Formazione IFEL
per i Comuni

IFEL
Fondazione ANCI

Nuovi strumenti di accountability dei titolari

a cura di Giuseppe D'Acquisto
17 Maggio 2018

Indice

- **Privacy by design e by default (art. 25)**
- **Sicurezza (art. 32)**
- **Data Breach (artt. 33-34)**
- **Data Protection Impact Assessment (artt. 35-36)**

Privacy by design e by default (art. 25)

1.Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, **del contesto** e delle finalità del trattamento, come anche **dei rischi** aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, **sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso** il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

2.Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per **impostazione predefinita**, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, **non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica**.

3.Un meccanismo di **certificazione** approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

Privacy by design e by default (art. 25)

Privacy by design esempi

- Pseudonimizzazione
- Minimizzazione
- Randomizzazione
- Anonimizzazione

Privacy by default esempi

- Azione positiva per il consenso
- Test di necessità
- No-indicizzazione
- Autenticazione by default

Sicurezza (art. 32)

1.Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del **contesto** e delle finalità del trattamento, come anche del **rischio** di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la **pseudonimizzazione** e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la **riservatezza, l'integrità, la disponibilità** e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di **ripristinare tempestivamente la disponibilità** e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura **per testare, verificare e valutare regolarmente** l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2.Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei **rischi** presentati dal trattamento che derivano in particolare **dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione** non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

3.L'adesione a un **codice di condotta** approvato di cui all'articolo 40 o a un **meccanismo di certificazione** approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

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.

Sicurezza (art. 32)

Step 1

Risk		Threat		Impact
Possibility that a threat will materialize in combination with the impact of this threat (if it comes in effect).	=	Anything that may cause harm to the assets that we want to protect.	X	The extend of negative effects that a threat may bring.

Step 2 Understanding and evaluation of impact	Confidentiality
	Integrity
	Availability
Step 3 Definition of possible threats and evaluation of their likelihood	Network and technical resources
	Processes/procedures related to the data processing operation
	Different parties and people involved in the data processing operation
	Business sector and scale of processing

Data Breach (artt. 33-34)

1.In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 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.

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

3.La notifica di cui al paragrafo 1 deve almeno:

a)descrivere la **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;

b) comunicare **il nome e i dati di contatto del responsabile della protezione dei dati** o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili **conseguenze** della violazione dei dati personali;

d) descrivere le **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.

4.Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere **fornite in fasi successive** senza ulteriore ingiustificato ritardo.

5.Il titolare del trattamento **documenta** qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Data Breach (artt. 33-34)

1.Quando la violazione dei dati personali è suscettibile di presentare un **rischio elevato** per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo

2.La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un **linguaggio semplice e chiaro** la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

3.**Non è richiesta la comunicazione all'interessato** di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

