PROCEDURA DATA BREACH

L'**IRCCS Neurolesi Bonino Pulejo di Messina** ai sensi del Regolamento Europeo 2016/679 (da qui in avanti GDPR), è tenuto a proteggere i dati personali trattati nell'ambito delle proprie attività istituzionali e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (incluse eventuali notifiche all'Autorità Garante competente ed eventuali comunicazioni agli interessati). È di fondamentale importanza predisporre procedure da attuare nell'eventualità in cui si presentino violazioni concrete, potenziali o sospette di dati personali, ciò al fine di evitare rischi per i diritti e le libertà degli interessati, nonché danni economici all'Ente Pubblico e per poter informare nei tempi e nei modi previsti dalla normativa europea l'Autorità Garante e/o gli interessati.

Lo scopo di questa procedura è quello di definire le modalità da osservare in caso di violazioni dei dati personali trattati dall'**IRCCS Messina** in qualità di Titolare del trattamento (di seguito "Titolare del trattamento"). Queste procedure sono ad integrazione delle procedure già adottate in materia di protezione dei dati personali ai sensi della legislazione vigente.
Una violazione di dati personali è: *ogni infrazione alla sicurezza degli stessi che comporti - 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 dal Titolare del trattamento.* La violazione di dati è un tipo particolare di incidente di sicurezza, per effetto del quale, il titolare non è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del GDPR per il trattamento dei dati personali.

Preliminarmente, dunque, il Titolare deve poter identificare l'incidente di sicurezza in genere, quindi, comprendere che l'incidente ha impatto sulle informazioni e, infine, che tra le informazioni coinvolte dall'incidente vi sono dati personali.

Ne discende che le generali attività di scoperta dell'incidente, come le successive di trattamento, devono essere documentate, adeguate (devono riportare le violazioni, le circostanze, le conseguenze ed i rimedi), tracciabili, replicabili ed essere in grado di fornire evidenza nelle sedi competenti.

Queste procedure sono rivolte a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento, quali:

• i lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto intercorrente - abbiano accesso ai dati personali trattati nel corso del proprio impiego per conto del Titolare del trattamento (collaboratori, tirocinanti, liberi professionisti)

• qualsiasi soggetto (persona fisica o persona giuridica) diverso dai soggetti sopra menzionati che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento ex art. 28 GDPR o di autonomo Titolare (art. 26 Contitolarità del trattamento).

Le diverse fasi della procedura riguardano:

1 Identificazione e indagine preliminare

2 Contenimento, recovery e risk assessment
3 Eventuale notifica all'Autorità Garante
4 Eventuale comunicazione agli interessati
5 Documentazione della violazione

