FICOG | Federation of Italian Cooperative Oncology Groups

GIDM Coordinatori di Ricerca Clinica
Gruppo Italiano Data Manager

UTILIZZO DEI DATI IN RICERCA CLINICA.
COME DESTREGGIARSI NEI VINCOLI DELLA NORMATIVA PRIVACY

Milano 14 aprile 2023

Gestione e responsabilità di un Data Breach

Relatore: Raffaella Elia

- Riferimenti normativi -

- **GDPR, Regolamento generale sulla protezione dei dati, Regolamento (UE) n. 2016/679** (GUUE del 4.05.2016, L119/1)

- **WP250, "Guidelines on personal data breach notification under Regulation 2016/679" del 3.10.2017/ "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679**", rev. 01, versione emendata ed adottata in data 6 febbraio 2018 (dal Gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali, istituito ai sensi dell'art. 29 della direttiva 95/46/CE), aggiornate dalle recenti "**Guidelines 9/2022 on personal data breach notification under GDPR**", **versione 2.0, adottata il 28 marzo 2023 dall'EDPB**, a seguito di consultazione pubblica conclusa in data 29 novembre 2022

- **WP260, "Guidelines on transparency under Regulation 2016/679"/ "Linee guida sulla trasparenza ai sensi del Regolamento 2016/679**" del 29 novembre 2017, versione emendata adottata l'11 aprile 2018 (dal Gruppo "Articolo 29")

- **Codice in materia di protezione dei dati personali,** D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (GU n. 205 del 4.09.2018)

- “**Linee-guida 01/2021** su esempi riguardanti la notifica di una violazione dei dati personali” adottate il 14 dicembre 2021, previa consultazione pubblica, dall’EDPB, European Data Protection Board/Comitato Europeo per la protezione dei dati

- ed in materia di sperimentazioni cliniche? -

- Parere 3/2019 dell’EDPB sull’interazione tra GDPR e Reg, n. 536/2014

- Bozza di linee guida EMA sulla trasparenza delle informazioni caricate sul Clinical Trial Information System (CTIS) del 7 aprile 2022

- Normative di attuazione del GDPR (l. 3/2018; d.lgs. n. 52/2019; D.M. 30.11.2021) non contengono disposizioni specifiche in materia di trattamento dei dati personali nell’ambito delle sperimentazioni cliniche e quindi…

- “**Linee guida per i trattamenti di dati personali nell’ambito delle sperimentazioni cliniche di medicinali**” (G.U. n. 190 del 14 agosto 2008), Deliberazione n. 52 del 24 luglio 2008 del Garante per la protezione dei dati personali

- ***Definizione*** -

- Articolo 4 ***GDPR***, "***Definizioni***":

"...12) *«violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*..."

- Nelle **linee guida WP250** e **9/2022** le violazioni sono state classificate in base ai seguenti principi di sicurezza delle informazioni:

1) **violazione della riservatezza**: in caso di divulgazione non autorizzata o accidentale di dati personali o di accesso non autorizzato o accidentale agli stessi;

2) **violazione dell'integrità**: in caso di modifica non autorizzata o accidentale di dati personali;

3) **violazione della disponibilita'**: in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali (esempio: dati cancellati accidentalmente o da persona non autorizzata oppure in casi di dati crittografati in maniera sicura quando la chiave di decifratura viene persa ed il titolare non è in grado di ripristinare l'accesso ai dati, ad esempio, ricorrendo ad un backup, la perdita di disponibilità sarà considerata permanente).

- ***Alcuni esempi individuati dal Garante***:

- l’accesso o l’acquisizione dei dati da parte di terzi non autorizzati;

- perdita di riservatezza a seguito dell’invio di una mail contenente dati personali a un destinatario errato;

- il furto o la perdita di dispositivi informatici o supporto di memorizzazione contenenti dati personali;

- la deliberata alterazione di dati personali;

- l’impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;

- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;

- la divulgazione non autorizzata dei dati personali

Nozione ampia: tutte le ipotesi di trattamento illegittimo compiuto in modo fraudolento o causale da parte di un terzo che acceda a dati personali trattati dal titolare o anche per fatti indipendenti dalla volontà di un soggetto oppure trattamenti illegittimi riconducibili ad una condotta del titolare anche omissiva → occorre dunque valutare le **condizioni oggettive** in cui si verifica la violazione.

- ***Principi fondamentali*** -

ACCOUNTABILITY* = *responsabilizzazione del titolare del trattamento

Cosa vuol dire?

Viene affidato al titolare il compito (e la responsabilità) di determinare in autonomia modalità, garanzie e limiti del trattamento dei dati personali, nel rispetto del Regolamento e delle disposizioni normative nazionali e responsabilità di adozione di comportamenti proattivi tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento.

Articolo 25 GDPR

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

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.

