AZIENDA SANITARIA LOCALE BR
Via Napoli n. 8 - 72100 Brindisi
C.F. P. IVA – 01647800745 - Web:http://www.asl.brindisi.it

PROCEDURA DI GESTIONE DELLA VIOLAZIONE DI DATI (DATA BREACH)

INDICE

1. PREMESSA

Il Data Breach è "*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"* dal Titolare del trattamento.
A norma dell'art. 33 del Regolamento Europeo 2016/679 (da qui in avanti GDPR), ogni violazione di sicurezza, come sopra descritta, deve essere notificata all'Autorità Garante, senza ingiustificato ritardo e, ove possibile, entro 72 ore, dal momento in cui si è venuto a conoscenza della violazione. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, la stessa deve essere corredata dai motivi del ritardo. La notifica al Garante non è necessaria quando sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.
Inoltre, ai sensi dell'art.34 del GDPR, 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 deve comunicare la violazione all'interessato senza ingiustificato ritardo.
Per la omessa notifica di Data Breach all'Autorità di Controllo o per l'omessa comunicazione agli interessati o per entrambi gli adempimenti, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 GDPR, sono previste pesanti sanzioni amministrative (art. 83 GDPR), il cui importo può arrivare a 10.000.000 di euro o al 2% del fatturato totale annuo dell'esercizio precedente, se superiore, nonché le misure correttive di cui all'art.58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati).
E' pertanto di fondamentale importanza predisporre una procedura organizzativa interna per la gestione di eventuali violazioni concrete, potenziali o sospette di dati personali per adempiere agli obblighi imposti dalla normativa europea ed evitare rischi per i diritti e le libertà degli interessati, nonchè danni economici per l'Azienda Sanitaria Locale BR.

2. NORMATIVA E DOCUMENTI DI RIFERIMENTO

- Regolamento UE 2016/679, considerando n. 85, 86, 87, 88, artt. 33, 34;
- Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) ai sensi del Regolamento 679/2016 (WP250) adottate dal Gruppo di lavoro art.29 (WP29), il 3/10/2017 – versione emendata e adottata il 06/02/2018;
- Best practices di settore sviluppatesi alla luce del Codice Privacy (D.Lgs.196/2003) e della giurisprudenza del Garante;
- Linee guida sui responsabili della protezione dei dati (WP243), adottate dal WP29, in via definitiva, il 5 aprile 2017;
- Dichiarazione relativa al ruolo di un approccio basato sul rischio nel quadro normativo in materia di protezione dati (WP218), adottata dal WP29 il 30 maggio 2014.

3. FINALITA'

La finalità di questa procedura organizzativa interna è quella di fornire delle indicazioni pratiche ed operative, individuando la metodologia che consenta la gestione delle violazioni dei dati personali trattati dalla ASL BR in qualità di Titolare del trattamento.

4. CATEGORIE DEI DATI OGGETTO DELLA PROCEDURA DI SEGNALAZIONE DEL DATA BREACH

I dati oggetto di riferimento sono i dati personali trattati "da "e "per conto" del Titolare del trattamento, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo.
In particolare, essi si distinguono nelle seguenti categorie:

• **dati "comuni" che permettono l'identificazione diretta** - come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. - **e l'identificazione indiretta**, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa);

• **dati rientranti in categorie particolari:** si tratta dei "*dati che rivelino l'origine razziale od etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale di una persona"* (art.9 GDPR);

• **dati relativi a condanne penali e reati**: si tratta dei dati c.d. *"giudiziari"*, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

5. CLASSIFICAZIONE DEL DATA BREACH

Il **WP29** (Gruppo di lavoro ex art. 29) ha classificato tre categorie generali di violazioni:

- **Violazione della riservatezza** – in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali, come ad esempio:
  - quando nella redazione di un atto non si redige la versione con omissione dei dati da non pubblicare e l'atto viene pubblicato nella sua interezza;
  - quando si inoltrano messaggi contenenti dati a soggetti non interessati al trattamento;
  - quando un operatore abbandona la propria postazione di lavoro senza prima prendere le opportune precauzioni (riporre la documentazione, lasciare attive procedure sulla risorsa informatica utilizzata, ecc..) e terze persone possono prendere visione di informazioni;
  - quando un soggetto in malafede comunica dei dati non pubblici a terzi in modo non autorizzato.

