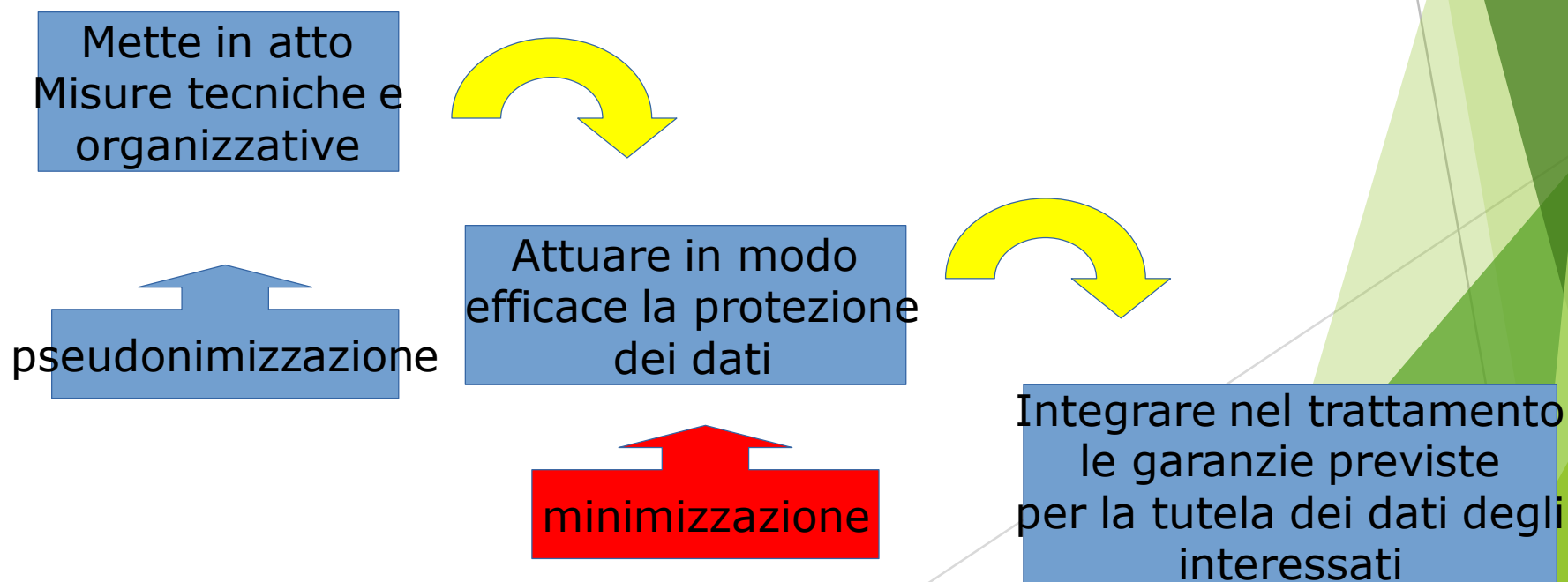
Modalità tecniche e organizzative del titolare del trattamento

Entrambi i principi intendono impartire agli addetti al trattamento dati un'idea di privacy c.d. "tecnologica"; pertanto il Legislatore comunitario vuole sensibilizzare gli Stati ad adottare strumenti volti a progettare sistemi di raccolta dati e software per garantire più semplicemente, grazie all'utilizzo della tecnologia, il pieno rispetto dei principi sanciti nel Regolamento.

Privacy by design (art. 25 1° comma)

Protezione dei dati fin dalla progettazione

Il titolare del trattamento



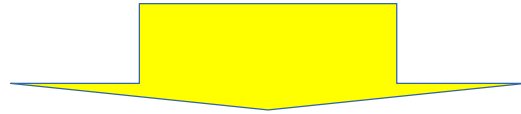
Privacy by design (art. 25 I° comma)

Le variabili:

Lo stato dell'arte e i costi di attuazione

Natura, ambito di applicazione, contesto e finalità del trattamento

Rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone



Considerando 75

I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori;

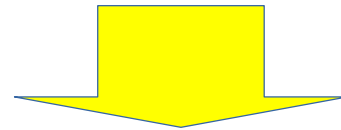
se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.