Linee guida del 2008

"***12 Custodia e sicurezza dei dati***...*La particolare delicatezza dei dati trattati nella sperimentazione impone l'adozione di specifici accorgimenti tecnici per incrementare il livello di sicurezza dei dati (art. 31 del Codice), senza pregiudizio di ogni altra misura minima che ciascun titolare del trattamento deve adottare ai sensi del Codice (art. 33 e ss.). Ciò, con particolare riferimento alle operazioni di registrazione con strumenti elettronici dei dati delle persone coinvolte nello studio presso i centri di sperimentazione, al loro trasferimento in via telematica verso un unico database presso il promotore o gli altri soggetti che svolgono, per conto di quest´ultimo, la validazione e l'elaborazione statistica dei dati, nonché alla gestione della medesima banca dati.*

In relazione a tali operazioni di trattamento, i promotori di sperimentazioni cliniche di medicinali, le organizzazioni di ricerca a contratto e i centri di sperimentazione, ciascuno per la parte di propria competenza in relazione al ruolo ricoperto nel trattamento dei dati e alle conseguenti responsabilità ai fini dell´adozione delle misure di sicurezza, devono adottare:

a. laddove siano utilizzati sistemi di memorizzazione o archiviazione dei dati, idonei accorgimenti per garantire la protezione dei dati registrati dai rischi di accesso abusivo, furto o smarrimento parziali o integrali dei supporti di memorizzazione o dei sistemi di elaborazione portatili o fissi (ad esempio, attraverso l´applicazione parziale o integrale di tecnologie crittografiche a file system o database, oppure tramite l´adozione di altre misure informatiche di protezione che rendano inintelligibili i dati ai soggetti non legittimati);

b. protocolli di comunicazione sicuri basati sull´utilizzo di standard crittografici per la trasmissione elettronica dei dati raccolti dai centri di sperimentazione al database centralizzato presso il promotore o gli altri soggetti che effettuano la successiva validazione ed elaborazione statistica dei dati;

c. con specifico riferimento al menzionato database:

- idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e trattamento;

- procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli incaricati del trattamento;

- sistemi di audit log per il controllo degli accessi al database e per il rilevamento di eventuali anomalie.

Il Garante si riserva, in relazione alle sperimentazioni cliniche multinazionali, di promuovere a livello comunitario e internazionale standard di sicurezza per i trattamenti di dati personali che prevedano un livello di protezione ancora più elevato in un quadro di armonizzazione delle misure e degli accorgimenti da adottare in tali ambiti per la custodia e la sicurezza dei dati".

…**obbligo di codificare** i dati personali/particolari dei partecipanti allo studio con tenuta soltanto nella disponibilità del Centro della lista che consente di associare il codice identificativo assegnato al nominativo dell'interessato:

"***3. Natura dei dati trattati*** *I promotori hanno sviluppato in genere specifiche procedure interne per consentire ai medici sperimentatori di codificare i dati medico/clinici delle persone coinvolte nello studio: solitamente, si utilizzano codici numerici che consentono di identificare univocamente i singoli interessati all´interno dello stesso studio, senza utilizzare il nominativo, l´indirizzo o numeri di identificazione personale….previsto che soltanto ciascun centro abbia la disponibilità della lista che consente di associare il nominativo della persona al relativo codice identificativo e che il promotore non debba venire a conoscenza della sua identità…*".

Il ***GDPR*** ha definito la misura di sicurezza della pseudonimizzazione, ***ex art. 4, punto 5)***:

"***«pseudonimizzazione»****: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile"* = sostituzione delle informazioni identificative con degli indicatori generati, di solito ma non solo, mediante algoritmi.

Altra misura menzionata nell'***art. 32 del GDPR*** è la "***cifratura"*** o **crittografia**: può essere simmetrica o asimmetrica ed è una procedura che rende il dato indecifrabile e che potrà essere nuovamente decifrato solo da coloro che possiedono la chiave di conversione, ossia, la combinazione che ha cifrato il dato.

Ricordiamo tuttavia il ***considerando (26) del GDPR***: "*È auspicabile applicare i principi di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile. I dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile…I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca*".

- i dati personali pseudonimizzati possono quindi sempre portare all'identificazione dell'interessato -

Esempio

dato identificativo Luigi Rossi 01/01/1990

dato pseudonimizzato D78F890

dato cifrato fhgf88kl@ff

dato anonimizzato "qualcuno" (statistiche, percentuali, no dati sanitari con i campi delle prime lettere del nome cognome o data di nascita, sesso)

- Adempimenti -
Articolo 33
Notifica di una violazione dei dati personali all'autorità di controllo

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.*

Il titolare, qualora preveda che dalla violazione derivino rischi per i diritti e le libertà degli interessati *deve, senza ritardo e, comunque, entro 72 ore da quando ne sia venuto a conoscenza, darne comunicazione al Garante.

* “***Considerando (85) GDPR*** *Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo”.*

Nelle ***WP250*** e, come confermato nelle ***Guidelines 9/2022***, viene precisato che la conoscenza del data breach decorre dal momento in cui il titolare abbia un certo grado di **certezza =** nel momento in cui il titolare del trattamento sia “*ragionevolmente certo che si è verificato un incidente di sicurezza che ha comportato una compromissione di dati*”.