- **Violazione dell'integrità** – in caso di alterazione non autorizzata o accidentale dei dati personali. L' "alterazione" è la situazione in cui i dati sono danneggiati, corrotti o non più completi. L'alterazione non autorizzata può essere la conseguenza di un attacco esterno o di una manipolazione inconsapevole da parte di personale non competente. Un'alterazione accidentale si può verificare per errore umano (ad es. nel momento di un aggiornamento delle informazioni) o per un disguido tecnico quando all'interno di una base dati si perdono i collegamenti a determinate informazioni (integrità referenziale);

- **Violazione della disponibilità** – in caso di accidentale o non autorizzata perdita di accesso o distruzione di dati personali.
  La "perdita di dati" è la situazione in cui i dati, presumibilmente, esistono ancora, ma il titolare ne ha perso il controllo o la possibilità di accedervi; la "distruzione" dei dati personali è la condizione in cui i dati non esistono più o non esistono più in un formato che sia utilizzabile dal titolare.

La violazione dei dati può avvenire a seguito di un attacco informatico, di un accesso abusivo, di un incidente (es. incendio, allagamento, etc.) o per la perdita di un supporto informatico (smartphone, notebook, chiavetta USB, etc.) o per la sottrazione di documenti con dati personali (furto, etc.).
A seconda delle circostanze, una violazione può riguardare anche tutti gli aspetti sopra indicati o una combinazione di essi.
La casistica è molto ampia.
A titolo esemplificativo, l'oggetto della segnalazione di un data breach può essere:

- l'accesso abusivo (ad esempio: accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- dati cancellati accidentalmente o da soggetti non autorizzati;

- perdita della chiave di decriptazione;
- dati persi dall'ambiente di produzione che non possano essere ripristinati integralmente dalle copie di sicurezza e si debba provvedere manualmente alla loro ricostruzione;
- interruzione significativa di un servizio ("black out" elettrico o attacchi di tipo "denial of service").
- divulgazione di dati confidenziali a persone non autorizzate;
- infedeltà aziendale (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
- perdita o il furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o il furto di documenti cartacei;
- pirateria informatica;
- virus o altri attacchi al sistema informatico o alla rete aziendale;
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "owner";
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
- invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

6. PRINCIPALI RISCHI CONNESSI AL DATA BREACH

La violazione dei dati può comportare elevati rischi per i diritti e le libertà delle persone fisiche.
I rischi principali sono:

- danni fisici, materiali o immateriali alle persone fisiche,
- perdita del controllo dei dati personali,
- limitazione dei diritti, discriminazione,
- furto di identità,
- perdite finanziarie, danno economico o sociale,
- decifratura non autorizzata della pseudonimizzazione,
- pregiudizio alla reputazione,
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

7. DESTINATARI DELLA PROCEDURA DI GESTIONE DEL DATA BREACH

La presente procedura interna è obbligatoria per tutti:

- **Gli AUTORIZZATI** al trattamento: lavoratori dipendenti e terzi non dipendenti che hanno accesso ai dati personali trattati nel corso della propria attività lavorativa presso la ASL BR;
- **I RESPONSABILI ESTERNI** ex art. 28 GDPR che, in ragione del rapporto contrattuale in essere con il Titolare, trattano dati per conto dello stesso.