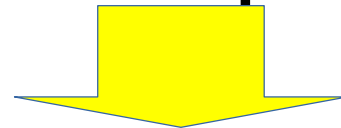
Privacy by default (art. 25 comma 2)

Protezione dati per impostazione predefinita

Il titolare del trattamento mette in atto misure tecniche e organizzative per



**Garantire che siano trattati –
per impostazione predefinita -**



**solo i dati personali
necessari per
ogni specifica finalità
del trattamento**

Obbligo valido per:
Quantità dei dati raccolti;
Portata del trattamento;
Periodo di conservazione;
accessibilità

Per impostazione predefinita non possono essere resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica

La minimizzazione costituisce una misura di riduzione del trattamento by default finalizzata a impostare a priori la massima protezione dei dati attraverso il loro minimo trattamento, sia in fase di raccolta sia in fase di trattamento successivo all'acquisizione dei dati personali, secondo i principi di necessità, pertinenza, adeguatezza e non eccedenza rispetto alle finalità.

Privacy by design e privacy by default

Il titolare del trattamento può utilizzare la certificazione ex art. 42 come elemento per dimostrare la conformità ai requisiti by design e by default

La certificazione non riduce la responsabilità del titolare o del responsabile del trattamento riguardo alla conformità al regolamento e lascia impregiudicati i compiti e i poteri dell'autorità di controllo

art. 35, commi 4-6
Casi di valutazione d'impatto privacy obbligatoria

ELENCHI REDATTI
DAL GARANTE


- l'Autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti per cui la DPIA è **obbligatoria**
- l'Autorità di controllo può redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali **non è richiesta** una DPIA (facoltativo)



entrambi comunicati al
Comitato europeo per la protezione dei dati
adozione del **meccanismo di coerenza** per attività
con effetti sulla libera circolazione dei dati personali
all'interno dell'Unione



I registri delle attività di trattamento



Non dei singoli
trattamenti


Il registro delle attività di trattamento concorre alla definizione dell'accountability

Il titolare non può dimostrare di aver correttamente protetto i dati personali se non ha fatto una ricognizione di tutti i trattamenti

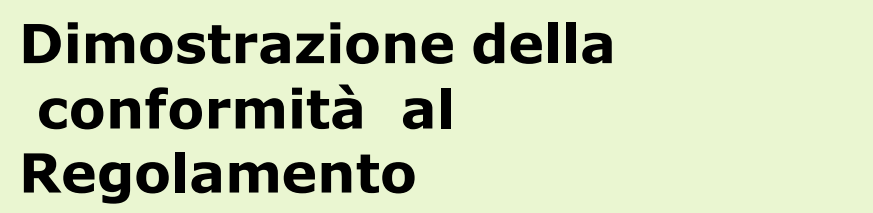
Cooperazione con
l'Autorità di
controllo

Monitoraggio per Autorità e titolare

*Il registro è la base per eseguire ulteriori adempimenti,
dalle informative alle misure di sicurezza*



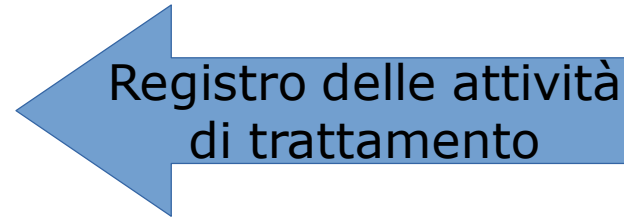
Finalità del
Registro
Cons. 82



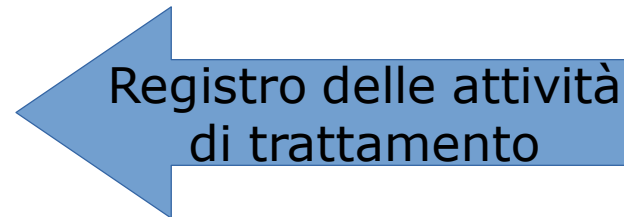
**Dimostrazione della
conformità al
Regolamento**