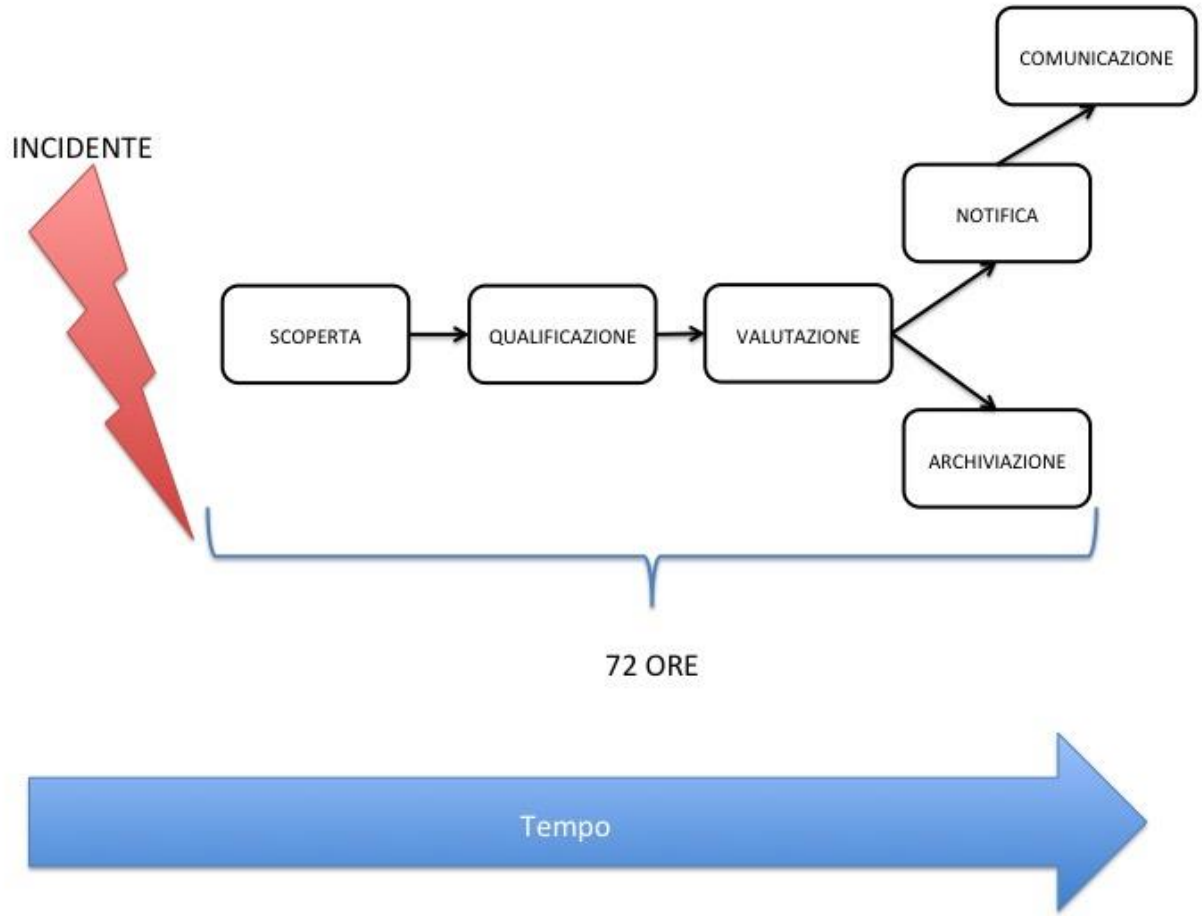
L'art. 33 del Regolamento Europeo 2016/679 (GDPR) impone al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali (data breach) entro **settantadue ore** dal momento in cui ne viene a conoscenza.

L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il **rischio fosse elevato,** allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.

L'eventuale ritardo nella notificazione deve essere giustificato, il **mancato rispetto dell'obbligo di notifica**, invece, pone l'Autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti dall'**art. 58 GDPR** (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati), la imposizione di sanzioni amministrative secondo l'**art. 83 GDPR**, il cui importo può arrivare a 10.000.000 di euro o al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Occorre in ogni caso tenere conto che, la mancata notifica e/o comunicazione, possono rappresentare per l'Autorità di controllo un indizio di carenze più profonde e strutturali quali ad esempio carenze od inadeguatezza di misure di sicurezza, in tal caso, trattandosi di ipotesi separate ed autonome, l'autorità procederà per l'ulteriore irrogazione di sanzioni.

Il rispetto degli obblighi di notifica (art. 33) e di comunicazione (art.34), in situazioni già mediamente complesse (in termini di dimensioni ed articolazione dell'organizzazione del titolare e/o in termini di numero di interessati di cui sono trattati i dati personali e/o in termini di operazioni di trattamento, o di quantità, varietà, natura dei dati trattati), richiede al Titolare di strutturare il trattamento dei dati personali avvalendosi di **un sistema di conformità**. Questo sistema deve essere in grado di rispettare i requisiti di trasparenza, evidenza e responsabilità prescritti dal GDPR; si ricorda che l'art. 24 punto 1 del GDPR richiede al Titolare di "mettere in atto misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR".



Il considerando 85 del GDPR spiega che lo scopo della notifica è di limitare i danni che possono derivare per effetto di una violazione a carico degli interessati e che l'efficacia di questo dovere di limitazione dipende dalla tempestività e dall'adeguatezza con cui la violazione è affrontata.

Il gruppo "Article 29 Data Protection Working Party" (WP29), oggi Comitato Europeo, chiarisce ulteriormente che la responsabilità del Titolare deve essere commisurata secondo la sua capacità di scoprire tempestivamente un incidente ed indagarlo al fine di valutare l'obbligatorietà della notifica.

