Epicentro italia srl
Via Aldo Moro, 48
25124 Brescia

Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali (seconda parte)

14 APRILE 2018

CONSIGLIO NAZIONALE DELLA F.N.O.V.I

DALLE MISURE MINIME ALL

Il Regolamento Europeo chiede alle organizzazioni di stabilire misure IDONEE a tutela e sicurezza delle banche dati.

A differenza del D.lgs 196/03, il regolamento non stabilisce un elenco di misure minime di sicurezza ma affida alle organizzazioni la responsabilità di identificare opportune cautele in funzione dei propri rischi.

COME DETERMINARE MISURE IDONEE

Le misure dunque devono tenere conto:

a. Dello stato dell'arte dell'organizzazione;
b. Dei costi di attuazione;
c. Della natura, oggetto, contesto e finalità di trattamento;
d. Probabilità e gravità del rischio per i diritti e le libertà delle persone fisiche

Le misure possono essere:

- Tecniche
- Organizzative

LE MISURE TECNICHE E GEN ONE DEI RISCHI ART. 32 REG.

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.

COSA E' IL RISCHIO?

Innanzitutto: COSA SI INTENDE PER RISCHIO?

Per rischio si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità.

Quando esiste la probabilità di un rischio elevato, per l'art.35 del regolamento?

Nel momento in cui il trattamento «*può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*»

D'altro canto, la "**gestione del rischio**" è definibile come l'insieme coordinato delle attività finalizzate a guidare e monitorare un ente o organismo nei riguardi di tale rischio.

ANALIZZARE I RISCHI

In che modo quantificare il rischio?

Esposizione = probabilità x danno

- **probabilità di accadimento della minaccia rilevata** (la probabilità è legata anche all'esistenza o meno di strumenti di controllo/regole atti a prevenire il verificarsi della minaccia rilevata)

- danno inteso come danno materiali o immateriale all'interessato derivante dal verificarsi dell'evento considerato a rischio.

probabilità	**alta (3)**	**3**	**6**	**9**
	media (2)	2	4	6
	bassa (1)	1	2	3
		minimo (1)	medio (2)	significativo(3)
		danno		

- **Significativo -> Azione urgente**
- **Medio -> Azione richiesta**
- **Minimo -> Monitor**

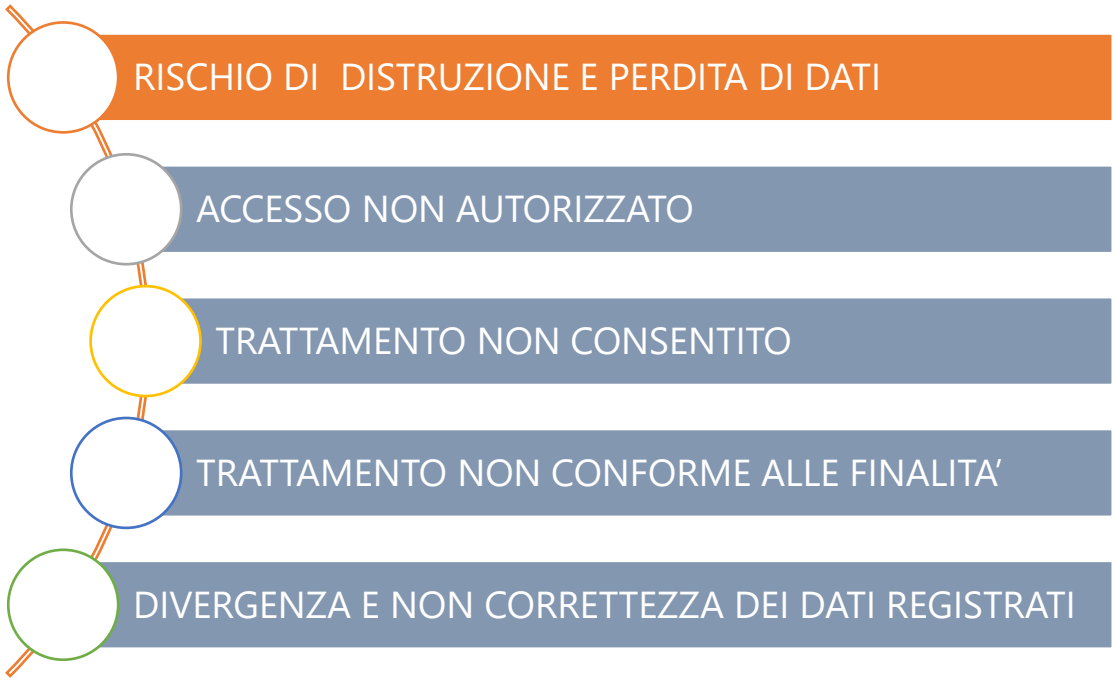
I 5 POSSIBILI RISCHI

- RISCHIO DI DISTRUZIONE E PERDITA DI DATI
- ACCESSO NON AUTORIZZATO
- TRATTAMENTO NON CONSENTITO
- TRATTAMENTO NON CONFORME ALLE FINALITA'
- DIVERGENZA E NON CORRETTEZZA DEI DATI REGISTRATI

RISCHIO N. 1 DISTRUZIONE E PERDITA DEI DATI

Il titolare del trattamento deve assicurare la conservazione, l'integrità e la disponibilità dei dati personali trattati, adottando idonee procedure aziendali in grado di prevenire i rischi – intenzionali od accidentali – di distruzione o di perdita dei dati.

