Il Regolamento europeo UE n. 2016/679
L’applicazione alle istituzioni scolastiche

Benveuto.....

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

-Decreto legislativo attuativo del Regolamento in corso di pubblicazione sulla GU

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.

I contenuti dei riquadri sono stati prelevati da materiali del Garante Privacy

Uniformizzazione in tutta la UE

Questo obiettivo è raggiunto attraverso:

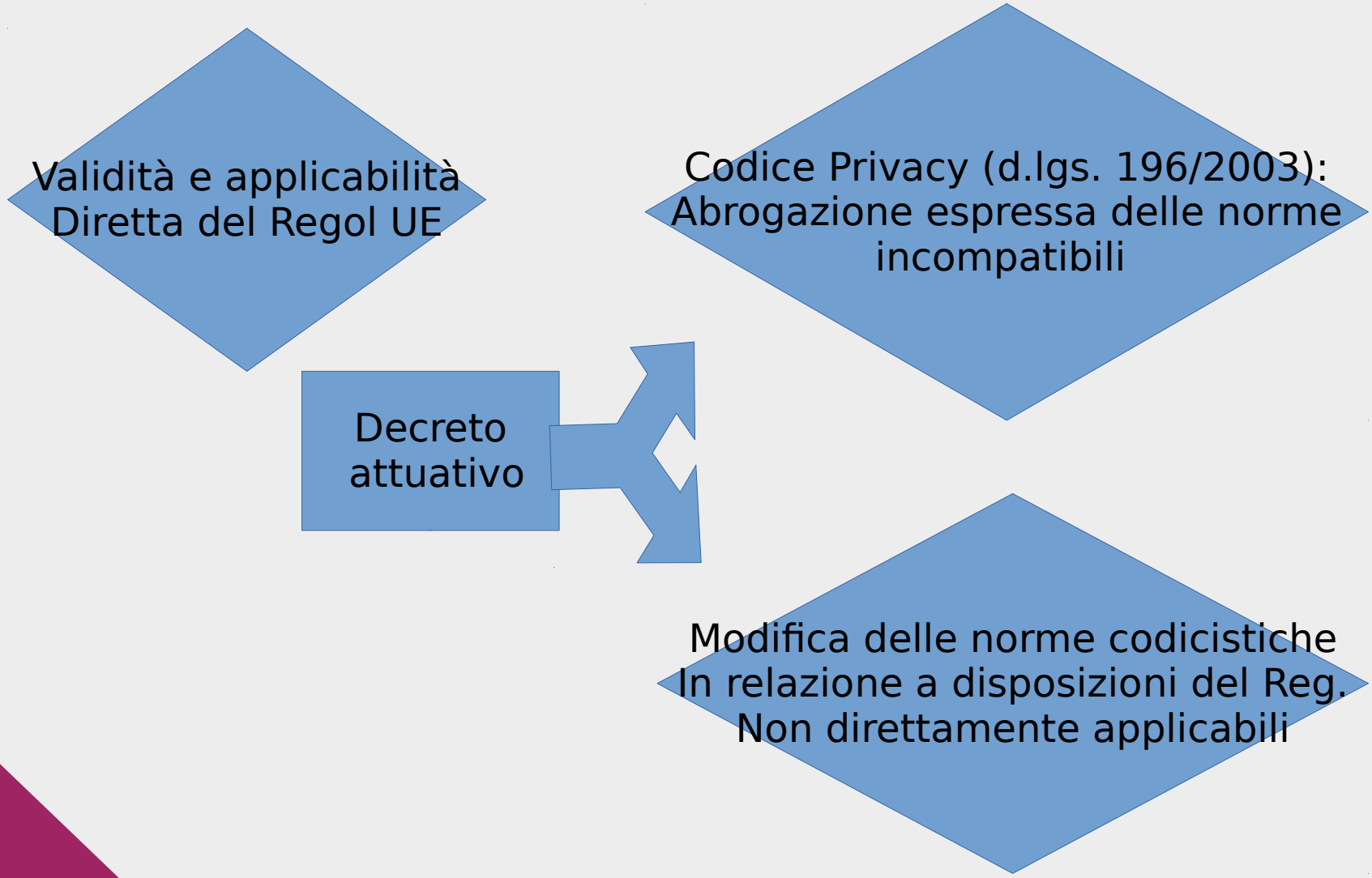
Responsabilizzazione

Diritti degli interessati

Ruolo dell’Autorità di controllo

Europeizzazione di standard e prassi

Il decreto legislativo attuativo del Regolamento 679/2016



Il Codice ha perso la sua centralità

- Codice e Regolamento seguono due filosofie diverse

Il Regolamento è basato sull'accountability: "responsabilizzazione". Questa consiste nell'obbligo per il titolare del trattamento di adottare misure appropriate ed efficaci per attuare i principi di protezione dei dati, nonché nella necessità di dimostrare, su richiesta, che sono state adottate misure appropriate ed efficaci.

Il Codice è prescrittivo

Presupposto: un approccio sistemico

Presupposti di liceità

Definizione di compiti

Valutazione d’impatto

accountability

Privacy by design

Privacy by default

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 toto ricordo dei suoi alunni;
studenti che scattano foto a coetanei

Le priorità realizzate 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

I contenuti dei riquadri sono stati prelevati da materiali del Garante Privacy

Accountability

Essere accountable è un criterio di attenuazione della responsabilità

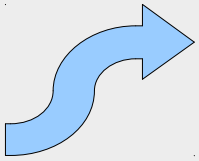
Approccio sistemico all'interno del titolare del trattamento.
Occorre legare i vari pezzi

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

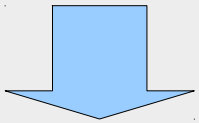
L'accountabilty è una trama all'interno del Regolamento

L’accountability e l’approccio basato sul rischio – il considerando 74

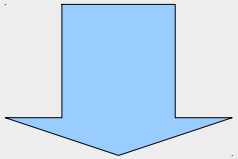
Le variabili:
- la natura dell’ambito di applicazione del contesto
- le finalità del trattamento
- i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche



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

“È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest’ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto…..”

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)

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) art. 2-ter Decreto legislativo attuativo

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

Qualità dei dati + sicurezza

Ex art. 11 Codice

È ampliato il catalogo dei dati sensibili

Dati biometrici e dati genetici (art. 9 RGPD)

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

[Esempio 4]
Una scuola pubblica chiede agli studenti il consenso ad utilizzare le loro fotografie in una rivista studentesca in formato cartaceo. In questo caso il consenso costituisce una scelta vera e propria a condizione che agli studenti non vengano negati l’istruzione o altri servizi e che gli studenti possano rifiutare il consenso senza subire pregiudizio16.