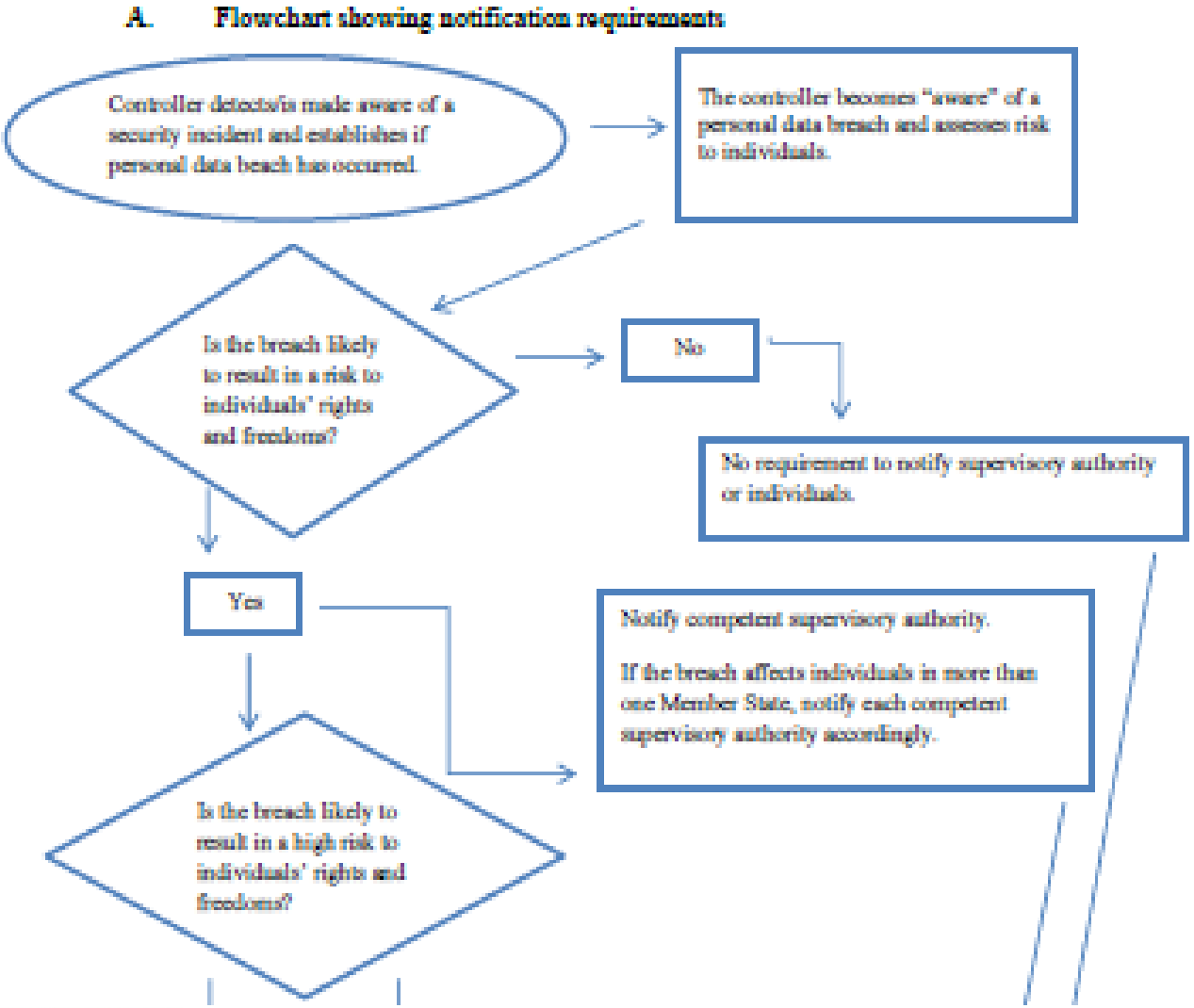
a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere **i dati personali incomprensibili** a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) 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;

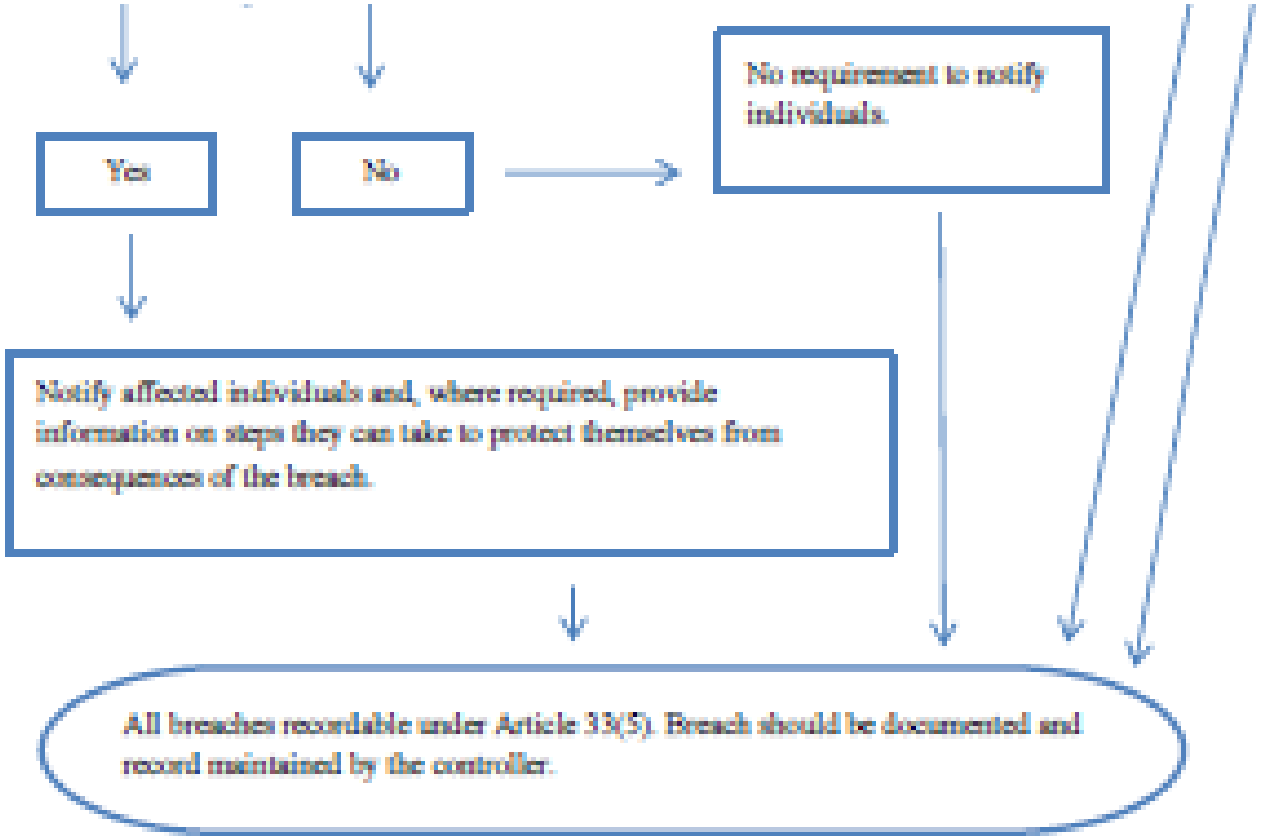
c) detta comunicazione richiederebbe **sforzi sproporzionati**. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