.



Quali eventi possono portare alla distruzione e perdita dei dati? Quali conseguenze?

Quali MISURE DI MITIGAZIONE DEL RISCHIO IMPLEMENTATE?

QUALE RISCHIO RESIDUO?

QUALI MISURE DI MIGLIORAMENTO?

RISCHIO N.1 DISTRUZIONE E PERDITA DEI DATI

EVENTI ACCIDENTALI CONTEMPLATI

- Eventi distruttivi, naturali o artificiali (quali ad esempio movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali…)
- Guasto ai sistemi complementari (quali ad esempio problemi all'impianto elettrico o di climatizzazione)
- Malfunzionamento, indisponibilità o degrado degli strumenti elettronici (quali ad esempio casi di danneggiamento di hard disk o processori)
- Carenza di consapevolezza, disattenzione o incuria (quali lo smarrimento di documenti)

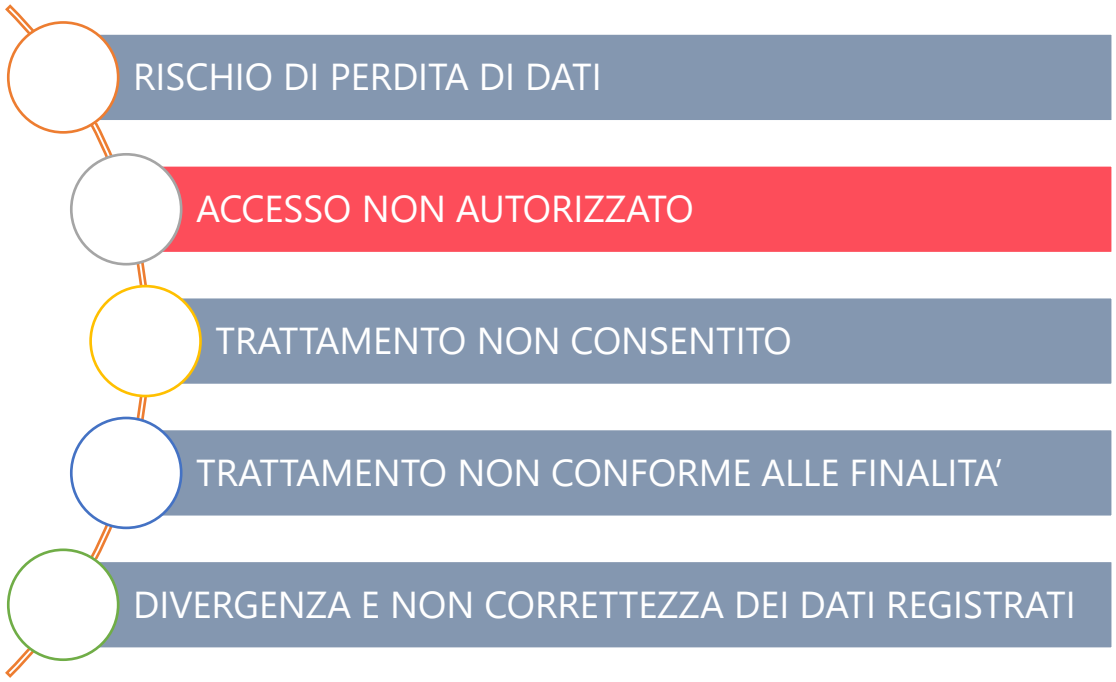
RISCHIO N.1 DISTRUZIONE E PERDITA DEI DATI

EVENTI INTENZIONALI CONTEMPLATI

- Comportamenti sleali o fraudolenti (quali ad esempio distruzione volontaria di documenti da parte del personale dipendente o collaboratori)
- Azione di virus informatici o di programmi suscettibili a recare danni (quali ad esempio l'installazione di virus in grado di alterare o cancellare i dati personali presenti in un data base);
- Sottrazione di strumenti contenenti dati o documentazione cartacea (quali ad esempio furto di supporti removibili contenenti dati sensibili)

Rischio n. 2 ACCESSO NON AUTORIZZATO

Il titolare del trattamento deve predisporre delle misure di sicurezza che garantiscano l'accesso agli archivi (cartacei e informatici) contenenti dati personali, esclusivamente a persone da lui preventivamente autorizzate.



Quali eventi possono portare all'accesso non autorizzato? Quali conseguenze?

Quali MISURE DI MITIGAZIONE DEL RISCHIO IMPLEMENTATE?

QUALE RISCHIO RESIDUO?

QUALI MISURE DI MIGLIORAMENTO?