L’obbligo di comunicazione origina soltanto nel caso in cui risulti **probabile** che la violazione comporti un rischio per i diritti e le libertà degli interessati, pertanto, **la notifica al Garante non è obbligatoria ma è subordinata alla valutazione del rischio per gli interessati che è in capo al titolare del trattamento.**

- Come inviare la notifica al Garante? -

A partire dal 1° luglio 2021, la notifica di una violazione di dati personali deve essere inviata al Garante **dal rappresentante legale del titolare o suo delegato** tramite procedura telematica: *https://servizi.gpdp.it/databreach/s/* (**Provvedimento del 27 maggio 2021, Registro dei provvedimenti n. 209 del 27 maggio 2021**).
Il Garante ha predisposto uno strumento di autovalutazione (***self assessment***) che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza:

1) Si è verificato un incidente di sicurezza che ha comportato la perdita di riservatezza, integrità o disponibilità di dati?

2) L'incidente di sicurezza ha coinvolto dati personali?

3) L'incidente di sicurezza occorso costituisce una violazione dei dati personali?

4) Sei titolare o responsabile del trattamento dei dati personali oggetto di violazione?

Se **responsabile**: occorre informare, senza ingiustificato ritardo, il titolare del trattamento circa la violazione dei dati personali occorsa (***obbligo di comunicazione****). Se l'incidente riguarda dati personali trattati per conto di più titolari, occorre informare ciascun titolare.
WP250 e ***Guidelines 9/2022***: **il responsabile del trattamento non è chiamato a valutare la probabilità che la violazione presenti un rischio per gli interessati.** Il responsabile deve accertare se si è verificata una violazione e in caso positivo notificarla al titolare del trattamento senza ritardo. Nel caso in cui informazioni di dettaglio circa le cause e circostanze della violazione non siano tempestivamente disponibili, il responsabile informa tempestivamente il titolare circa l'avvenuta violazione, comunicando le informazioni di dettaglio in un momento successivo, non appena disponibili.
*l'**art. 28, comma 3, GDPR** dispone che il trattamento da parte di un responsabile del trattamento è disciplinato da un **contratto** o da un altro atto giuridico ed alla let. f) precisa che il contratto o l'atto deve prevedere che il responsabile "***assista il titolare*** *del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento*".

Se **titolare**: è probabile che la violazione presenti un rischio per i diritti e le libertà degli interessati?
Il rischio sussiste quando la violazione può comportare un danno fisico, materiale o immateriale, per le persone fisiche i cui dati sono stati violati.
La **valutazione del rischio** derivante da una violazione dei dati personali, deve tener conto della probabilità e della gravità del suo impatto sulle persone fisiche i cui dati sono stati coinvolti (cfr. **considerando 76 GDPR**: "*La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato*"), è un importante adempimento che, conformemente al principio di responsabilizzazione, **spetta unicamente al titolare del trattamento**.

Parametri oggettivi che il titolare deve valutare per decidere se sia necessaria la notifica all'autorità di controllo:

- tipo di violazione (perdita, distruzione, divulgazione, sottrazione di dati)
- natura, carattere sensibile e volume dei dati personali
- facilità di identificazione delle persone fisiche (assenza di crittografia o di pseudonimizzazione)
- gravità delle conseguenze per le persone fisiche (furto identità, frode, danno fisico, psicologico, danno alla reputazione, violazione di segreto professionale, discriminazione)
- caratteristiche particolari dell'interessato (minori o altri individui vulnerabili)
- caratteristiche particolari del titolare del trattamento (strutture sanitarie, istituti di credito)
- numero di persone fisiche interessate

Se **titolari autonomi**: art. 11.10 del template contrattuale Aifa: "*Qualora una parte accerti una violazione dei dati personali, si impegna a comunicarlo all'altra entro 48 ore dall'accertamento della violazione, ferma restando l'autonomia della stessa nella valutazione della sussistenza delle condizioni e nell'adempimento degli obblighi previsti dagli artt. 33 e 34 del GDPR*".

E se **contitolari**? L'art. **26 GDPR** specifica che essi devono determinare le rispettive responsabilità in merito all'osservanza del Regolamento = accordi contrattuali interni tra contitolari devono includere disposizioni che stabiliscano quale titolare assumerà la gestione o sarà responsabile del rispetto degli obblighi di notifica delle violazioni ai sensi del GDPR, ex artt. 33 e 34.

Ed ancora il titolare dovrebbe domandarsi…

5) La violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche?

Il titolare comunica la violazione all'interessato senza ingiustificato ritardo.

Ricordiamo che il titolare dovrebbe predisporre "*…misure tecnologiche e organizzative adeguate di protezione per* ***stabilire immediatamente*** *se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato…*" ai sensi del **considerando (87) GDPR**.

L'importanza delle misure di protezione è ribadita nel **considerando (88) GDPR**: "*Nel definire modalità dettagliate relative al formato e alle procedure applicabili alla notifica delle violazioni di dati personali, è opportuno tenere debitamente conto delle circostanze di tale violazione, ad esempio* ***stabilire se i dati personali fossero o meno protetti con misure tecniche adeguate di protezione atte a limitare efficacemente il rischio*** *di furto d'identità o altre forme di abuso…*".