4.Nel caso in cui il titolare del trattamento **non abbia ancora comunicato** all'interessato la violazione dei dati personali, **l'autorità di controllo può richiedere**, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta

Data Breach (artt. 33-34)



Data Breach (artt. 33-34)



DPIA (art. 35)

1.Quando un tipo di trattamento, allorché prevede in particolare **l'uso di nuove tecnologie**, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un **rischio elevato** per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. **Una singola valutazione** può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

2.Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, **si consulta con il responsabile della protezione dei dati**, qualora ne sia designato uno.

3.La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:

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

b) il **trattamento, su larga scala**, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o

c) la **sorveglianza sistematica su larga scala** di una zona accessibile al pubblico.

4.L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.

5.L'autorità di controllo **può** inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.

DPIA (art. 35)

7.La valutazione contiene almeno:

a) una **descrizione sistematica dei trattamenti** previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della **necessità e proporzionalità** dei trattamenti in relazione alle finalità;
c) una valutazione dei **rischi per i diritti e le libertà degli interessati** di cui al paragrafo 1; e
d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8.Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei **codici di condotta** approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

9.Se del caso, il titolare del trattamento **raccoglie le opinioni degli interessati** o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

DPIA (art. 35)

10.Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), **trovi nel diritto dell'Unione o nel diritto dello Stato membro** cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e **sia già stata effettuata una valutazione d'impatto** sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

11.Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono **variazioni del rischio** rappresentato dalle attività relative al trattamento.

DPIA (art. 36)

1.Il titolare del trattamento, prima di procedere al trattamento, **consulta l'autorità di controllo** qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un **rischio elevato in assenza di misure** adottate dal titolare del trattamento per attenuare il rischio.

2.Se ritiene che il trattamento previsto di cui al paragrafo 1 violi il presente regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, **l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto** al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58. Tale periodo può essere **prorogato di sei settimane**, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini **può essere sospesa** fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.

DPIA (art. 36)

3.Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento **comunica all'autorità** di controllo:

a) ove applicabile, **le rispettive responsabilità** del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;

b) le **finalità e i mezzi** del trattamento previsto;

c) le **misure** e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento;

d) ove applicabile, **i dati di contatto del titolare della protezione dei dati;** 4.5.2016 L 119/54 Gazzetta ufficiale dell'Unione europea IT