Comunicazione e diffusione di dati da parte di soggetti pubblici (art. 2 ter decreto legislativo applicativo Reg. 679/2016

3. La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente se previste ai sensi del comma 1 (norma di legge o regolamento)

a) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile **o dal suo rappresentante nel territorio dell'Unione europea**, dalle persone autorizzate, ai sensi dell'articolo **2-quaterdecies**, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;

b) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Decreto legislativo attuativo del Regolamento UE art. 2-ter

3. La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente se previste ai sensi del comma 1.

"comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile **o dal suo rappresentante nel territorio dell'Unione europea**, dalle persone autorizzate, ai sensi dell'articolo **2-quaterdecies**, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;

b) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Fonte: Camera dei Deputati. Audit ageduamento disciplina Privacy al Reg. UR 679/2016 pag. 17

Articolo 7

Modifiche alla Parte II, Titolo VI, del decreto legislativo 30 giugno 2003, n. 196

1. Alla Parte II, Titolo VI, del decreto legislativo 30 giugno 2003, n. 196, l'articolo 96 è sostituito dal seguente:

"Art. 96

(*Trattamento di dati relativi a studenti*)

1. Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, le istituzioni del sistema nazionale di istruzione, i centri di formazione professionale regionale, le scuole private non paritarie nonché le istituzioni di alta formazione artistica e coreutica e le università statali o non statali legalmente riconosciute su richiesta degli interessati, possono comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti formativi, intermedi e finali, degli studenti e altri dati personali diversi da quelli di cui agli articoli 9 e 10 del Regolamento, pertinenti in relazione alle predette finalità e indicati nelle informazioni rese agli interessati ai sensi dell'articolo 13 del Regolamento. I dati possono essere successivamente trattati esclusivamente per le predette finalità.

2. Resta ferma la disposizione di cui all'articolo 2, comma 2, del decreto del Presidente della Repubblica 24 giugno 1998, n. 249, sulla tutela del diritto dello studente alla riservatezza. Restano altresì ferme le vigenti disposizioni in materia di pubblicazione dell'esito degli esami mediante affissione nell'albo dell'istituto e di rilascio di diplomi e certificati."

ANP (Dirigenti scolastici): chiede un'integrazione all'art. 96, affinché previa adeguata informativa agli interessati e nel rispetto del principio di minimizzazione dei trattamenti, con rigorosa selezione da parte della scuola, sia chiaramente consentito alle scuole l'uso di foto ed immagini anche attraverso forme di pubblicazione sul sito istituzionale.

Le modifiche al Codice Privacy (dlgs 196/2003) contenute nel decreto legislativo attuativo del Regolamento

Art. 2-ter

(Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri)

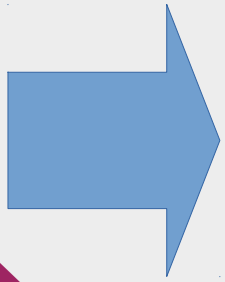
1. La base giuridica prevista dall'articolo 6, paragrafo 3, lettera b), del Regolamento è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento.

2. La comunicazione fra titolari che effettuano trattamenti di dati personali, diversi da quelli ricompresi nelle particolari categorie di cui all'articolo 9 del Regolamento e di quelli relativi a condanne penali e reati di cui all'articolo 10 del Regolamento, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è ammessa se prevista ai sensi del comma 1. In mancanza di tale norma, la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di quarantacinque giorni dalla relativa comunicazione al Garante, senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati.

Art. 2-*sexies*

Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante

1. I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi **del paragrafo 2, lettera g),** del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, **nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.**



C 2, lett. bb) istruzione e formazione in ambito scolastico, professionale, superiore o universitario;
cc) trattamenti ai fini di archiviazione nel pubblico interesse o di ricerca storica
dd)instaurazione, gestione ed estinzione, di rapporti di lavoro

Decreto legislativo applicativo del Regolamento UE Art. 2-*sexies*

(*Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante*)

1. I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

2. Fermo quanto previsto dal comma 1, si considera rilevante l’interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all’esercizio di pubblici poteri nelle seguenti materie:
a) accesso a documenti amministrativi e accesso civico;
l) attività di controllo e ispettive;
m) concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;
o) rapporti tra i soggetti pubblici e gli enti del terzo settore;
r) rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose;
s) attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci;
bb) istruzione e formazione in ambito scolastico, professionale, superiore o universitario;
cc) trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l’ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di **interesse storico particolarmente importante** rilevante interesse storico, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale;
dd) instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell’ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva.
3. Per i dati genetici, biometrici e relativi alla salute il trattamento avviene comunque nel rispetto di quanto previsto dall’articolo 2-*septies*.

Art. 9 Reg 679 Trattamento di categorie particolari di dati personali

Il trattamento è ammesso, tra gli altri nei seguenti casi

b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

(**C 55, C 56**)

Decreto di adeguamento del Codice Privacy

Art. 2-*sexies*

(*Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante*)

1. I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi **del paragrafo 2, lettera g),** del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, **nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.**

Decreto adeguamento del regolamento UE Art. 2-*septies*

(*Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute*)

Questo art. prevede gli adempimenti di cui all'art. 9, par. 4 del Reg 679

2. Il provvedimento che stabilisce le misure di garanzia di cui al comma 1 è adottato con cadenza almeno biennale e tenendo conto:
a) delle linee guida, delle raccomandazioni e delle migliori prassi pubblicate dal Comitato europeo per la protezione dei dati e delle migliori prassi in materia di trattamento dei dati personali;
b) dell'evoluzione scientifica e tecnologica nel settore oggetto delle misure;
c) dell'interesse alla libera circolazione dei dati personali nel territorio dell'Unione europea.
3. Lo schema di provvedimento è sottoposto a consultazione pubblica per un periodo non inferiore a sessanta giorni.
4. Le misure di garanzia sono adottate nel rispetto di quanto previsto dall'articolo 9, paragrafo 2, del Regolamento, e riguardano anche le cautele da adottare relativamente a:
a) contrassegni sui veicoli e accessi a zone a traffico limitato;
b) profili organizzativi e gestionali in ambito sanitario;
c) modalità per la comunicazione diretta all'interessato delle diagnosi e dei dati relativi alla propria salute;
d) prescrizioni di medicinali

Decreto di ADEGUAMENTO DEL Codice Privacy
Art. 2-*octies*
(Principi relativi al trattamento di dati relativi a condanne penali e reati)

In raccordo con quanto previsto dalla direttiva 2016/680 e dal relativo decreto di recepimento, viene introdotta una disposizione (l'art. 2-octies) relativa al trattamento di dati concernenti condanne penali e reati, limitando le operazioni di trattamento ai soli casi in cui queste siano previste da una norma di legge o di regolamento. In particolare, la liceità di tale trattamento, ove non sia svolto sotto il controllo di un'autorità pubblica, è subordinata alla sussistenza di una disposizione di legge o di regolamento che lo autorizzi e che preveda al contempo garanzie appropriate per i diritti degli interessati. La ratio di tale disposizione è da rinvenire nella volontà di tutelare l'interessato da trattamenti particolarmente invasivi della propria privacy, considerate le finalità del trattamento e la tipologia dei dati. Una tutela effettiva può essere garantita solo dal vaglio di un'autorità pubblica, in grado di bilanciare gli interessi nazionali con quelli di riservatezza del singolo ovvero da un'espressa disposizione normativa contenente garanzie ulteriori, rispetto a quelle normalmente adottate, per la riservatezza dell'interessato.