Quanti registri

Il titolare



Il Responsabile esterno



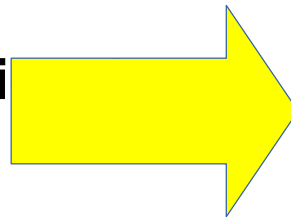
Da dove cominciare

Dall'utilizzo del contenuto del Regolamento per il trattamento dei dati sensibili e giudiziari

DM 305/2006

Dal Documento Programmatico sulla sicurezza

Chi sono i soggetti obbli



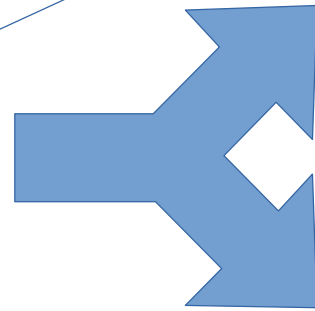
Tutti i titolari
Tutti i responsabili esterni
del trattamento

Il contenuto del Registro del Titolare

I dati di contatto: titolare, RPD, Contitolare

Correlazione con
contenuto
dell'informativa

Finalità del trattamento



Opportunità dell'indicazione:
le finalità di rilevante interesse
pubblico

Base giuridica

Categorie di interessati e dati

Categorie di destinatari e trasferimenti di dati

Termini per la cancellazione dati

Sicurezza

Registri delle attività di trattamento

Il Registro del titolare (CONTENUTI)

Finalità del trattamento

- art. 30, p. 1, lett. b)

(stessi dati contenuti
nell'informativa art. 13,
par. 1, lett. c)

OPPORTUNO
INDICARE

ELENCO DI TUTTE LE
FINALITÀ

le finalità di
rilevante
interesse
pubblico

la norma di riferimento,
la base giuridica del
trattamento (utile anche
per individuare i destinatari
delle comunicazioni)

Registri delle attività di trattamento

Il Registro del titolare (CONTENUTI)

Misure di sicurezza

- art. 30, p. 1, lett. g)



NECESSARIO
INDICARE

ove possibile

una descrizione generale
delle misure di sicurezza
tecniche e organizzative di
cui all'articolo 32, par. 1.

esempi:
pseudonimizzazione,
cifratura, resilienza dei
sistemi e dei servizi di
trattamento, ripristino
dati, procedura per
verificare dell'efficacia
delle misure la
sicurezza

altri e responsabili: la mappa dei trattamenti e la gestione delle violazioni di sicurezza

Il Registro del titolare

CONTENUTI EVENTUALI esempi

- VALUTAZIONE D'IMPATTO (E EVENTUALMENTE CONSULTAZIONE PREVENTIVA AL GARANTE)
- ADESIONE A CODICI DI CONDOTTA
- CERTIFICAZIONI
- CATEGORIE DI INCARICATI
- DATA DI INIZIO DEL TRATTAMENTO

Il contenuto del Registro del Responsabile

I dati di contatto: Responsabile, di ogni titolare per conto del quale agisce, del RPD

Categorie di trattamenti effettuati per conto di ogni titolare

Trasferimenti verso un paese terzo o un'organizzazione internazionale e documentazione delle garanzie adeguate

Descrizione generale delle misure di sicurezza tecniche e organizzative

Eventuale contenuto ulteriore

La sicurezza dei dati personali

Adempimenti riguarda 

Parte informatica

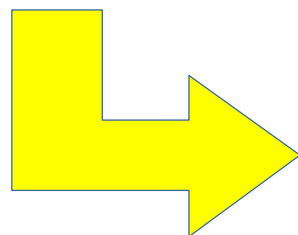
Parte organizzativa del

Fondamentale
è la
formazione
del
personale

L'obiettivo della sicurezza è la garanzia della protezione delle persone a mezzo della integrità dei dati e della difesa degli stessi da attacchi esterni