Dato che l'obbligo di notifica spetta al Titolare, è molto importante che, nell'affidare servizi a **Responsabili del trattamento**, questi, preliminarmente, si accerti della capacità del fornitore nel gestire tempestivamente e adeguatamente un incidente di sicurezza (art. 28 p.1 GDPR) e, quindi, preveda idonee clausole contrattuali (art. 28 p.3 GDPR) che regolino il rapporto di fornitura in modo da garantire il rispetto del GDPR.

L'art. 33 p.2 GDPR prevede espressamente il dovere per il Responsabile, quando viene a conoscenza di una violazione, di informare, senza ingiustificato ritardo, il Titolare. A questo scopo è stato elaborato un **modello di comunicazione al Titolare** che viene fornito contestualmente alla firma del contratto di Responsabile esterno. Il modello seve per guidare il Responsabile nella disamina dell'accaduto, per fornire informazioni precise e deve permettere al Titolare di valutare la portata di questo in termini di impatto rispetto ai dati personali ed ai diritti e la libertà degli interessati.
Il Responsabile è obbligato ad effettuare la comunicazione al Titolare entro 24 ore dall'evento.

Si possono distinguere tre tipi di violazioni:

1) **Violazione di riservatezza**, ovvero *quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale.*

2) **Violazione di integrità**, ovvero *quando si verifica un'alterazione di dati personali non autorizzata o accidentale.*

3) **Violazione di disponibilità**, ovvero *quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali*.

In particolari circostanze le violazioni potrebbero essere combinate tra loro.

L'**art. 32** del GDPR richiede al titolare di mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio; in particolare:

– la lettera B) richiede: "la capacità di **assicurare su base permanente la disponibilità** dei sistemi e dei servizi di trattamento;

– la lettera C) la capacità di **ripristinare tempestivamente la disponibilità** e l'accesso dei dati personali in caso di incidente fisico o tecnico.

Da quanto sopra si ricava che un incidente che determini la non disponibilità di dati per un periodo di tempo deve essere comunque considerato violazione e, dunque, deve essere comunque documentato.

Il **considerando 85** offre utili elementi per determinare i rischi che possono determinare l'obbligo di notifica, in particolare, occorre valutare la possibilità che la violazione possa causare **danni fisici, materiali o immateriali alla persona fisica**. La disposizione a titolo d'esempio elenca: *perdita del controllo dei dati personali che li riguardano; limitazione dei loro diritti; discriminazione; furto o usurpazione di 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 per la persona interessata*.

Il **considerando 86** del GDPR chiarisce che l'obbligo di comunicazione risponde allo scopo di consentire all'interessato, qualora sussista una violazione che presenta rischi elevati, di prendere le precauzioni necessarie.

Le violazioni di dati personali **sono gestite dal Titolare del trattamento o da un suo Delegato, sotto la supervisione del DPO.** In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la stessa sia affrontata immediatamente e correttamente al fine di minimizzare l'impatto della violazione e prevenire che si ripeta. Nel caso in cui uno dei Destinatari si accorga di una concreta, potenziale o sospetta violazione dei dati personali, dovrà immediatamente informare dell'incidente il superiore gerarchico il quale si occuperà, con il supporto dei Destinatari stessi, di informare il Titolare del trattamento mediante la compilazione del "**Modello di segnalazione di Data Breach**" da inviare a mezzo mail all'indirizzo PEC:

azienda@pec.irccsneurolesiboninopulejo.it e per conoscenza al D.P.O. all'indirizzo: alessandra.piccolo@irccsme.it .

Nel caso in cui si tratti di violazione di dati di un sistema informatico, il Titolare del trattamento o un suo Delegato, dovrà coinvolgere in tutta la procedura il Responsabile dell'Ufficio IT.

Una volta stabilito che un Data Breach è avvenuto, il Titolare del trattamento o un suo delegato insieme al DPO dovranno stabilire:

- se esistono azioni che possano limitare i danni che la violazione potrebbe causare (per esempio: riparazione fisica di strumenti; utilizzo di file di back up per il recupero dei dati persi o danneggiati; cambio di codici di accesso; isolamento/chiusura di un settore compromesso dalla rete.
- Una volta identificate tali azioni, quali siano i soggetti che devono agire per contenere la violazione.
- Se sia necessario notificare la violazione all'Autorità Garante
- Se sia necessario comunicare la violazione agli interessati (ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche.