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

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"

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

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

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

Art. 23 RGPD

Art. 85 RGPD

Art. 89 RGPD

Art. 2-undicies d.lgs. sdeguamento

L'articolo 2-duodecies, sotto la rubrica "Limitazioni per ragioni di giustizia" disciplina, nel rispetto di quanto disposto dall'articolo 23, paragrafo 1, lettera f) del regolamento, le limitazioni dei diritti degli interessati di cui agli articoli da 12 a 22 e 34, per esigenze di salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari, relativamente a dati trattati nell'ambito di procedimenti dinanzi agli uffici giudiziari di ogni ordine e grado nonché dinanzi al Consiglio superiore della magistratura e agli altri organi di governo autonomo delle magistrature speciali o presso il Ministero della giustizia, ovvero relativamente a trattamenti che, in materia di trattamento giuridico ed economico del personale di magistratura, hanno una diretta incidenza sulla funzione giurisdizionale, nonché relativamente alle attività ispettive su uffici giudiziari. Tali limitazioni non si applicano per l'ordinaria attività amministrativo-gestionale di personale, mezzi o strutture, quando non è pregiudicata la segretezza di atti direttamente connessi alla trattazione dei procedimenti.

Si prevede che i diritti sanciti dagli articoli da 15 a 22 del regolamento non possano essere esercitati con richiesta al titolare o al responsabile del trattamento ovvero con reclamo, qualora possa derivarne un pregiudizio effettivo e concreto: agli interessi tutelati in base alle disposizioni vigenti in materia di riciclaggio o di sostegno alle vittime di richieste estorsive; all'attività di Commissioni parlamentari d'inchiesta; alle attività svolte da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità; allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria

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

L’interessato può anche chiedere la limitazione del trattamento

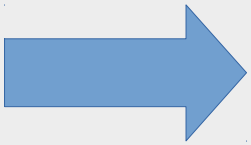
Il diritto di cancellazione (diritto all’oblio) (art. 17)

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

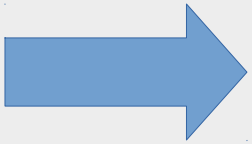
Diritto di limitazione del trattamento (art. 18)

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)

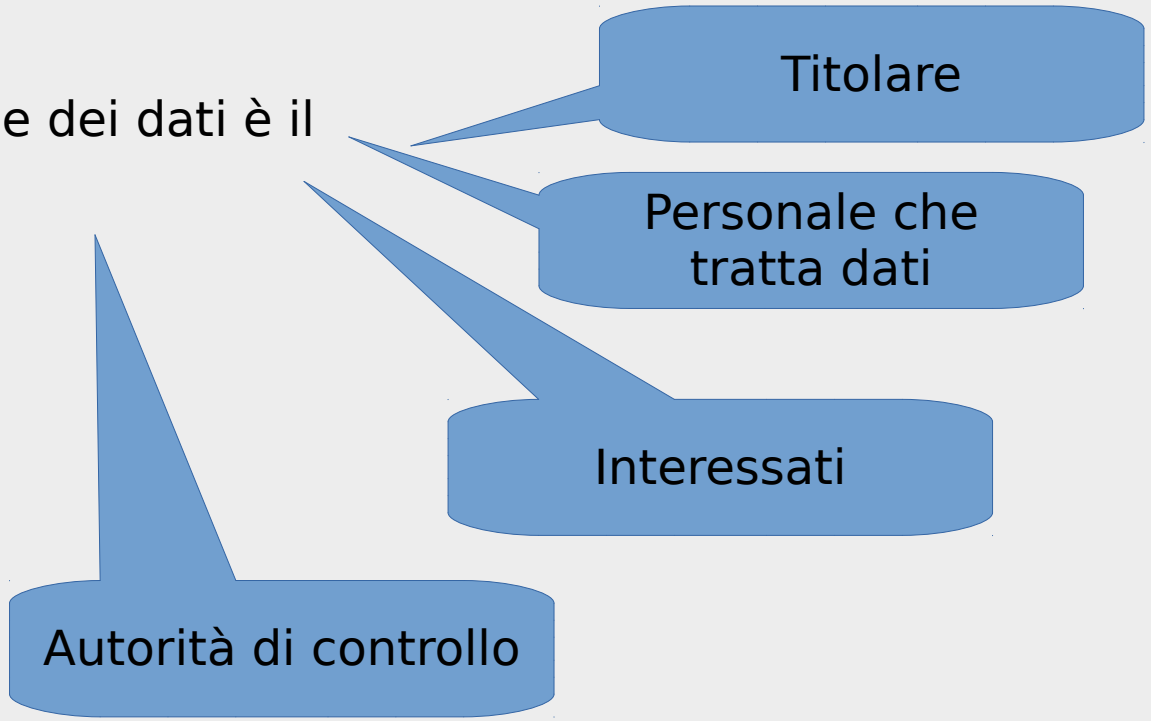
Si applica ai trattamenti automatizzati

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

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)

Nella Governance dei dati è il riferimento per



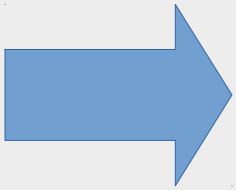
Il responsabile della protezione dati

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

I contenuti dei riquadri sono stati prelevati da materiali del Garante Privacy

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)