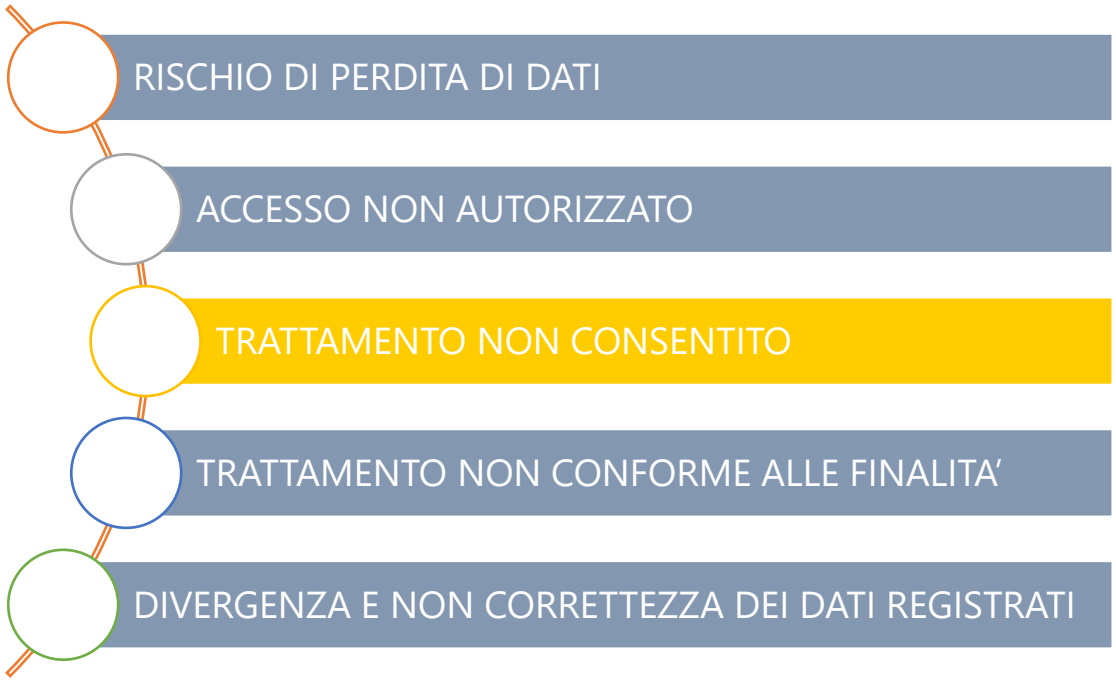
EVENTI CONTEMPLATI

Rischio n.2 ACCESSO NON AUTORIZZATO

- Sottrazione delle credenziali di autenticazione, ovvero di login e password
- Carenza di consapevolezza, di disattenzione o incuria nella gestione degli accessi (quale ad esempio il lasciare aperto un archivio riservato ad accesso selezionato)
- Comportamenti sleali o fraudolenti da parte del personale (quali ad esempio il consegnare copia delle chiavi di uffici o ad archivi a personale della concorrenza);
- Errori materiali ed umani nella gestione della sicurezza fisica (quali ad esempio non aver attivato il sistema dall'allarme prima della chiusura degli uffici)
- Tecniche di sabotaggio (quali ad esempio l'installazione di software malevolo al fine di accedere al sistema informatico);
- Ingressi non autorizzati a locali o reparti ad accesso ristretto (quali ad esempio l'elusione del sistema di gestione degli accessi aziendali)

Rischio n. 3 TRATTAMENTO NON CONSENTITO: Aggiunte, soppressioni o modifiche dei dati non autorizzate

Il titolare del trattamento dovrà procedere ad instaurare delle misure volte a garantire la CONFIDENZIALITÀ DEI DATI ovvero studiate appositamente per prevenire il rischio di aggiunte, soppressioni o modifiche dei dati non autorizzate.



Quali eventi possono portare al trattamento non consentito? Quali conseguenze?

Quali MISURE DI MITIGAZIONE DEL RISCHIO IMPLEMENTATE?

QUALE RISCHIO RESIDUO?

QUALI MISURE DI MIGLIORAMENTO?

EVENTI

- Disattenzione o incuria nel trattamento (come ad esempio nel caso di dimenticanza di cancellazione di tutti i file contenenti dati personali oggetto della richiesta di un interessato);

- Errori materiali e umani nel trattamento (invio di una mail ad un indirizzo di destinatario errato);

- Intercettazione di informazioni in rete, accessi non autorizzati al sistema informatico o spamming (come ad esempio nel caso di trattamento illecito di dati personali da parte di hackers)

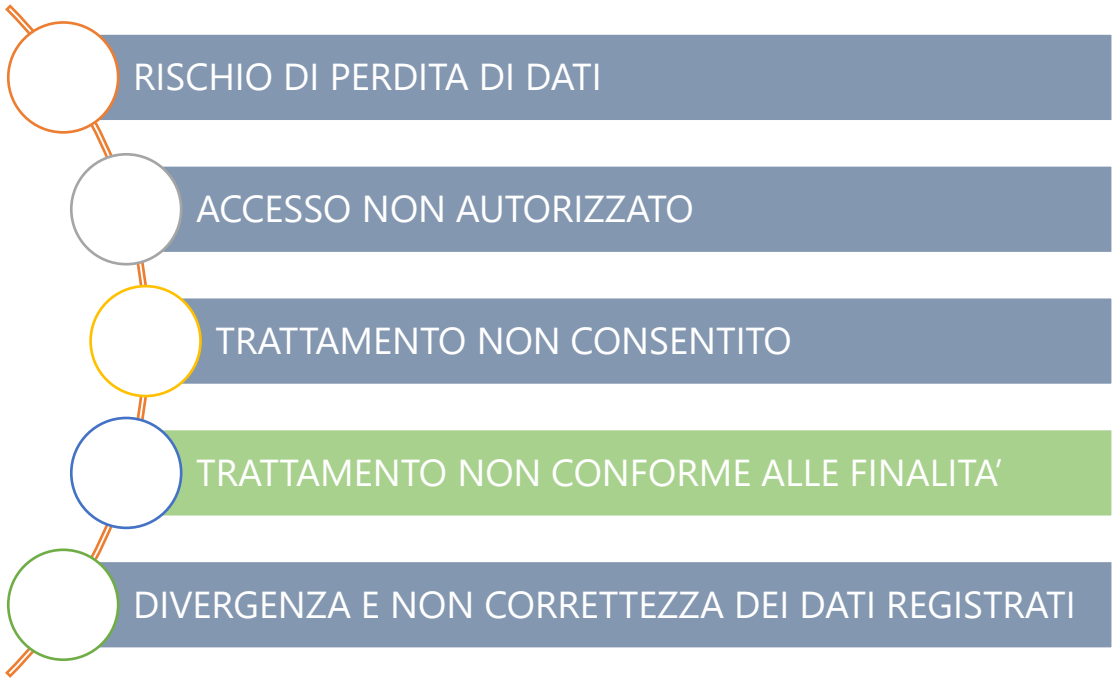
- Sottrazione di strumenti contenenti dati (come ad esempio nel caso di trattamento illecito di dati personali inseguito a furto di una copia di backup)