Attenzione ai tipi di trattamento che potenzialmente presentano un rischio elevato per i diritti e le libertà delle persone fisiche (es. utilizzo nuove tecnologie, trattamenti di nuovo tipo o su larga scala): "*In tali casi, è opportuno che il titolare del trattamento effettui una* ***valutazione d'impatto sulla protezione dei dati prima del trattamento, per valutare la particolare probabilità e gravità del rischio****, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio…*"

La valutazione d'impatto, infatti, dovrebbe vertere in particolare sulle misure, sulle garanzie e sui meccanismi previsti per attenuare tale rischio assicurando la protezione dei dati personali (**considerando 89, 90 e 91 GDPR**).

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

- ***Contenuto della notifica*** -

Definito nell'**art. 33, comma III, GDPR** e nel "**Provvedimento del Garante sulla notifica delle violazioni dei dati personali" del 30 luglio 2019 (registro dei provvedimenti n. 157 del 30 luglio 2019**).

In particolare, la notifica deve almeno:

- descrivere la natura della violazione occorsa compresi, ove possibile, le categorie e il numero approssimativo di interessati nonché le categorie e il numero approssimativo di registrazioni dei dati personali;

- comunicare il nome e dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;

- descrivere le probabili conseguenze della violazione dei dati personali;

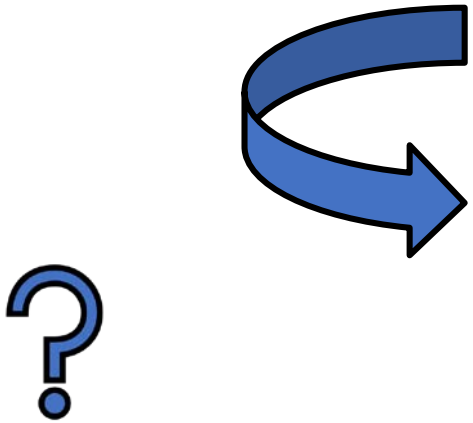
- descrivere le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e anche, se del caso, per attenuare i possibili effetti negativi per gli interessati.

Possibilità di procedere per step ex **art. 33, comma IV, GDPR** purché il titolare, al momento della notifica, indichi che si tratta di una **notifica preliminare**, impegnandosi a comunicare tutte le informazioni e i dettagli circa la violazione occorsa **non appena disponibili e senza ingiustificato ritardo** attraverso una notifica integrativa.

In ogni caso, i**l titolare del trattamento deve documentare tutte le violazioni dei dati personali** che si verificano, indipendentemente dalla circostanza che una violazione debba o meno essere notificata al Garante: principio di **responsabilizzazione** (**art. 5, comma II ed art. 24, GDPR**).

Obbligo di tenuta di un registro interno delle violazioni occorse che può essere oggetto di consultazione da parte del Garante e che dovrà attestare oltre a cause, fatti, tipologia di dati personali violati, effetti e conseguenze della violazione ma anche la ratio alla base delle decisioni adottate in risposta ad una violazione nonché le azioni correttive poste in essere anche per contenere il danno, tempistiche di intervento, modalità di comunicazione della violazione agli interessati.

Ancora un rilievo sulla notifica



Le "**Guidelines 9/2022 on personal data breach notification under GDPR**" sono state sottoposte a consultazione pubblica solo per il paragrafo 73 fino al 29 novembre 2022.
Cosa prevede dunque il paragrafo 73? - Requisiti per provvedere alla notifica nell'ambito di attività svolte da parte di titolari non stabiliti nel territorio dell'UE per il tramite dei propri rappresentanti designati ai sensi dell'art. 27 GDPR -
Nell'ipotesi di un titolare non stabilito nell'Unione Europea le linee guida precedenti prevedevano l'obbligo di notifica nei confronti dell'autorità di controllo dello Stato membro in cui era stabilito il rappresentante ex art. 27 GDPR ma ricordiamo che le linee guida WP244 per l'individuazione dell'autorità di controllo capofila in relazione ad uno specifico titolare del trattamento o responsabile del trattamento dispongono: "*Se una società non dispone di uno stabilimento nell'UE, la semplice esistenza di un rappresentante designato in uno Stato membro non comporta l'intervento del meccanismo di "sportello unico". Ciò significa che un titolare del trattamento che non sia stabilito in alcun paese dell'UE dovrà interfacciarsi con le autorità di controllo di ciascuno Stato membro in cui opera, per il tramite del rappresentante designato.*"

Il principio dello "*sportello unico*" è espressamente escluso dalla nuova formulazione che impone **l'obbligo di notifica a ciascuna autorità di controllo di riferimento rispetto agli interessati coinvolti dalla violazione.**

Dunque...i titolari extra UE dovranno notificare una violazione "ad ogni singola autorità per la quale gli interessati risiedono nel loro Stato membro" = notificare una violazione a numerose autorità di protezione dei dati entro il termine di 72 ore.

Occorre dunque una attività di analisi dell'incidente più complessa che non è detto si possa svolgere entro 72 ore....