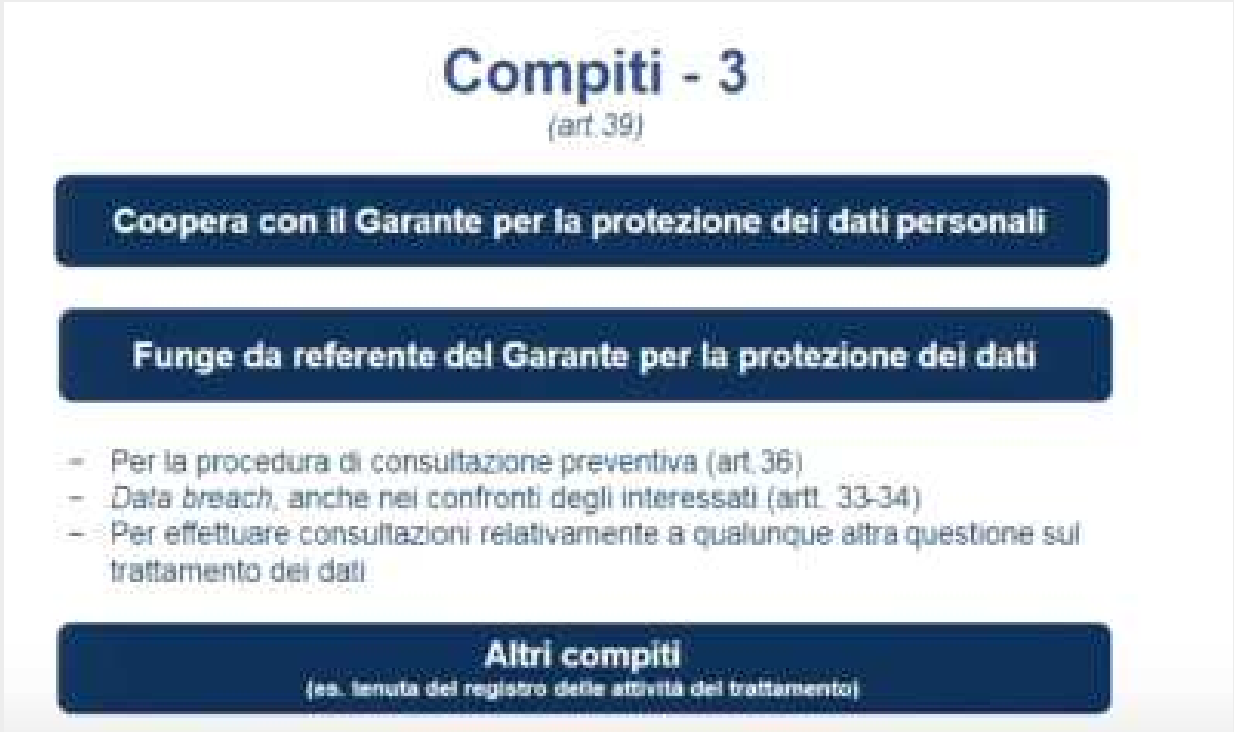
Ruolo nella valutazione d'impatto (DPIA)

- 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

I contenuti dei riquadri sono stati prelevati da materiali del Garante Privacy



I contenuti dei riquadri sono stati prelevati da materiali del Garante Privacy

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);

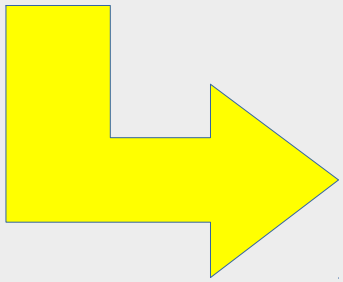
Istituzione scolastica

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 contenuti dei riquadri sono stati prelevati da materiali del Garante Privacy

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.

I contenuti dei riquadri sono stati prelevati da materiali del Garante Privacy

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

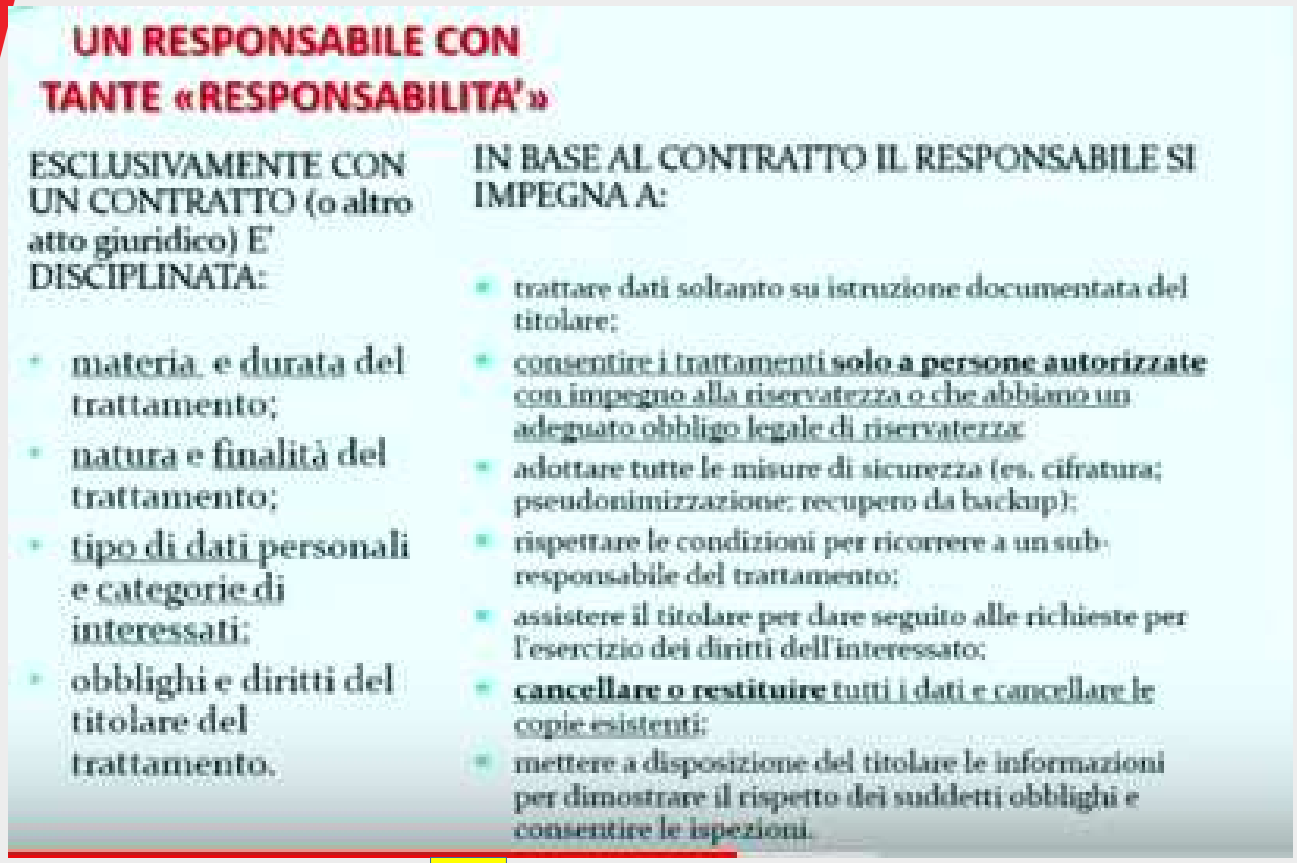
Il responsabile **può nominare sub-responsabili** per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e «responsabile primario».

ATTENZIONE

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

I contenuti dei riquadri sono stati prelevati da materiali del Garante Privacy

Le responsabilità del responsabile in outsourcing



UN RESPONSABILE CON TANTE «RESPONSABILITA'»

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.

OCCORRE ACCORDO ACCESSIVO AL CONTRATTO SUL TRATTAMENTO DEI DATI PERSONALI

I contenuti dei riquadri sono stati prelevati da materiali del Garante Privacy

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.

Regolamento UE 679
4-bis. Fermo restando quanto previsto ai commi 1, 2, 3 e 4, il titolare puo' avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualita' 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 finalita' perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalita' di trattamento; i predetti atti sono adottati in conformita' 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).

Art. 2- quaterdecies Dlgs di adeguamento del Codice

(Attribuzione di funzioni e compiti a soggetti designati)

1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.

2. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.

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.

I contenuti dei riquadri sono stati prelevati da materiali del Garante Privacy

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 a 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.

I contenuti dei riquadri sono stati prelevati da materiali del Garante Privacy

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

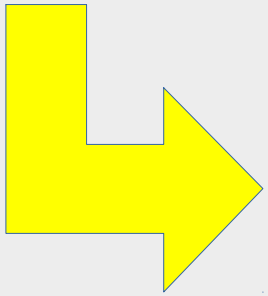
Le tappe fondamentali nella gestione della Privacy

Registro delle attività di trattamento → Mappa aggiornata dei dati e della loro vita

Analisi del rischio → Metodo per impostare una politica di protezione dei dati

Analisi di impatto → Previsione dell'impatto del trattamento di particolari dati sui diritti di libertà delle persone

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.

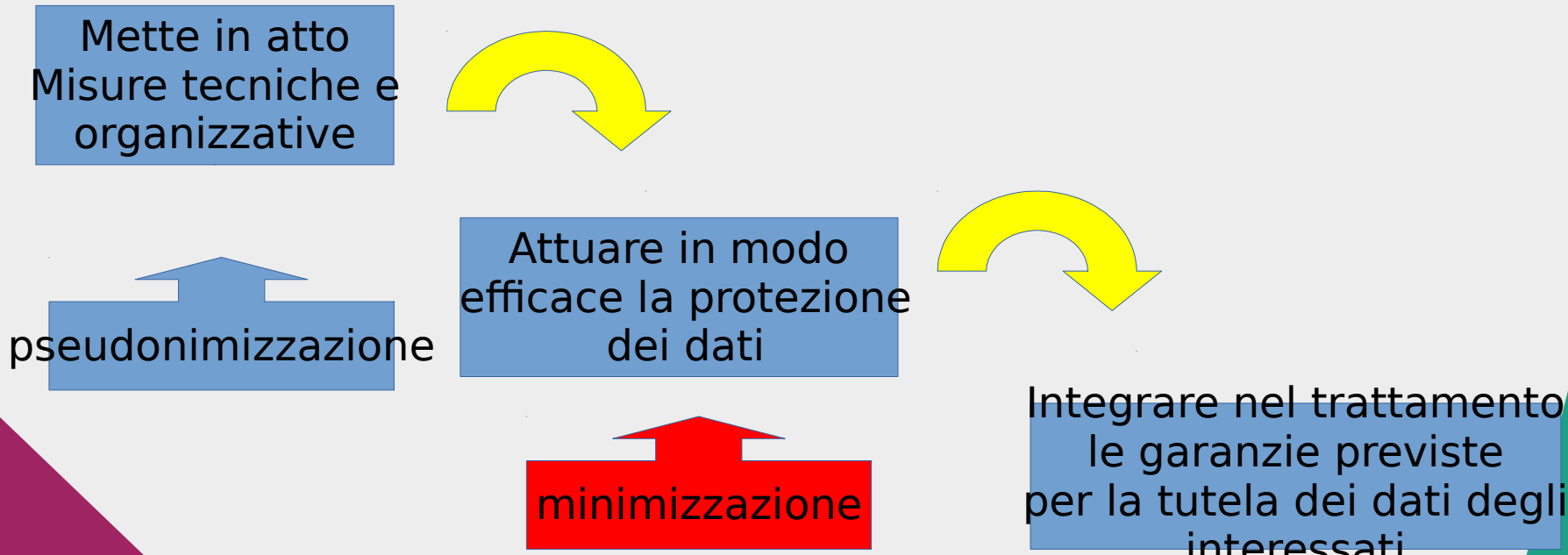
Modalità tecniche e organizzative del titolare del trattamento

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 contenuti dei riquadri sono stati prelevati da materiali del Garante Privacy

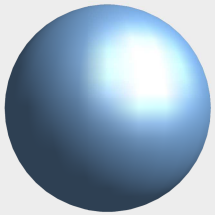
I registri delle attività di trattamento

Non dei singoli trattamenti

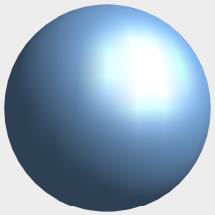
Finalità del Registro Cons. 82

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

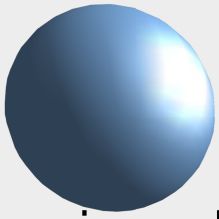
Il titolare non può dimostrare di aver correttamente protetto i dati personali se non ha fatto una ricognizione di tutti i trattamenti



Cooperazione con l'Autorità di controllo



Monitoraggio per Autorità e titolare

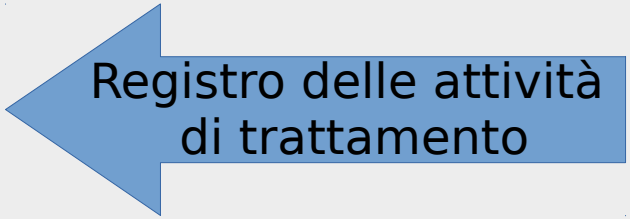


Dimostrazione della conformità al Regolamento

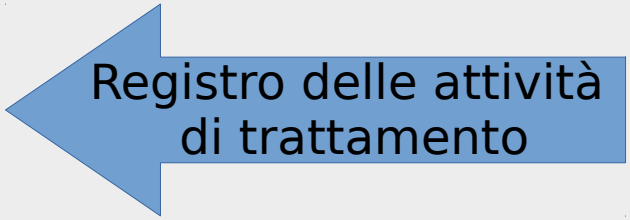
Il registro è la base per eseguire ulteriori adempimenti, dalle informative alle misure di sicurezza

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

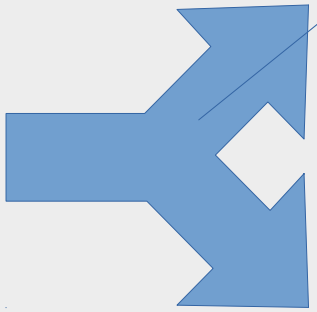
Chi sono i soggetti obbligati

Tutti i titolari
Tutti i responsabili esterni del trattamento

Il contenuto del Registro del Titolare

I dati di contatto: titolare, RPD, Contitolare

Finalità del trattamento



Opportunità dell’indicazione: le finalità di rilevante interesse pubblico

Base giuridica

Correlazione con contenuto dell’informativa

Categorie di interessati e dati

Categorie di destinatari e trasferimenti di dati

Termini per la cancellazione dati

Sicurezza

I contenuti dei riquadri sono stati prelevati da materiali del Garante Privacy

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

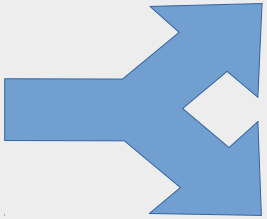
Trasferimenti verso un paese terzo o un’organizzazione internazionale e documentazione delle garanzie adeguate