- Manipolazione delle informazioni acquisite

- Diffusione di dati sensibili

Rischio n. 4 TRATTAMENTO NON CONFORME ALLE FINALITA'

Il titolare deve garantire che il trattamento dei dati raccolti sia sempre effettuato secondo le finalità dichiarate e comunicate all'interessato nell'informativa e sia limitato solamente ai dati per i quali il titolare abbia ricevuto libero ed espresso consenso al trattamento.



Quali eventi possono portare al trattamento non conforme alle finalità? Quali conseguenze?

Quali MISURE DI MITIGAZIONE DEL RISCHIO IMPLEMENTATE?

QUALE RISCHIO RESIDUO?

QUALI MISURE DI MIGLIORAMENTO?

Rischio n. 4 TRATTAMENTO NON CONFORME ALLE FINALITA'

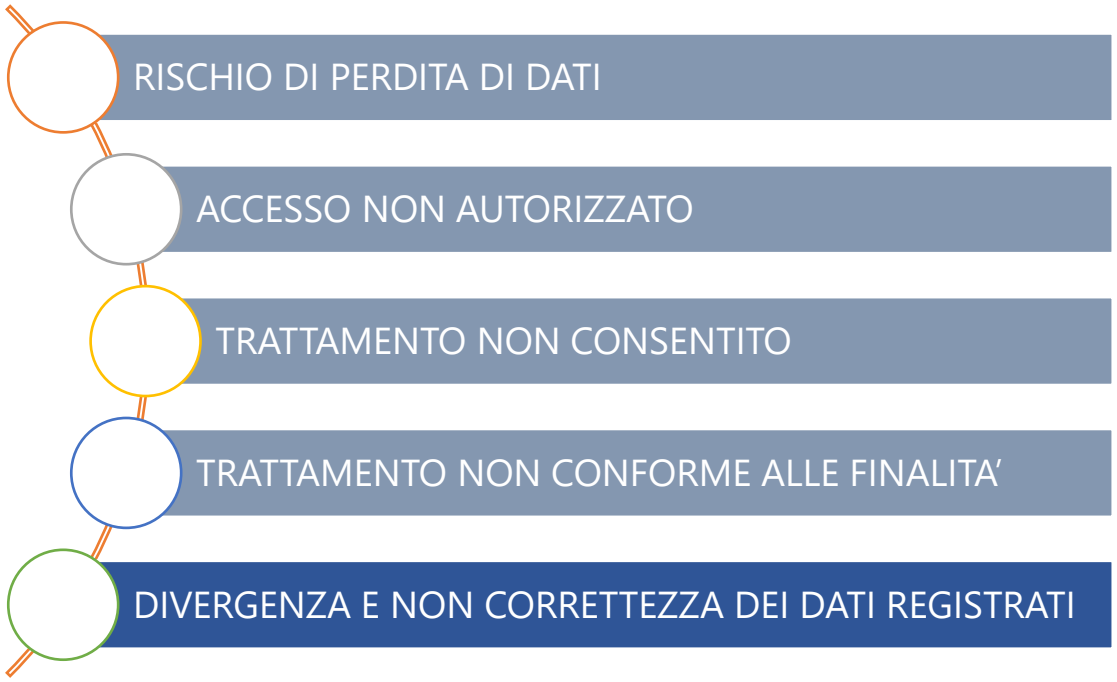
Il titolare deve garantire che il trattamento dei dati raccolti sia sempre effettuato secondo le finalità dichiarate e comunicate all'interessato nell'informativa e sia limitato solamente ai dati per i quali il titolare abbia ricevuto libero ed espresso consenso al trattamento.

EVENTI

- Operazioni non autorizzate dall'interessato;
- Operazioni non pertinenti rispetto alle finalità del trattamento concordate

Rischio n. 5 DIVERGENZA E NON CORRETTEZZA DEI DATI REGISTRATI

Il titolare deve garantire la correttezza e completezza dei dati registrati.



Quali eventi possono portare errori nella registrazione? Quali conseguenze?

Quali MISURE DI MITIGAZIONE DEL RISCHIO IMPLEMENTATE?