- La comunicazione all'interessato –

Articolo 34
Comunicazione di una violazione dei dati personali all'interessato

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.*

"***senza ingiustificato ritardo***": l'obiettivo principale della comunicazione è fornire agli interessati informazioni specifiche sulle misure che questi possono adottare per tutelarsi, ovvero, la tempestività della comunicazione aiuterà gli interessati ad adottare provvedimenti idonei per proteggersi da eventuali conseguenze negative della violazione

...e quale possibile motivo di giustificazione del ritardo, il **GDPR (considerando (88)** menziona le indagini dell'Autorità competente: "*Nel definire modalità dettagliate relative al formato e alle procedure applicabili alla notifica delle violazioni di dati personali, è opportuno tenere debitamente conto delle circostanze di tale violazione, ad esempio stabilire se i dati personali fossero o meno protetti con misure tecniche adeguate di protezione atte a limitare efficacemente il rischio di furto d'identità o altre forme di abuso. Inoltre, è opportuno che tali modalità e procedure tengano conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali*".

- ***Contenuto della comunicazione*** -

Ex art. 34, comma 2, GDPR, **WP250** e ***Guidelines 9/2022***, occorre fornire con un "*linguaggio semplice e chiaro*":

- una descrizione della natura della violazione;

- il nome e dati di contatto del responsabile della protezione dei dati (RDP) o di altro punto di contatto presso cui ottenere più informazioni;

- una descrizione delle probabili conseguenze della violazione dei dati personali;

- una descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e anche, se del caso, per attenuare i possibili effetti negativi per gli interessati

...questo è il contenuto minimo ("*almeno*")... lo stesso Garante nella documentazione pubblicata per il self assessment precisa che ***il titolare del trattamento dovrebbe fornire anche consulenza specifica alla persone fisiche sul modo in cui proteggersi dalle possibili conseguenze della violazione.***

- ***Come contattare l'interessato*** -

La violazione dovrebbe essere comunicata direttamente agli interessati coinvolti (ad esempio, mediante messaggi di posta elettronica, SMS, comunicazione postale), salvo che ciò richieda uno *"sforzo sproporzionato"*: in tal caso, si procede mediante una comunicazione pubblica o misura simile (ad esempio, banner o notifiche su siti web di primo piano, pubblicità di rilievo sulla stampa ex WP29) che permetta di informare gli interessati con analoga efficacia, ai sensi dell'**art. 34, comma 3**.

Si devono utilizzare *messaggi dedicati* che non devono essere inviati insieme ad altre informazioni

- ***Quando la comunicazione non è necessaria*** -

Art. 34, comma 3, GDPR

- il titolare ha posto in essere misure tecniche ed organizzative prima della violazione, in particolare, misure che rendano i dati non comprensibili a chiunque non sia autorizzato all'accesso, quali la cifratura;

- il titolare ha adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà dell'interessato o di terzi dopo la violazione;

- la comunicazione richiederebbe uno sforzo sproporzionato, fermo restando che in tale caso dovrà comunque essere adottata una comunicazione pubblica o misura simile con analoga efficacia (WP29: sms, e-mail, messaggi diretti o banners in evidenza sul sito del titolare, comunicazioni a mezzo posta o pubblicità sulla carta stampata).

...solo il Centro di sperimentazione può effettuare la comunicazione all'interessato, essendo il titolare autonomo in possesso dei dati identificativi del paziente...

- ***Processo interno di gestione e valutazione dell'evento*** -

"**Guidelines 9/2022 on personal data breach notification under GDPR**", versione 2.0, adottata il 28 marzo 2023 dall'EDPB, introduzione:

"…I titolari e i responsabili del trattamento sono pertanto incoraggiati a pianificare anticipatamente e a mettere in atto processi per essere in grado di rilevare e limitare tempestivamente gli effetti di una violazione, valutare il rischio per le persone fisiche e stabilire se sia necessario notificare la violazione all'autorità di controllo competente e comunicarla alle persone fisiche interessate, ove necessario. La notifica all'autorità di controllo dovrebbe costituire parte del piano di intervento in caso di incidente…"

RILEVAZIONE EVENTO ANOMALO, TITOLARE VIENE A CONOSCENZA DELLA VIOLAZIONE

↓

LA VIOLAZIONE POTREBBE COMPORTARE UN RISCHIO PER I DIRITTI E LE LIBERTA'DELLE PERSONE FISICHE?

ANALISI DELLA VIOLAZIONE E VALUTAZIONE DEI RISCHI (in base alle procedure interne del titolare)

↓ RISCHI ASSENTI

REGISTRAZIONE E ARCHIVIAZIONE DELLA VIOLAZIONE

↓ RISCHI PRESENTI

↓ PROBABILE MA NON ELEVATO

NOTIFICA AL GARANTE

↓ PROBABILE ED ELEVATO

NOTIFICA AL GARANTE E COMUNICAZIONE AGLI INTERESSATI PROVVEDENDO AD INFORMARLI SULLE MISURE ADOTTABILI PER TUTELARSI DALLE CONSEGUENZE DELLA VIOLAZIONE

IN OGNI CASO

REGISTRAZIONE DELLA VIOLAZIONE EX ART. 33, COMMA 5, GDPR DA PARTE DEL TITOLARE ED ADOZIONE MISURE CORRETTIVE MIGLIORATIVE + FORMAZIONE