Descrizione generale delle misure di sicurezza tecniche e organizzative

Eventuale contenuto ulteriore

La sicurezza dei dati personali

Adempimenti riguardano



Parte informatica

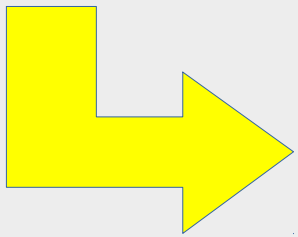
Parte organizzativa

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

Documento della valutazione dei rischi

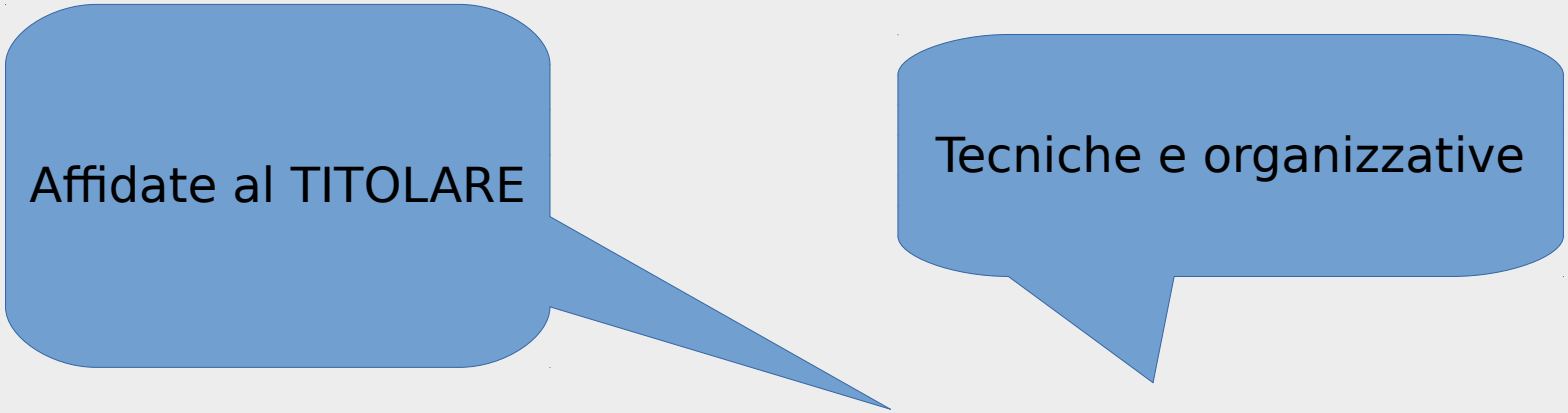
Obiettivi strumentali alla finalità di protezione della persona fisica



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

I contenuti dei riquadri sono stati prelevati da materiali del Garante Privacy

I contenuti dei riquadri sono stati prelevati da materiali del Garante Privacy



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 Erroti 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)

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.

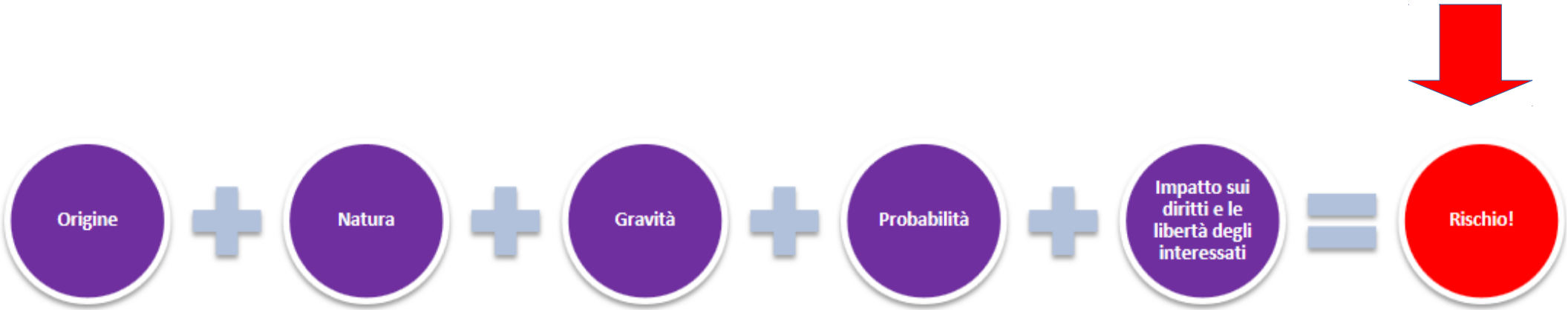
Quando il trattamento presenta un **rischio elevato per i diritti e le libertà delle persone** fisiche è necessario effettuare una valutazione dell’impatto dei trattamenti previsti sulla protezione dei dati personali

Documento “valutazione di impatto sulla protezione dei dati”

Ed eventuale consultazione preventiva

La valutazione dell’impatto

ELEMENTI DA CONSIDERARE NELLA INDIVIDUAZIONE DEL RISCHIO



I contenuti dei riquadri sono stati prelevati da materiali del Garante Privacy

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!