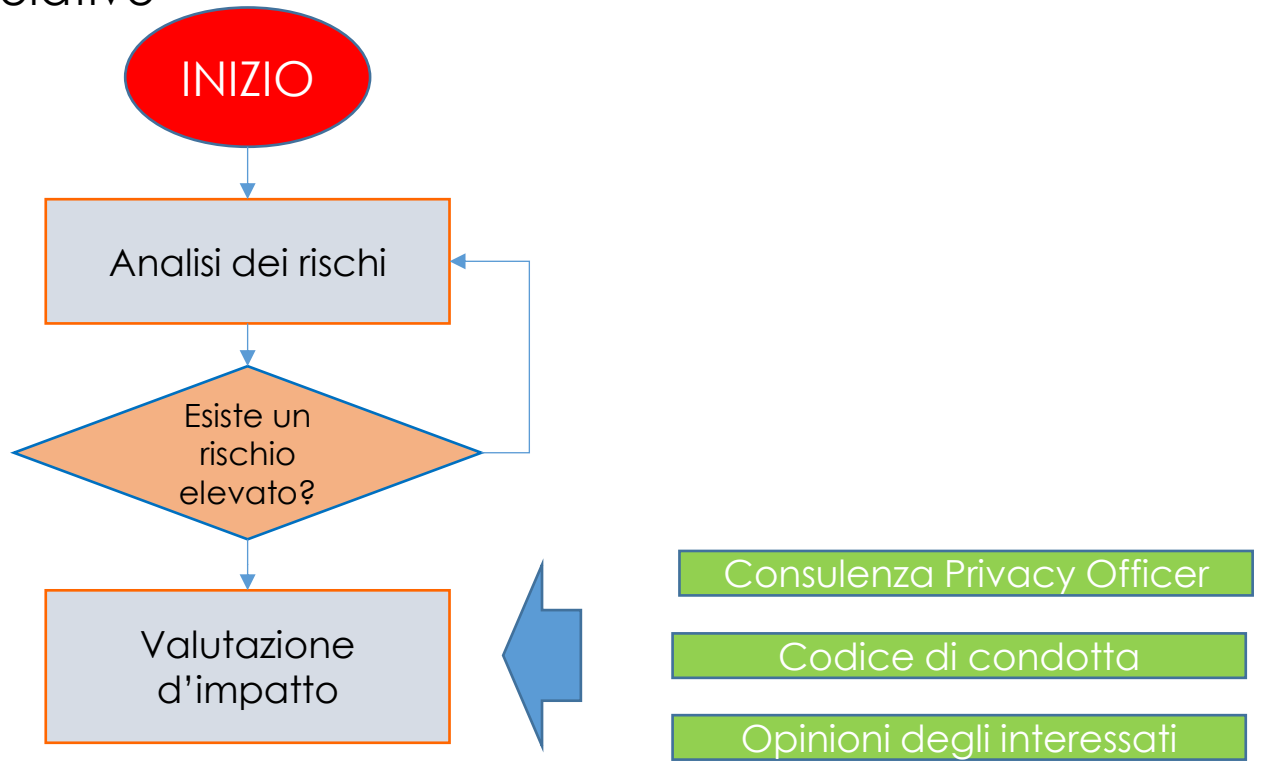
QUALI MISURE DI MIGLIORAMENTO?

QUALE RISCHIO RESIDUO?

Valutazione d'impatto

La valutazione d'impatto consiste in un processo volto a:

- Descrivere i trattamenti previsti e le relative finalità,
- Valutarne la necessità e la proporzionalità
- Gestire i rischi,
- determinare le misure più idonee
- dimostrare la conformità al regolamento



VALUTAZIONE D'IMPATTO SULLA PRO

LA VALUTAZIONE DI IMPATTO E' ESEGUITA OBBLIGATORIAMENTE NEI SEGUENTI CASI:

1. quando si ha 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;
2. nel momento in cui si trattano, su larga scala, categorie particolari di dati personali, o dati relativi a condanne penali e reati
3. nei casi in cui si ha una sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

QUANDO FARE LA VALUTAZ
CRITERI

	Descrizione	Esempi
1. Trattamenti valutativi o di scoring, compresa la profilazione e attività predittive	A partire da aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato	Screening finanziario dei clienti utilizzando rischio creditizio, Database per la lotta alle frodi, riciclaggio e finanziamento del terrorismo. Test genetici sui consumatori di aziende del settore biotecnologie; Una società che crei profili comportamentali o di marketing sul web
2. Decisioni automatizzate che producono significativi effetti giuridici o di analoga natura		Casellario giudiziario
3. Monitoraggio sistematico	Trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta attraverso le reti o «la sorveglianza sistematica di un'area accessibile al pubblico.	
4. Dati sensibili o dati di natura estremamente personale		Cartelle cliniche di pazienti, appunti agende

	Descrizione	Esempi
5. Trattamenti di dati su larga scala	- Numero interessati; - Volume di dati; - Durata; - Ambito geografico	
6. Combinazione o raffronto di insiemi di dati	Due trattamenti gestiti da titolari distinti secondo modalità che esulano dalle ragionevoli aspettative dell'interessato	
7. Dati relativi a interessati vulnerabili	La categoria degli interessati vulnerabili comprende anche minori, che si può ritenere non sia in grado di opporsi o acconsentire	Psichiatrici, Richiedenti asilo, anziani, pazienti, bambini
8. Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative		Internet delle cose
9. Tutti trattamenti che impediscono poi di fatto di esercitare un diritto o di avvalersi di un servizio o di un contratto	Ciò comprende i trattamenti finalizzati a consentire, modificare o negare l'accesso degli interessati a un servizio o la stipulazione di un contratto	Flusso alla centrale dei rischi

QUANDO NON E' NECESSA VALUTAZIONE D'IMPATTO?