Obiettivi strumentali alla finalità di protezione della persona fisica

Documento della valutazione dei rischi



Manuale per la sicurezza ad uso degli autorizzati e altre policies specifiche relative a tecnologie o trattamenti particolari

Affidate al TITOLARE

Tecniche e organizzative

**Non più misure minime di sicurezza ma misure adeguate
Attraverso un processo di revisione continua (valutazione
dell'impatto)**

Elenco di alcuni rischi secondo il RGPD

Distruzione

Perdita

Modifica

Divulgazione non autorizzata

Accesso accidentale o illegale

Misure tecniche/organizzative

- .Pseudonimizzazione

- .Cifratura

- .Assicurazione permanente di Riservatezza, Integrità, Disponibilità;

- .Resilienza

- .Ripristino tempestivo disponibilità dati;

- .Ripristino tempestivo accesso ai dati in caso di incidente fisico o tecnico

- .Procedure di test periodico per verificare e valutare efficacia misure adottate

Elenco di alcuni rischi

Comportamenti degli operatori	Sottrazione di credenziali di autenticazione Carenza di consapevolezza, disattenzione o incuria Comportamenti sleali o fraudolenti Errore materiale
Eventi relativi agli strumenti	Azione di virus informatici o di programmi che possono arrecare danno Spamming o tecniche di sabotaggio Malfunzionamento o deterioramento degli strumenti Accessi esterni non autorizzati Intercettazione di informazioni in rete
Eventi relativi al contesto	Accessi non autorizzati a locali Sottrazione di strumenti contenenti dati Eventi distruttivi, naturali o artificiali, dolosi o accidentali o dovuti a incuria Guasto a sistemi complementari Errori umani nella gestione della sicurezza fisica

Valutazione d'impatto sulla protezione dati (art. 35)

Rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone

Cos'è un rischio

“Per rischio si intende uno scenario descrittivo di un evento e delle relative conseguenze che sono stimate in termini di gravità e probabilità” (Gruppo art. 29)

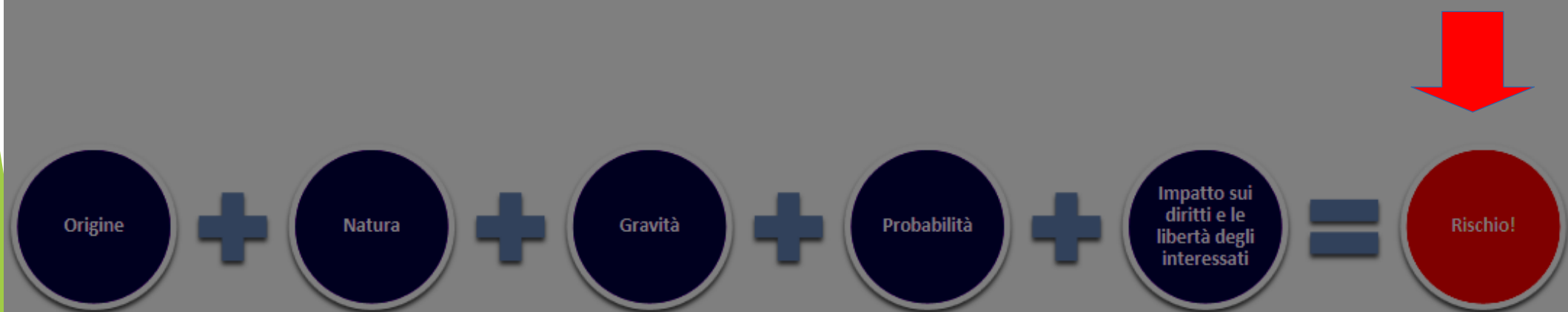
Quando il trattamento presenta un **rischio elevato per i diritti e le libertà delle persone** fisiche è necessario effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali

Documento “valutazione di impatto sulla protezione dei dati”

PERCHÉ?

La DPIA è uno strumento importante in termini di responsabilizzazione (*accountability*) in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del RGPD, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni. In altri termini, **la DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali**. Vista la sua utilità, il Gruppo Art. 29 suggerisce di valutarne l'impiego **per tutti i trattamenti, e non solo** nei casi in cui il Regolamento la prescrive come obbligatoria.