- ***Casistica*** -

Linee guida n. 01/2021

1) Attacco ransomware:
un codice dannoso crittografa i dati personali e l'attaccante chiede al titolare un riscatto in cambio del codice di decrittazione, in questi casi l'EDPB distingue a secondo che il titolare abbia o meno un backup dei dati criptati o che vi sia o meno stato l'esfiltrazione degli stessi;
- misure adottabili: mantenere attivo il firmware, il sistema operativo e il software applicativo sui server, sui computer client componenti di rete e qualsiasi altra macchina sulla stessa LAN (compresi i dispositivi Wi-Fi) aggiornati;
garantire che siano in atto misure di sicurezza IT appropriate, assicurandosi che siano efficaci e mantenere regolarmente aggiornati quando l'elaborazione o le circostanze cambiano o si evolvono;
l'esistenza di una procedura di backup aggiornata, sicura e testata;
un software antimalware appropriato, aggiornato, efficace e integrato;
un firewall appropriato, aggiornato, efficace e integrato e di rilevamento delle intrusioni;
formazione dei dipendenti sui metodi per riconoscere e prevenire gli attacchi informatici;
identificare il tipo di codice dannoso per attestare le conseguenze;
crittografia forte e autenticazione a più fattori, in particolare per l'accesso amministrativo ai sistemi IT;
gestione appropriata di chiavi e password;
test di vulnerabilità e penetrazione su base regolare;
istituire un Computer Security Incident Response Team (CSIRT) o Computer Emergency Response Team (CERT) all'interno dell'organizzazione, o aderire a un CSIRT/CERT collettivo;
Recovery Plan e un Business Continuity Plan ed assicurarsi che questi siano accuratamente testati.
- misure organizzative: fondamentale la formazione dei dipendenti sui metodi di riconoscimento e prevenzione degli attacchi informatici, pianificazione di testi di vulnerabilità e penetrazione su base regolare e la creazione di un computer security incident response team e poi piani di incident response, disaster recovery, testati.

2) Esfiltrazione dei dati:
tali attacchi sfruttano la vulnerabilità dei sistemi e mirano a copiare, esfiltrare ed usare i dati personali per fini illeciti (violazioni della riservatezza ed a volte anche dell'integrità dei dati);
- misure tecniche: adozione sistemi di crittografia e gestione delle chiavi (es, per dati particolari) e preferire uso di metodi di autenticazione che evitano la necessità di elaborare le password sul lato server;
- misure organizzative: policy di gestione degli utenti e di controllo degli accessi nonché programmare ed effettuare verifiche sistematiche della sicurezza IT e valutazioni/test della vulnerabilità.

3) Errore umano:

eventi, volontari e non, causati da comportamenti umani che portano a delle violazioni (esempio, esfiltrazione di dati da parte di un dipendente o invio accidentale tramite email di dati a soggetti non autorizzati o perdita di device e documenti contenenti dati);
- misura organizzativa: fondamentale è la programmazione di piani di formazione e sensibilizzazione periodica del personale attivo presso la struttura del titolare e fondamentale è l'apporto del DPO, ex art. 39, comma II, let. b), GDPR. In particolare, il personale dovrebbe essere istruito sulle procedure: policy di controllo di accesso ai sistemi/regole per disabilitazione account aziendale non appena la persona lascia l'azienda/meccanismi di controllo del flusso di dati insoluto tra il file server e le stazioni di lavoro mentre il titolare dovrebbe adottare per l'uso dei device le seguenti misure: disabilitare la funzione di stampa dello schermo nel sistema operativa/clean desk/bloccare pc dopo un tempo di inattività/crittografia del dispositivo/ritardo nell'invio del messaggio con possibilità di eliminarlo o modificarlo per un certo periodo dopo aver cliccato per l'invio/disabilitazione del completamento automatico quando vengono digitati indirizzi e-mail.

Ricordiamo però che ogni attività di trattamento è diversa quindi il titolare del trattamento deve adottare le misure più idonee alla situazione concreta.

E' importante dunque che **il titolare adotti piani e procedure che gli consentano di gestire le violazioni in maniera ottimale** investendo ad esempio sulla formazione inerente all'identificazione dei data breach e relative azioni da intraprendere: un manuale di gestione delle violazione volto ad individuare tutti gli elementi caratterizzanti del trattamento e documentare tutte le misure tecniche ed organizzative implementate.

Caso 1: ransomware con backup adeguato e senza esfiltrazione

Azioni necessarie		
Documentazione interna	Notifica Autorità Competente	Comunicazione Interessato
Sì	No	No

Caso 2: ransomware senza un backup adeguato

Azioni necessarie		
Documentazione interna	Notifica Autorità Competente	Comunicazione Interessato
Sì	Sì	No

Caso 3: ransomware con backup adeguato e senza esfiltrazione in un ospedale

Azioni necessarie		
Documentazione interna	Notifica Autorità Competente	Comunicazione Interessato
Sì	Sì	Sì