- Quando non può comportare un rischio elevato
- Esiste una Valutazione d'Impatto simile
- Quando il trattamento è stato autorizzato prima del maggio 2018
- Quando ha una base legale
- Quando NON è compreso nella lista dei trattamenti che prevedono la VI

CONTENUTI MINIMI DELLA TO

PRIMA PARTE: DESCRIZIONE SISTEMATICA DEL TRATTAMENTO

- Natura, contesto e finalità
- Interessati, destinatari e periodo di conservazione
- Descrizione funzionale
- Strumenti coinvolti nel trattamento
- Osservanza di codici di condotta approvati

SECONDA PARTE: VALUTAZIONE NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

- Misure che determinano la liceità del trattamento;
- Misure che contribuiscono ai diritti degli interessati

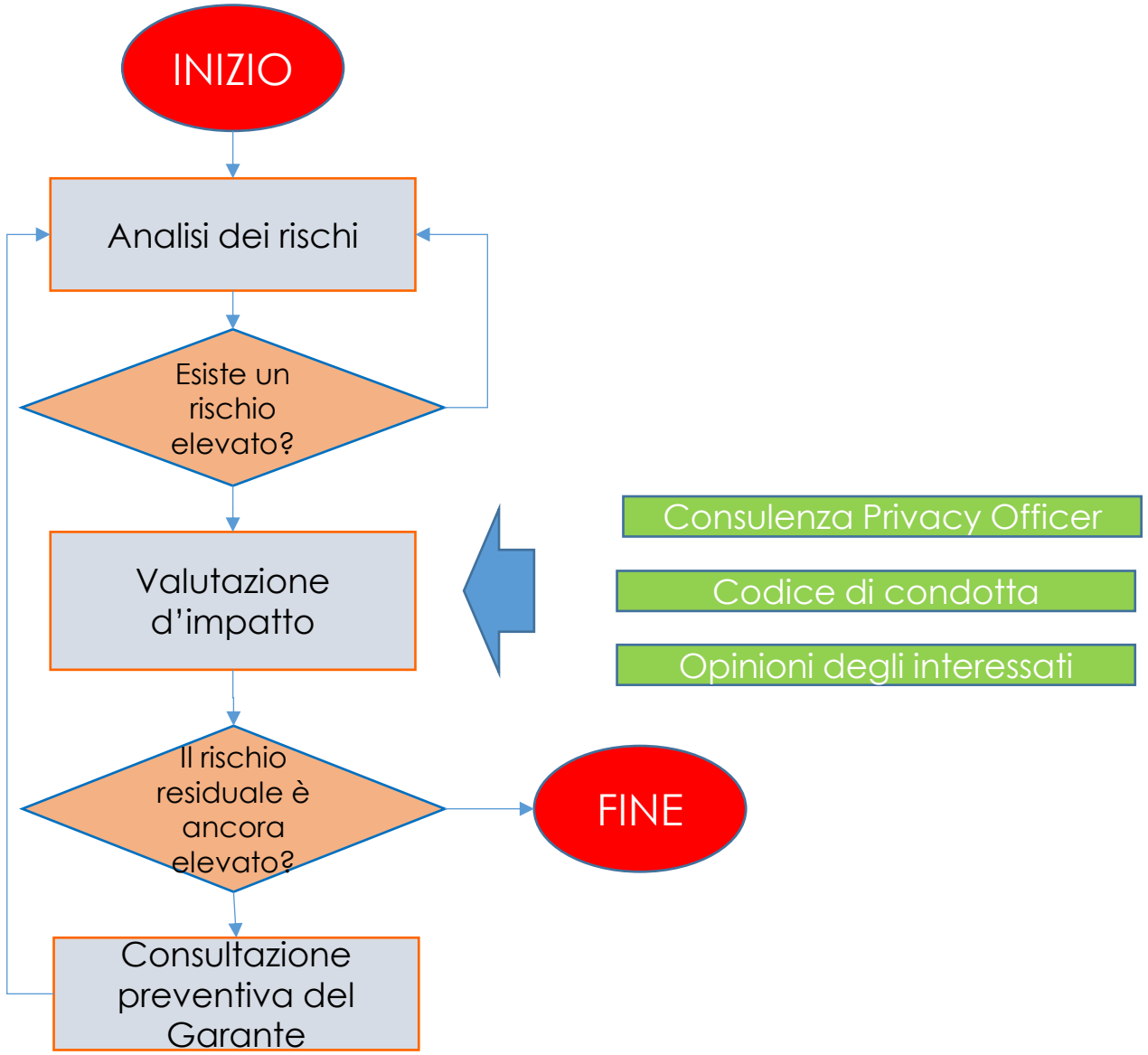
TERZA PARTE: GESTIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI

- Origine, natura, particolarità e gravità dei rischi (es. accesso illegittimo, modifiche indesiderate, indisponibilità dei dati), dal punto di vista degli interessati
- Misure previste per gestire i rischi

QUARTA PARTE: COINVOLGIMENTO DEI SOGGETTI INTERESSATI

- Consulenza Privacy Officer
- Consulenza interessati o rappresentanti

RIESAME DEL TRATTAMENTO DEL TITOLARE



LA CONSULTAZIONE PREVE

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

Al momento di consultare il Garante, il Titolare del trattamento gli comunica:

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);

a) le finalità e i mezzi del trattamento previsto;

c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati

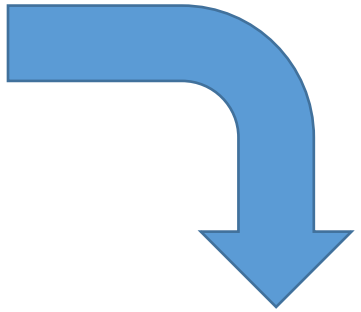
d) ove applicabile, i dati di contatto del **Responsabile della protezione dei dati**;

e) la valutazione d'impatto sulla protezione dei dati e ogni altra informazione richiesta dal Garante

LA VIOLAZIONE DEI DATI PERSONALI

Che cos'è una violazione?