ELEMENTI DA CONSIDERARE NELLA INDIVIDUAZIONE DEL **RISCHIO**



ERRORI DA EVITARE:

Non bisogna confondere la gestione dei rischi con il tema delle misure di sicurezza

Il rischio non si riferisce al titolare ma al soggetto interessato



ATTENZIONE!

Non solo la sicurezza del trattamento

La valutazione del rischio deve riguardare

Ma anche gli effetti complessivi del trattamento

Gli effetti complessivi del trattamento





Cos'è il rischio elevato

È un principio di carattere generale

Può derivare dall'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento

La valutazione d'impatto è uno strumento di gestione del rischio



E in più:

Sorveglianza sistematica su larga scala di una zona accessibile al pubblico

Categorie particolari di dati trattati su larga scala

Dati comuni

Categorie particolari di dati trattati su larga scala Art. 35, c. 3, lett. b)



Trattamenti in parte già previsti dal DM 305/2006

Criteri di carattere generale Rischio elevato

Indicatori elaborati dal gruppo ex art. 29:

Trattamenti valutativi o di scoring
Decisioni automatizzate che producono significativi effetti giuridici o di analoga natura
Monitoraggio sistematico
Dati sensibili o dati di natura estremamente personale
Trattamenti di dati su larga scala
Combinazione e raffronto di insiemi di dati
Dati relativi a interessati vulnerabili
Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative
Trattamenti che di per sé impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Altri casi da valutare:

Geolocalizzazioni

Transazioni finanziarie

Comunicazioni elettroniche

Dati di minori

Cons. 75: i rischi possono derivare da un trattamento che può comportare discriminazioni, furto o usurpazione di identità.....; se sono trattati dati personali di persone fisiche vulnerabili, **in particolare minori.....**

Almeno due di questi criteri

QUANDO LA DPIA NON E' OBBLIGATORIA?

Secondo le Linee guida del Gruppo Art. 29, la DPIA NON è necessaria per i trattamenti che:

- non presentano rischio elevato per diritti e libertà delle persone Fisiche;
- hanno natura , ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
- fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.