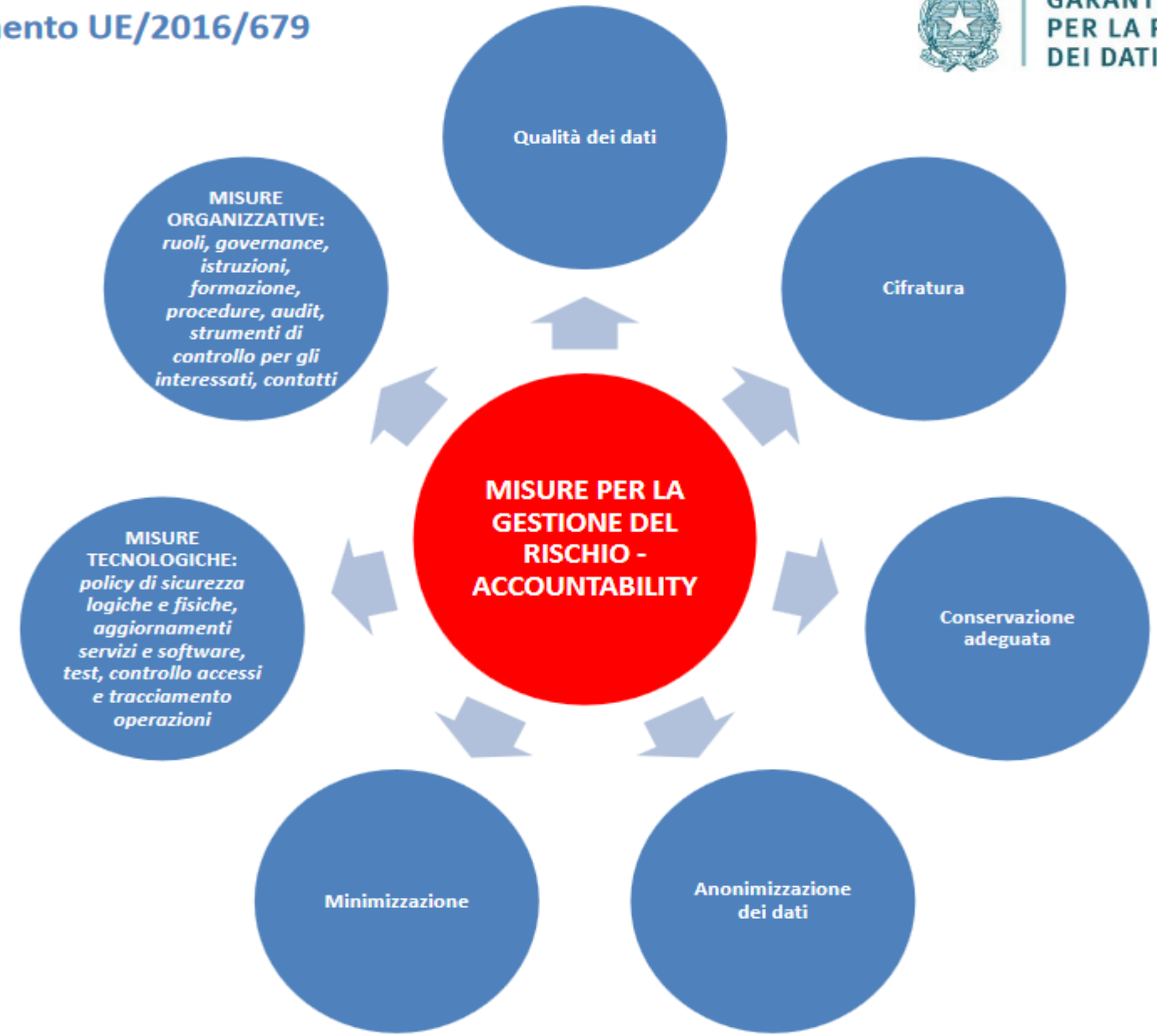
I contenuti dei riquadri sono stati prelevati da materiali del Garante Privacy

Gli effetti complessivi del trattamento

I contenuti dei riquadri sono stati prelevati da materiali del Garante Privacy

Regolamento UE/2016/679

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



I contenuti dei riquadri sono stati prelevati da materiali del Garante Privacy

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

I contenuti dei riquadri sono stati prelevati da materiali del Garante Privacy

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

Trattamenti in parte già previsti dal DM 305/2006

I contenuti dei riquadri sono stati prelevati da materiali del Garante Privacy

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

Almeno due di questi criteri

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....**

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;

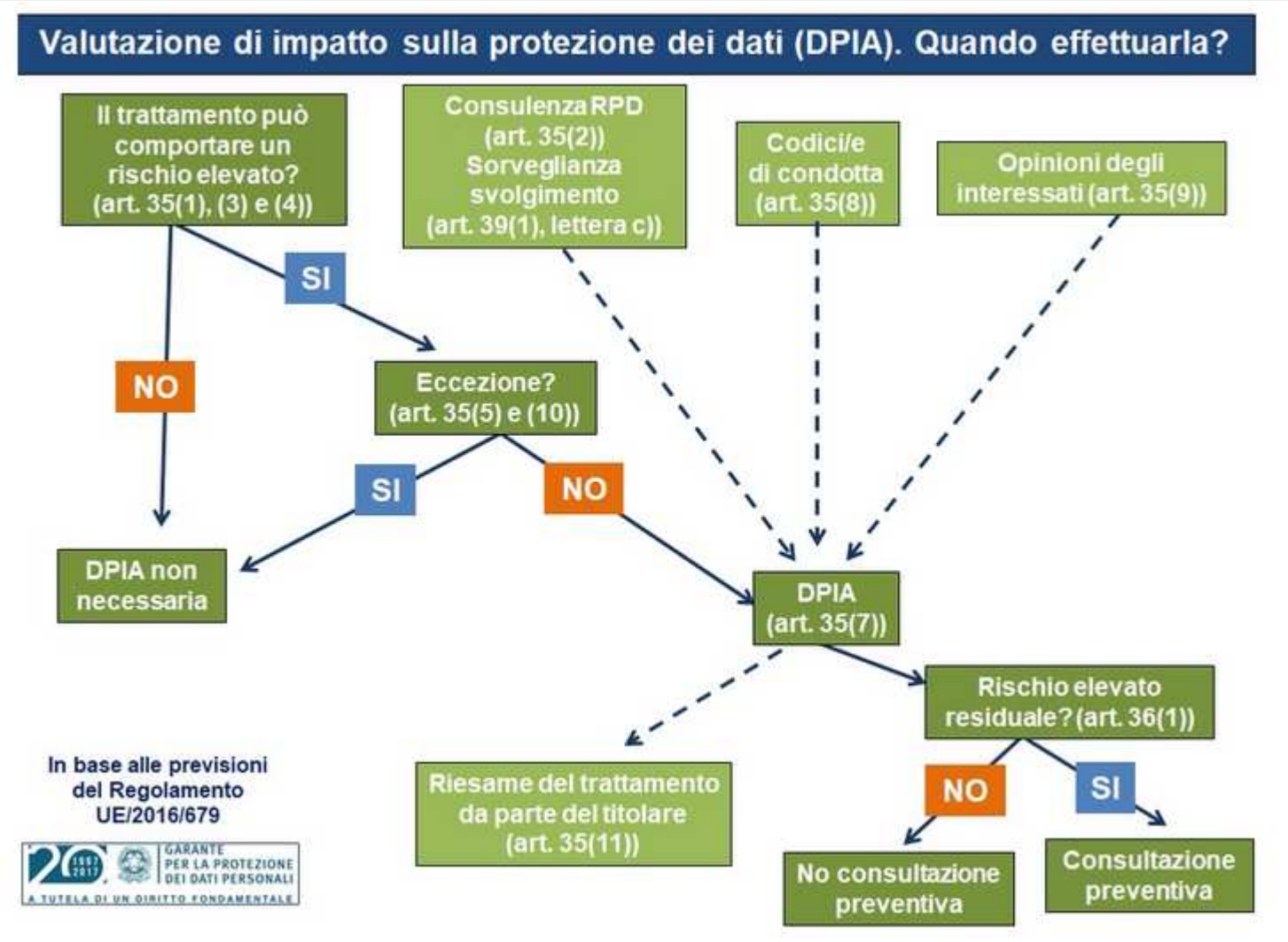
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;