ESEMPI (tratti da WP250/Guidelines 9/2022)	NOTIFICA AL GARANTE	COMUNICAZIONE AGLI INTERESSATI	NOTE
Il Titolare ha effettuato un back up di un archivio di dati personali crittografati su una chiave USB. La chiave viene rubata durante un'effrazione.	NO	NO	I dati sono crittografati con un algoritmo all'avanguardia, esiste un back up degli stessi, la chiave univoca non viene compromessa e i dati possono essere ripristinati in tempo utile.
In un call center si verifica una breve interruzione di corrente per alcuni minuti: gli utenti non possono accedere al servizio	NO	NO	Non è un data breach da notificare ma va registrato ai sensi dell'art. 33.5 GDPR
Un Titolare subisce un attacco ransomware (sw dannoso che cifra i dati del Titolare finché non viene pagato un riscatto) che provoca la cifratura di tutti i dati. Non sono disponibili backup up e i dati non possono essere ripristinati.	Si, effettuare la segnalazione all'autorità dl controllo, se vi sono probabili conseguenze per le persone fisiche in quanto si tratta di una perdita di disponibilità.	Si, effettuare la segnalazione alle persone fisiche, a seconda della natura dei dati personali interessati e del possibile effetto della mancanza di disponibilità dei dati, nonché di altre possibili conseguenze.	Se fosse stato disponibile un back up e i dati avessero potuto essere ripristinati in tempo utile non sarebbe stato necessario segnalare la violazione all'autorità di controllo o alle persone fisiche, in quanto non si sarebbe verificata nessuna perdita permanente di disponibilità o riservatezza.
I dati sanitari di un ospedale non sono disponibili per un periodo di trenta ore a causa di un attacco informatico.	Si, in quanto può verificarsi un rischio elevato per la salute e fa tutela della vita privata dei pazienti.	Si, informare le persone fisiche coinvolte.	
I dati personali di un grande numero di studenti vengono inviati per errore ad una mailing list sbagliata, con più di mille destinatari	Sì	Sì, segnalare l'evento alle persone coinvolte in base alla portata, al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	

- ***Elementi oggetto della valutazione del rischio*** -

Tipo di dato oggetto della violazione
(dati personali, genetici, biometrici,…)

Effetti sui dati personali
(distruzione, perdita, modifica, divulgazione non autorizzata,…)

Tipo di violazione
(lettura, copia, alterazione, cancellazione, furto, accesso abusivo,…)

Eventi dannosi che potrebbero verificarsi nei confronti dell'interessato
(discriminazione, furto di identità, danno economico e/o sociale, danni fisici materiali o immateriali,…)

Quali misure tecniche ed organizzative sono state adottate preventivamente?
(es. pseudonimizzazione e cifratura dei dati personali)

Sono state adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati successivamente alla violazione?

Livello di gravità della violazione dei dati personali
(basso: piccoli inconvenienti/medio: notevoli disagi superabili con alcune difficoltà/alto: conseguenze significative magari superabili ma con gravi difficoltà/molto alto: conseguenze anche irreversibili non superabili)

Livello di Rischio (LR)	Ove possibile entro 72 h	Senza ingiustificato ritardo
	Notifica all'Autorità	Comunicazione agli interessati
Rischio alto/molto alto	SI'	SI'
Rischio medio	SI	NO
Rischio basso	NO	NO

Perdita o furto di dispositivi aziendali /documenti cartacei

Il titolare deve valutare le circostanze del trattamento, il tipo di dati memorizzati e le misure di sicurezza adottate: l'attivazione della crittografia del dispositivo e l'uso di password sicure unitamente all'autenticazione a più fattori; access control; divieto di memorizzazione delle informazioni sensibili sui dispositivi mobili evitano la dispersione dei dati (salvo la possibilità di attivare una procedura di sicurezza a distanza che consenta la cancellazione dei dati inseriti all'interno dei tablet) e poi è fondamentale il **backup = garantisce la disponibilità dei dati personali**.

Ricordiamo solo alcune semplici regole da osservare nella ***trasmissione via e-mail di categorie particolari di dati personali:***

- l'utilizzo della posta elettronica non offre garanzie in termini di sicurezza;
- attenzione nella selezione del soggetto destinatario: tali informazioni vanno comunicate unicamente all'interessato o a terzi solo se legittimati sulla base di idoneo presupposto giuridico o su indicazione dello stesso interessato (delega scritta);
- il Garante ha dichiarato come illecito l'invio di una comunicazione contenente dati personali mediante un unico messaggio di posta elettronica indirizzato ad un numero plurimo di destinatari: la comunicazione contenente dati personali deve essere inviata a ciascun soggetto destinatario separatamente;
- il documento contenente dati particolari dovrà essere spedito in allegato ad un messaggio e-mail e non come testo compreso nel corpo del messaggio;
- il file contenente il documento dovrà essere protetto con modalità idonee, ad esempio, tramite password resa nota agli interessati tramite canali di comunicazione differenti da quelli utilizzati per la spedizione.

- Poteri dell'autorità di controllo -

Art. 58 del GDPR:

- **poteri di indagine** (acquisizione di informazioni, accesso ai dati, ai locali);

- **poteri correttivi** (può prescrivere misure correttive anche per quanto concerne l'adeguatezza delle misure di sicurezza tecniche ed organizzative applicate ai dati oggetto di violazione fino ad arrivare alla comminazione di **sanzioni amministrative pecuniarie** fino a 10 milioni di euro o, in caso di imprese, fino al 2% del fatturato totale annuo mondiale), valutando le conseguenze della violazione **ex considerando 85 del GDPR** e potendo prescriverle in modo indipendente o in associazione ad una misura correttiva.