Valutazione d'impatto

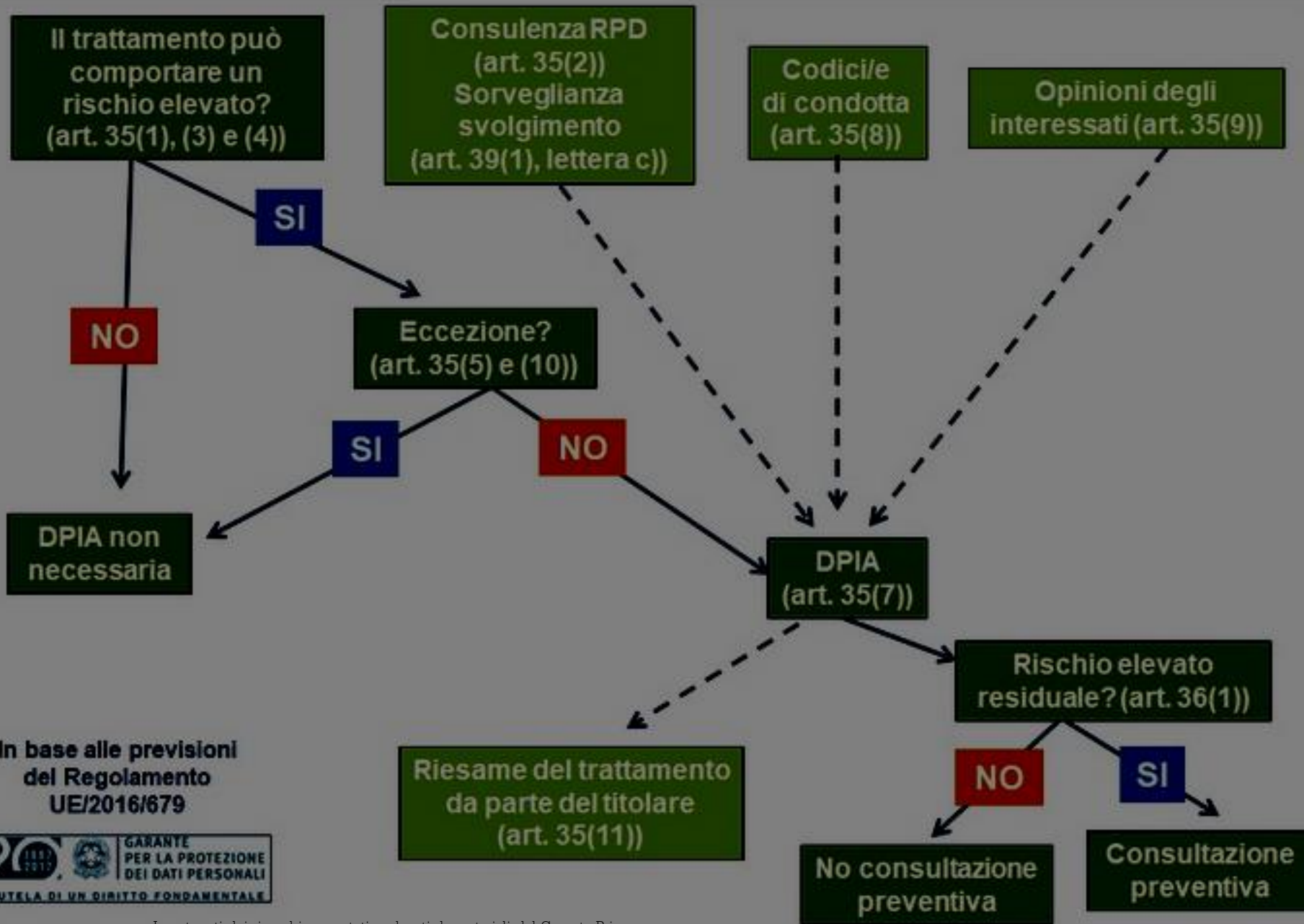
Chi: il titolare del trattamento si consulta con il DPO

La conduzione materiale della DPIA può essere affidata anche a un altro soggetto ma la responsabilità ricade sul titolare



Prima di procedere
Al trattamento

Valutazione di impatto sulla protezione dei dati (DPIA). Quando effettuarla?



In base alle previsioni
del Regolamento
UE/2016/679



Inosservanza obbligo DPIA

Mancato svolgimento della valutazione d'impatto

Svolgimento non corretto di una valutazione d'impatto

Mancata consultazione dell'autorità di controllo

Sanzione amministrativa

Data breach (artt. 32-34)

**“Violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso o l’accesso ai dati personali trasmessi, conservati o trattati”
(art. 4, definizione n. 12)**

Obblighi del titolare in caso di data breach (art. 33)

notifica della violazione all'autorità di controllo senza ingiustificato ritardo e, ove possibile, **entro 72 ore** dal momento in cui ne è venuto a conoscenza (**a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche**).

Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei **motivi del ritardo**.

Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione

almeno:

descrizione natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

comunicazione nome e **dati di contatto** del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

descrizione delle **probabili conseguenze** della violazione dei dati personali;

descrizione delle **misure adottate** o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi

Altri adempimenti data breach

Comunicazione data breach all'interessato (art. 34)