- 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



I contenuti dei riquadri sono stati prelevati da materiali del Garante Privacy

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

I contenuti dei riquadri sono stati prelevati da materiali del Garante Privacy

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 eprsone fisiche

Tempi: senza ingiustificato ritardo

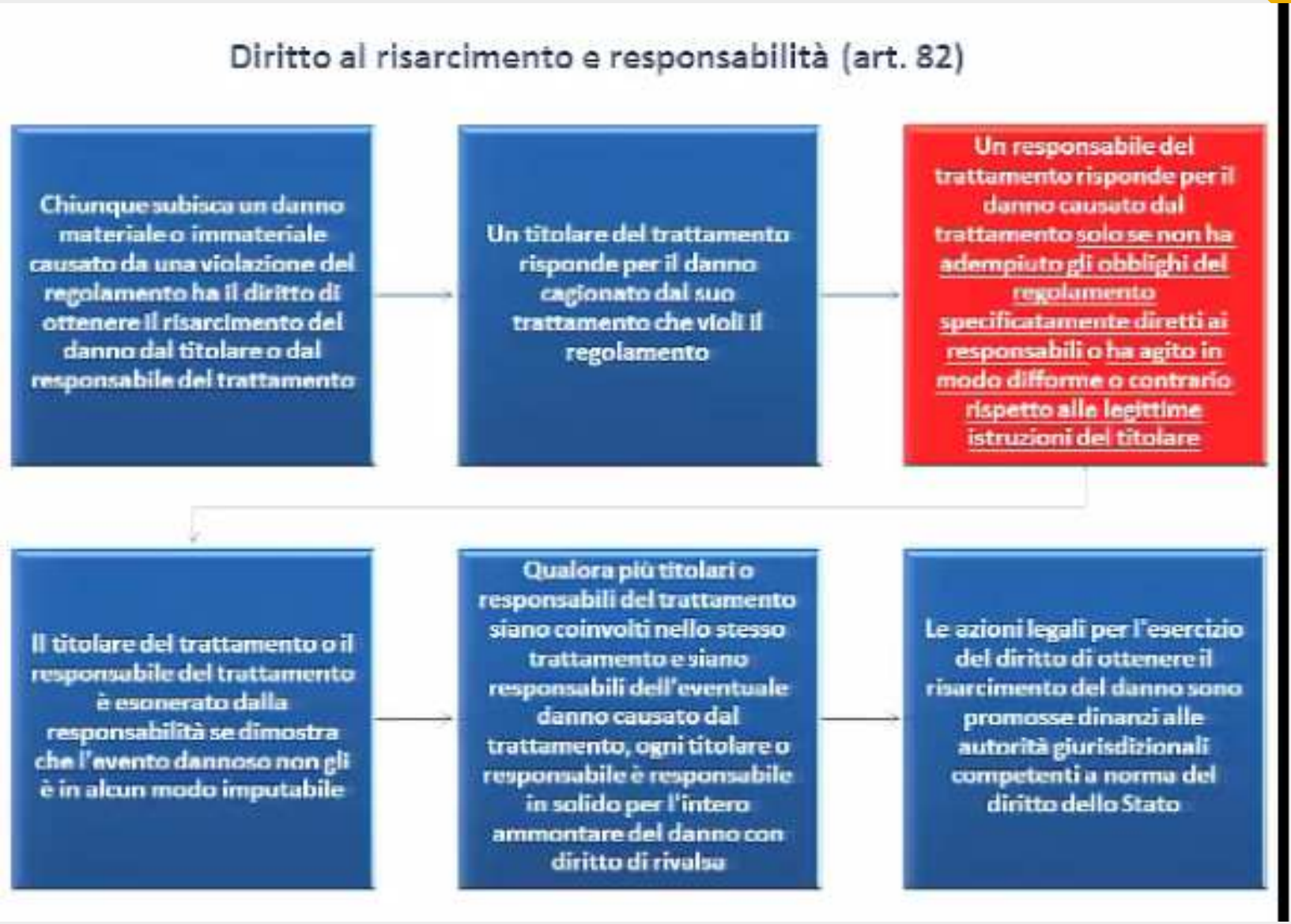
Cosa: descrizione con un linguaggio semplice e chiaro della natura della violazione dei dati personali e delle informazioni e delle misure (art. 33, par 3, lett b, c ed e=.

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 analoga efficacia

I contenuti dei riquadri sono stati prelevati da materiali del Garante Privacy



I contenuti dei riquadri sono stati prelevati da materiali del Garante Privacy

Art. 2-*octies*

(Principi relativi al trattamento di dati relativi a condanne penali e reati)

5. Quando il trattamento dei dati di cui al presente articolo avviene sotto il controllo dell'autorità pubblica si applicano le disposizioni previste dall'articolo 2-*sexies*.

ART. 3

(*Modifiche alla rubrica e al Titolo I della Parte II, del decreto legislativo 30 giugno 2003, n. 196*)

1. La rubrica della Parte II del decreto legislativo 30 giugno 2003, n. 196, è sostituita dalla seguente: “Disposizioni specifiche per i trattamenti necessari per adempiere ad un obbligo legale o per l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri nonché disposizioni per i trattamenti di cui al capo IX del Regolamento”.

a) all’articolo 59:
1) alla rubrica sono aggiunte, in fine, le seguenti parole: “e accesso civico”;
2) al comma 1, le parole “sensibili e giudiziari” sono sostituite dalle seguenti: “di cui agli articoli 9 e 10 del Regolamento” e le parole “Le attività finalizzate all’applicazione di tale disciplina si considerano di rilevante interesse pubblico.” sono soppresse;
3) dopo il comma 1 è aggiunto il seguente: “1-*bis*. I presupposti, le modalità e i limiti per l’esercizio del diritto di accesso civico restano disciplinati dal decreto legislativo 14 marzo 2013, n. 33.”;

b) l’articolo 60 è sostituito dal seguente:
“Art. 60
(*Dati relativi alla salute o alla vita sessuale o all’orientamento sessuale*)
1. Quando il trattamento concerne dati genetici, relativi alla salute, alla vita sessuale o all’orientamento sessuale della persona, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell’interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale.”;

Alla Parte II, Titolo VIII, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) la rubrica è sostituita dalla seguente: “Trattamenti nell’ambito del rapporto di lavoro”;

b) l’articolo 111 è sostituito dal seguente:

“Art. 111

(*Regole deontologiche per trattamenti nell’ambito del rapporto di lavoro*)

1. Il Garante promuove, ai sensi dell’articolo 2-*quater,* l’adozione di regole deontologiche per i soggetti pubblici e privati interessati al trattamento dei dati personali effettuato nell’ambito del rapporto di lavoro per le finalità di cui all’articolo 88 del Regolamento, prevedendo anche specifiche modalità per le informazioni da rendere all’interessato.”;

“Art. 111-bis

(Informazioni in caso di ricezione di curriculum)

1. Le informazioni di cui all’articolo 13 del Regolamento, nei casi di ricezione dei curricula spontaneamente trasmessi dagli interessati al fine della instaurazione di un rapporto di lavoro, vengono fornite al momento del primo contatto utile, successivo all’invio del curriculum medesimo. Nei limiti delle finalità di cui all’articolo 6, paragrafo 1, lettera b), del Regolamento, il consenso al trattamento dei dati personali presenti nei curricula non è dovuto.

Grazie a tutti per l'attenzione

Anna Armone