"Una violazione della sicurezza dei dati è un evento che porta alla distruzione accidentale o illecita, perdita, alterazione, divulgazione non autorizzata o accesso a dati personali trasmessi, archiviati o altrimenti elaborati."



1. "Violazione della riservatezza" - in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali.
2. "Violazione dell'integrità": in caso di alterazione non autorizzata o accidentale dei dati personali.
3. "Violazione della disponibilità" - in caso di perdita accidentale o non autorizzata di accesso o distruzione di dati personali.

NOTIFICAZIONE DELLA VIO
33 Reg.

1. **DOCUMENTARE** tutte le violazioni;

2. **NOTIFICARE** la violazione all'autorità garante **SENZA INGIUSTIFICATO RITARDO** e, ove possibile, entro 72 ore.

3. **COMUNICARE, IN LINEA GENERALE, LA VIOLAZIONE ALL'INTERESSATO** senza ingiustificato ritardo, salvo eccezioni.

NOTIFICAZIONE DELLA VIO
33 Reg.

COMUNICA, IN LINEA GENERALE, LA VIOLAZIONE ALL'INTERESSATO

*Eccezioni:

1) 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

2) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato

3) detta comunicazione richiederebbe sforzi sproporzionati

NOTIFICAZIONE DELLA VIO
33 Reg.

CONTENUTI DELLA NOTIFICAZIONE

1) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati
2) I dati di contatto del responsabile della protezione dei dati o di altro punto di contatto
3) descrivere le probabili conseguenze della violazione dei dati personali
4) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento

SANZIONI

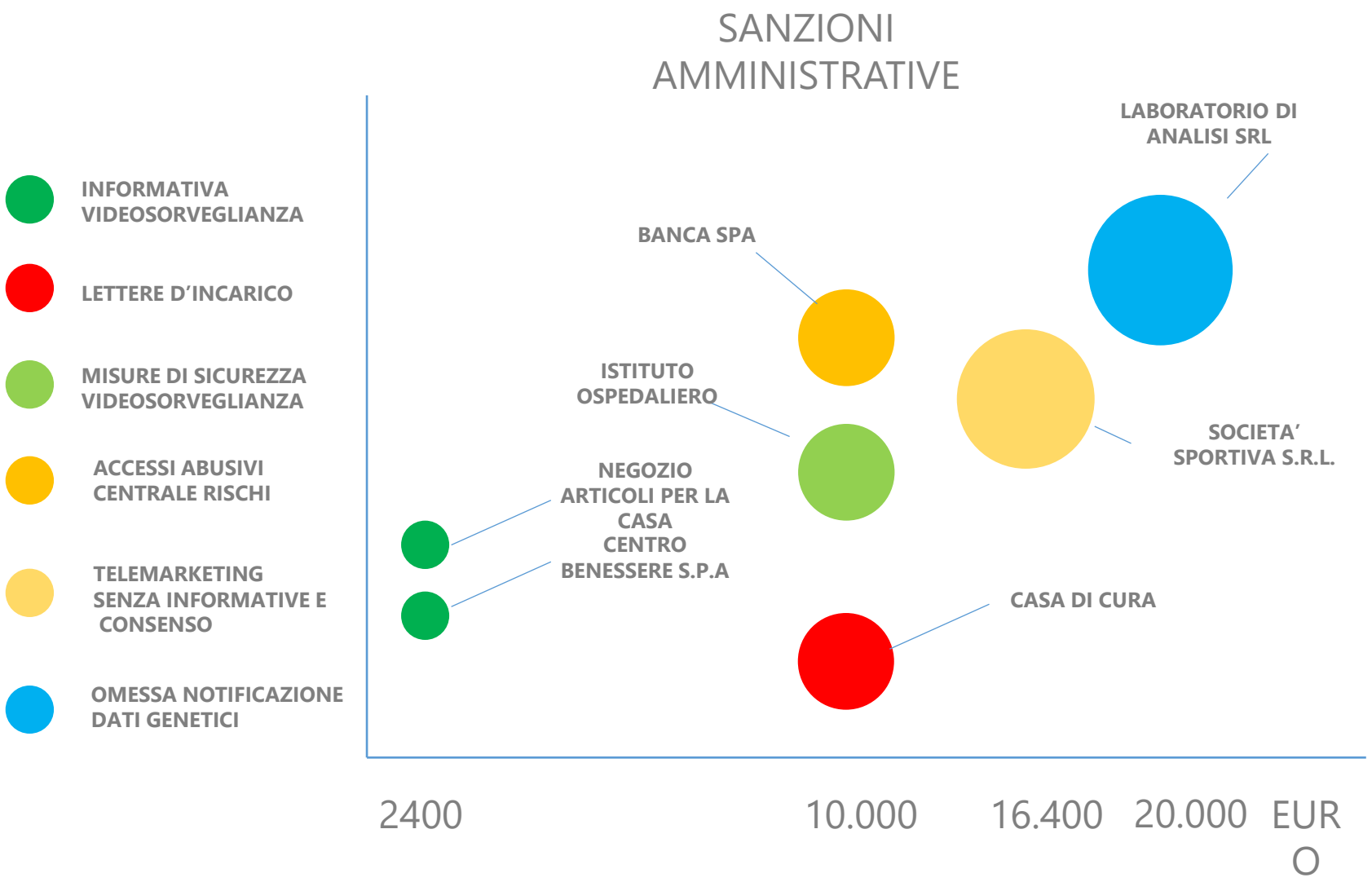
NUOVO PIANO SANZIONATORIO

Il regolamento prevede due forme di sanzioni: amministrativa, e in taluni casi penale.

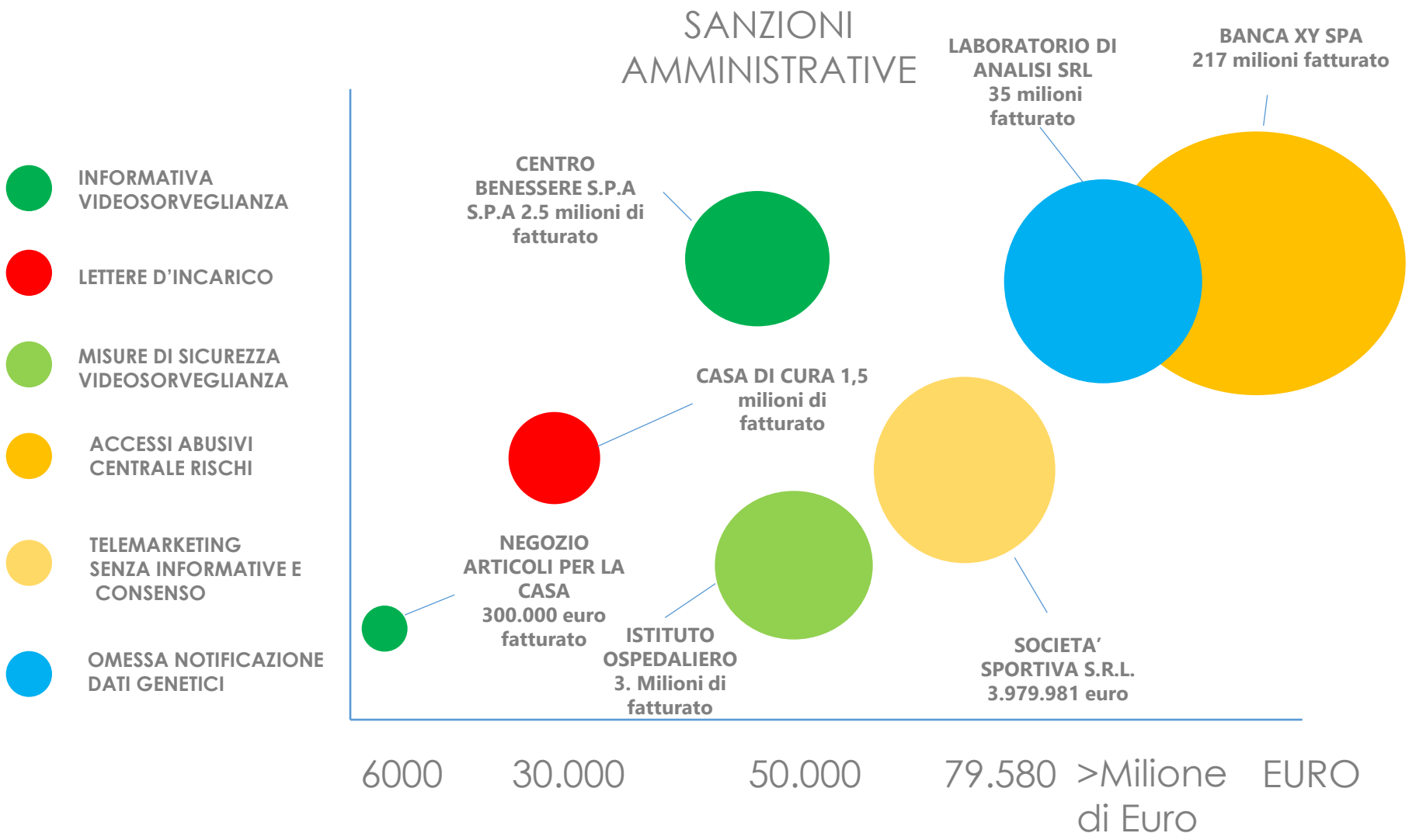
Le sanzioni amministrative sono generalmente di tipo pecuniario, e possono prevedere multe sino al 2% o 4% del fatturato mondiale dell'esercizio precedente, se superiore.

Le sanzioni penali sono stabilite in base alle disposizioni di ciascun Stato Membro.

ESITO DEI CONTROLLI



ESITO DEI CONTROLLI SINC



I CRITERI

a) la natura, la gravità e la durata della violazione

b) il carattere doloso o colposo della violazione

c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;

d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative;

e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;

f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

g) le categorie di dati personali interessate dalla violazione;

h) 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;

i) 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;

j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42;

k) 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.