Articolo 58 GDPR

Poteri

*1. Ogni autorità di controllo ha tutti i **poteri di indagine** seguenti:*

a) ingiungere al titolare del trattamento e al responsabile del trattamento e, ove applicabile, al rappresentante del titolare del trattamento o del responsabile del trattamento, di fornirle ogni informazione di cui necessiti per l'esecuzione dei suoi compiti;

b) condurre indagini sotto forma di attività di revisione sulla protezione dei dati;

c) effettuare un riesame delle certificazioni rilasciate in conformità dell'articolo 42, paragrafo 7;

d) notificare al titolare del trattamento o al responsabile del trattamento le presunte violazioni del presente regolamento;

e) ottenere, dal titolare del trattamento o dal responsabile del trattamento, l'accesso a tutti i dati personali e a tutte le informazioni necessarie per l'esecuzione dei suoi compiti; e

f) ottenere accesso a tutti i locali del titolare del trattamento e del responsabile del trattamento, compresi tutti gli strumenti e mezzi di trattamento dei dati, in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri.

*2. Ogni autorità di controllo ha tutti i **poteri correttivi** seguenti:*

a) rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente regolamento;

b) rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del presente regolamento;

c) ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal presente regolamento;

d) ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine;

e) ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali;

f) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;

g) ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19;

h) revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti;

i) infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle misure di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso; e

j) ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

3. Ogni autorità di controllo ha tutti i poteri autorizzativi e consultivi seguenti:...

…e l'**art. 82, GDPR**:

Articolo 82

Diritto al risarcimento e responsabilità

1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

4. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

5. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2.

6. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2.

Articolo 83 GDPR (ed art. 166 Codice Privacy)
Condizioni generali per infliggere sanzioni amministrative pecuniarie

1. Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive.

2. Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure. Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:
a) 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;
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 da essi messe in atto ai sensi degli articoli 25 e 32;
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; e
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.

3. Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave.

4. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:
a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43;
b) gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;
c) gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4;...

...5. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;

b) i diritti degli interessati a norma degli articoli da 12 a 22;

c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;

d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;

e) l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

6. In conformità del paragrafo 2 del presente articolo, l'inosservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

7. Fatti salvi i poteri correttivi delle autorità di controllo a norma dell'articolo 58, paragrafo 2, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro.

8. L'esercizio da parte dell'autorità di controllo dei poteri attribuitile dal presente articolo è soggetto a garanzie procedurali adeguate in conformità del diritto dell'Unione e degli Stati membri, inclusi il ricorso giurisdizionale effettivo e il giusto processo.

9. Se l'ordinamento giuridico dello Stato membro non prevede sanzioni amministrative pecuniarie, il presente articolo può essere applicato in maniera tale che l'azione sanzionatoria sia avviata dall'autorità di controllo competente e la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali, garantendo nel contempo che i mezzi di ricorso siano effettivi e abbiano effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità di controllo. In ogni caso, le sanzioni pecuniarie irrogate sono effettive, proporzionate e dissuasive. Tali Stati membri notificano alla Commissione le disposizioni di legge adottate a norma del presente paragrafo al più tardi entro 25 maggio 2018 e comunicano senza ritardo ogni successiva modifica.

La metodologia proposta dall'**EDPB nelle linee guida 4/2022** sull'applicazione e previsione delle sanzioni amministrative pecuniarie "Guidelines 04/2022 on the calculation of administrative fines under the GDPR", del 12 maggio 2022 (allo stato attuale, oggetto di consultazione pubblica) prevede cinque fasi:

1. le autorità per la protezione dei dati devono stabilire se il caso in questione riguarda uno o più casi di condotta sanzionabile e se questi hanno portato a una o più violazioni;
2. le autorità valutano la base di calcolo della sanzione secondo un modello definito dal Comitato per la Protezione dei Dati;
3. le autorità devono considerare i fattori aggravanti o attenuanti che possono aumentare o diminuire l'importo della sanzione;
4. determinare i massimali legali delle ammende e garantire che tali importi non vengano superati;
5. le autorità devono analizzare se l'importo finale calcolato soddisfa i requisiti di effettività, proporzionalità e dissuasione o se sono necessari ulteriori adeguamenti dell'importo.

Concludendo….cosa manca?

A seguito dell'entrata in vigore del GDPR siamo ancora in attesa di un intervento innovativo ad hoc nel settore delle sperimentazioni cliniche da parte del Garante della privacy che disamini anche – ma non solo – la tematica della disciplina della gestione delle violazioni in tale ambito, in considerazione dei ruoli delle Parti coinvolte (promotore/centro di sperimentazione - titolare/responsabile) e di quanto definito, da ultimo, dalle linee guida n. 9/2022 dell'EDPB…

Grazie per l'attenzione!

relia@cittadellasalute.to.it