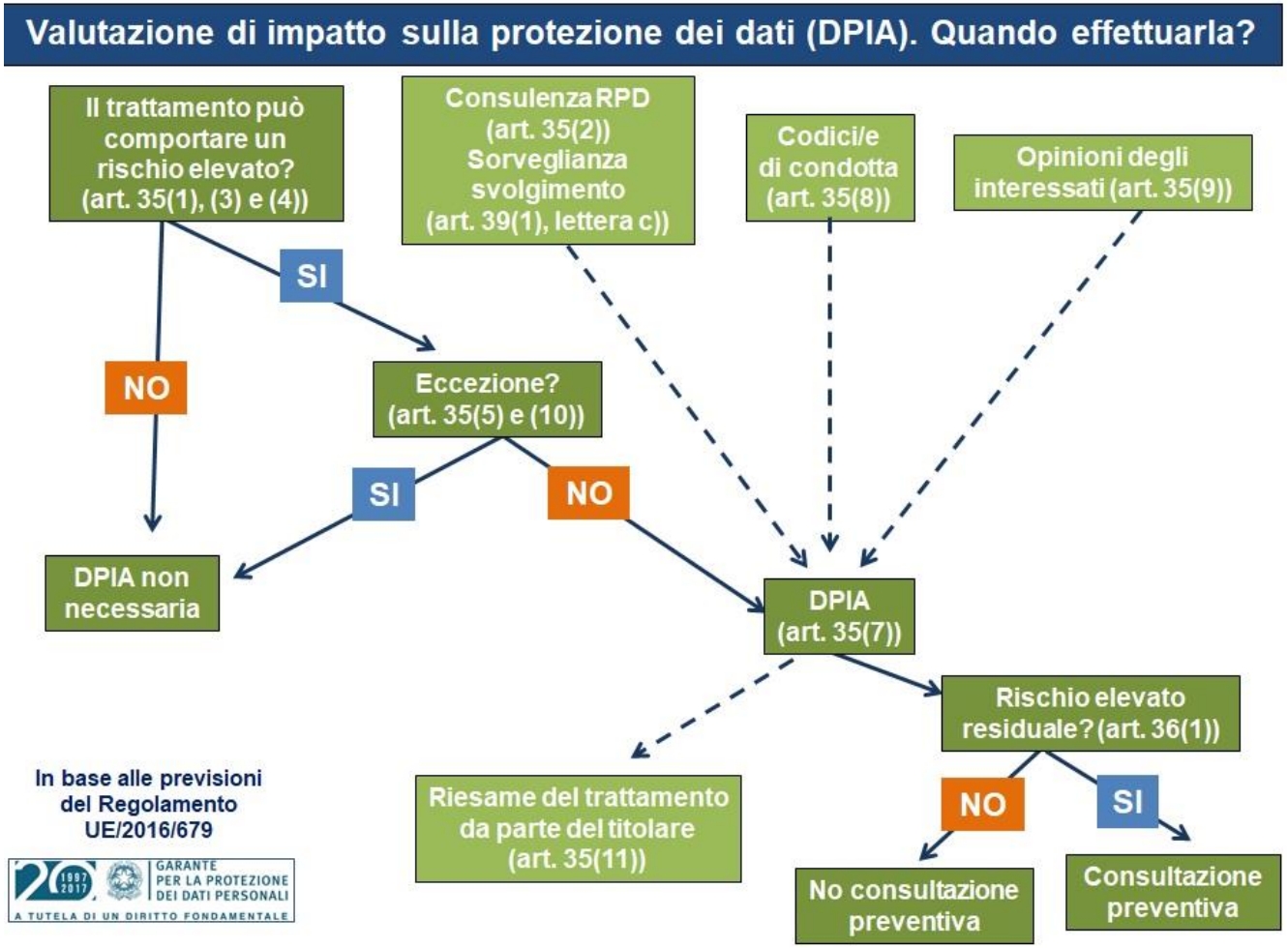
e) **la valutazione d'impatto** sulla protezione dei dati di cui all'articolo 35;

f) ogni altra informazione richiesta dall'autorità di controllo.

4.Gli **Stati membri** consultano l'autorità di controllo **durante l'elaborazione di una proposta di atto legislativo** che deve essere adottato dai parlamenti nazionali o di misura regolamentare basata su detto atto legislativo relativamente al trattamento.

5.Nonostante il paragrafo 1, **il diritto degli Stati membri** può prescrivere che **i titolari** del trattamento **consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare**, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un **compito di interesse pubblico**, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica.

DPIA (artt. 35 - 36)



Formazione IFEL
per i Comuni

IFEL
Fondazione ANCI

Grazie per l'attenzione

Giuseppe D'Acquisto

I materiali didattici saranno disponibili su
www.fondazioneifel.it/formazione

Twitter Facebook YouTube