Valutata la necessità di effettuare la notifica della violazione dei dati, **l'IRCCS Neurolesi di Messina**, dovrà procedere senza ritardo secondo le modalità stabilite dagli artt. 33 e 34 del GDPR.
Indipendentemente dalla necessità della comunicazione all'Autorità di controllo ed all'interessato, il Titolare provvederà a stilare un **Registro di Data Breach** contenente:

- il numero della violazione;
- la data della violazione;
- la natura della violazione;
- la categoria degli interessati;
- la categoria dei dati coinvolti;
- le conseguenze della violazione;
- le contro misure adottate;
- la comunicazione o meno al Garante ed all'interessato.

Notifica di una violazione di dati all'Autorità di controllo - Art. 33 p.3 GDPR

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 per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

INDIRIZZO PEC DEL GARANTE DELLA PRIVACY:

protocollo@pec.gpdp.it

Comunicazione di una violazione dei dati all'interessato - Art. 34 p.2 GDPR

a) Descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali.

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 per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

La comunicazione dovrebbe essere data direttamente e personalmente agli interessati coinvolti dalla violazione, a meno che ciò comporti sforzi sproporzionati. In tal caso, si procede invece ad una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con la medesima efficacia.

La comunicazione deve essere distinguibile rispetto altre diverse comunicazioni che vengono fatte dal titolare agli interessati, in altri termini, la comunicazione deve essere chiara, inequivocabile e richiamare l'attenzione dell'interessato.

Il rispetto di questi requisiti richiede che il titolare, già prima che si verifichi una causa di comunicazione, considerati i dati che tratta e le categorie di interessati, predisponga un piano specifico di comunicazione.

La comunicazione, pur sussistendo la condizione di rischio elevato, **si ritiene soddisfatta** quando:

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.
Mentre per far scattare l'obbligo di notifica è sufficiente che sussista una violazione di dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche, per la comunicazione occorre che tale rischio sia elevato.

Il titolare è dunque tenuto non solo ad individuare e qualificare i rischi connessi a violazioni di dati personali, ma, qualora tali rischi riguardino i diritti e le libertà delle persone fisiche, deve anche procedere ad una valutazione del livello di rischio.

Il considerando **76 del GDPR** chiarisce che 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.

Il Comitato Europeo suggerisce ulteriori criteri per permettere una valutazione più accurata:

- Tipo di violazione
- Natura, sensibilità e volume dei dati personali
- Facilità di riconoscimento degli interessati
- Serietà delle conseguenze per le persone fisiche
- Caratteristiche specifiche delle persone fisiche
- Quantità di persone fisiche coinvolte
- Caratteristiche specifiche del titolare

La valutazione dei rischi non sempre è semplice, il Comitato raccomanda al Titolare, in caso di dubbio, di **scegliere la strada di maggior tutela procedendo alla notifica**.

I presidi della notifica e della comunicazione seppure richiedono adempimenti specifici, non possono essere letti ed interpretati correttamente senza considerare la loro correlazione con l'intero GDPR, quali organi di un medesimo corpo.

In particolare sono fondamentali gli articoli 24 e 32 del GDPR, essi impongono ad ogni titolare di:

1) mettere in atto misure tecniche e organizzative adeguate per garantire il rispetto del GDPR;

2) essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR;

3) riesaminare ed aggiornare tali misure quando necessario;

4) garantire un livello di sicurezza adeguato al rischio.

Gli obblighi di cui sopra devono essere valutati tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche propri di ciascun titolare.

La valutazione dell'incidente presuppone la definizione dei criteri di valutazione, la formazione del personale incaricato, la predisposizione di procedure.

La tempestività nella notifica può essere assicurata solo attraverso il sistema di comunicazione interno, per il personale adeguatamente formato che collabora a vario titolo con l'IRCCS Messina, esterno (Responsabili) perché *"presentano garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate"* in grado di *"garantire la tutela dei diritti dell'interessato."*

Infine, la stessa documentazione delle violazioni che la norma prescrive di conservare (anche per quelle che non determinano obbligo di notifica), è possibile in quanto è stato strutturato un sistema di gestione degli incidenti.

Concludendo, l'**IRCCS Neurolesi Bonino Pulejo di Messina**, attraverso questa procedura intende costruire lo strumento di guida e di controllo da utilizzare nella gestione della propria organizzazione per garantire una corretta protezione dei dati, per definire le prescrizioni da osservare e le possibili soluzioni da adottare, in caso di incidenti.