Quando: Se la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche

Tempi: senza ingiustificato ritardo

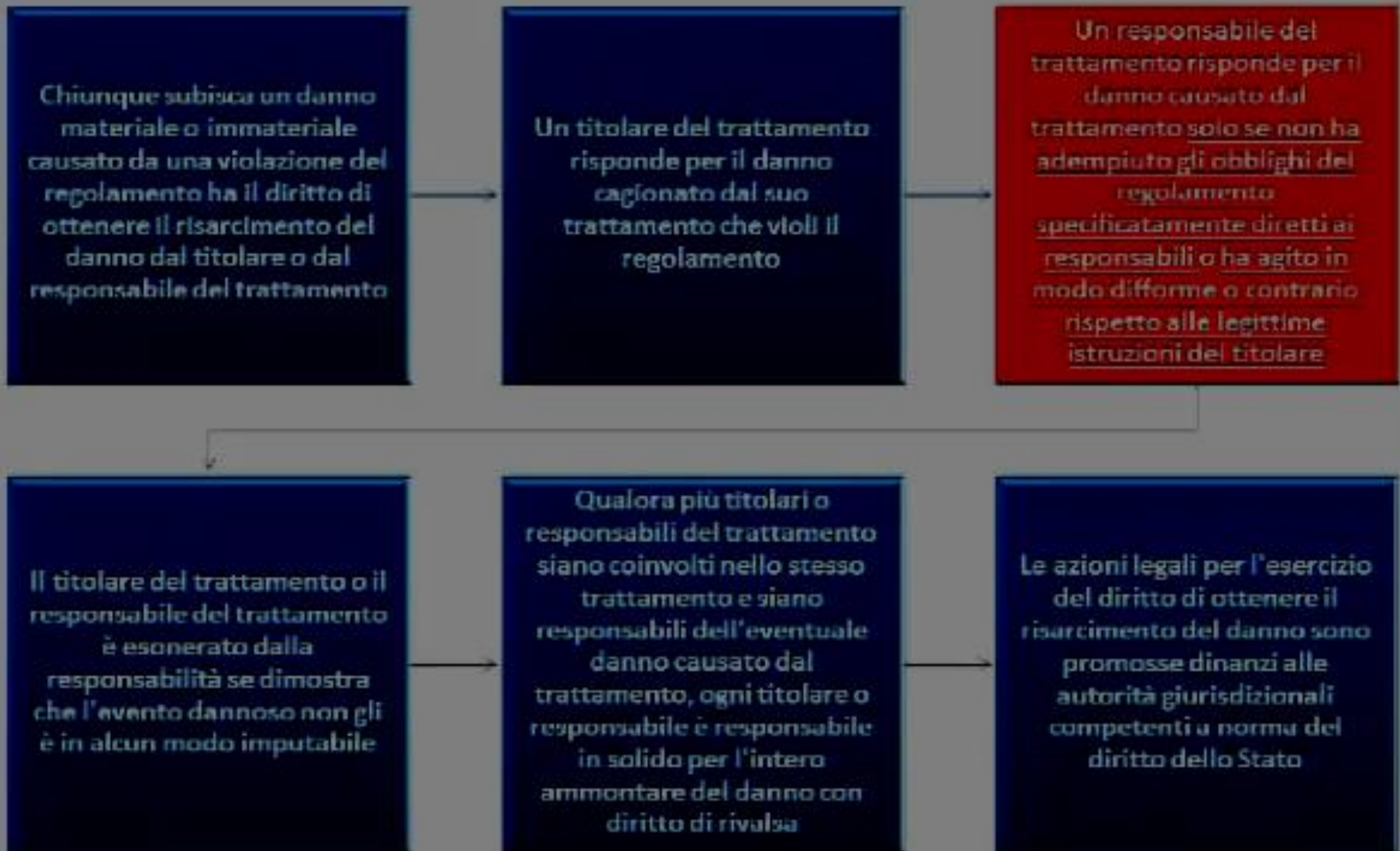
Cosa: descrizione con un linguaggio semplice e chiaro della natura della violazione dei dati personali e delle informazioni e delle misure (art. 33, par 3, lett b, c ed e).

Eccezioni comunicazione data breach all'interessato

Non è richiesta la comunicazione all'interessato se:

- il titolare del trattamento ha messo in atto le **misure tecniche e organizzative adeguate** di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- il titolare del trattamento **ha successivamente adottato misure** atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
- detta comunicazione richiederebbe **sforzi sproporzionati**. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analogha efficacia

Diritto al risarcimento e responsabilità (art. 82)



Grazie a tutti per l'attenzione

Anna Armone