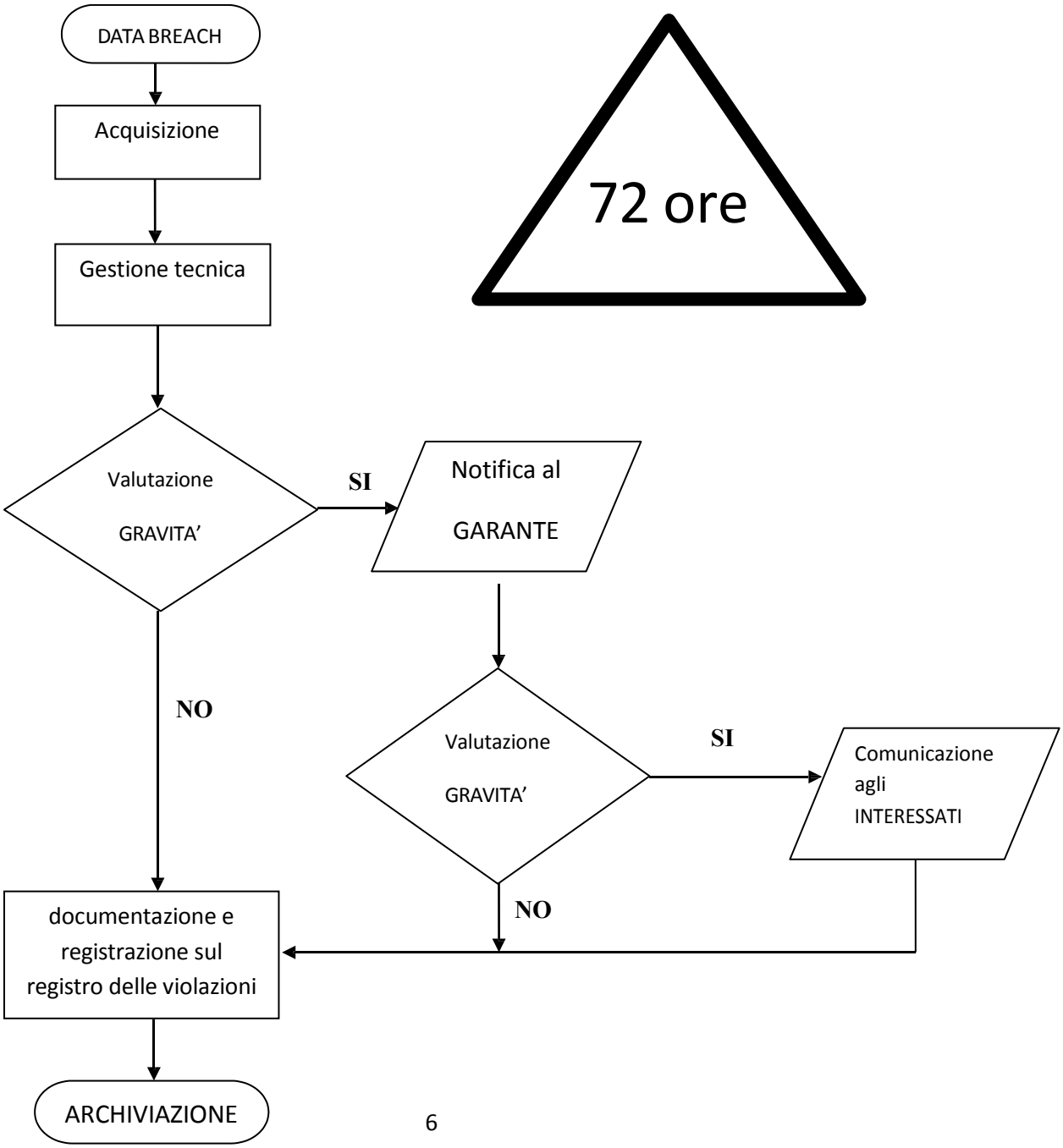
La mancata conformità alle regole di comportamento previste dalla stessa può comportare provvedimenti disciplinari a carico dei dipendenti inadempienti, ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.

8. CONTENUTO DELLA SEGNALAZIONE

Per la segnalazione del DATA BREACH occorre debitamente compilare il modello allegato alla presente ed identificato come **allegato A)**.
Ai fini di una corretta analisi della segnalazione, è necessario raccogliere fatti concreti prima di segnalare qualsiasi tipo di violazione, illecito ed irregolarità in ambito di tutela dei dati personali.
A tal fine le segnalazioni devono essere fondate su elementi di fatto precisi, circonstanziati e concordanti.

9. FASI DELLA PROCEDURA "DATA BREACH"

1) ACQUISIZIONE	A) rilevazione evento ed invio segnalazione B) raccolta informazioni C) comunicazione DATA BREACH
2) GESTIONE TECNICA	A) accertamento B) raccolta informazioni C) definizione soggetti coinvolti D) Eventuali azioni correttive
3) VALUTAZIONE D'IMPATTO	
4) NOTIFICA AL GARANTE (eventuale)	
5) SEGNALAZIONE EVENTUALE AD ALTRE AUTORITA' (ORGANI DI POLIZIA, ECC.)	
6) COMUNICAZIONE AGLI INTERESSATI (eventuale)	
7) REGISTRAZIONE DELLA VIOLAZIONE	



FASI DELLA PROCEDURA "DATA BREACH"

F	ATTIVITA'	SOGGETTI TENUTI	DESTINATARI	TERMINE	MODALITA'
1.A	**RILEVAZIONE EVENTO ED INVIO SEGNALAZIONE**	• Tutto il personale dipendente e non, in servizio presso la ASL BR • Responsabili	• Responsabile amministrativo della struttura di riferimento • Designato al trattamento • RPD	Appena si viene a conoscenza del Data Breach	utilizzando le vie più brevi (telefono, di persona, e-mail)
1.B	**RACCOLTA INFORMAZIONI**	Il responsabile della struttura, insieme ai soggetti coinvolti nella violazione		Appena ricevuta la segnalazione	Compilando il modello A) e raccogliendo informazioni dai soggetti coinvolti nella segnalazione e nel trattamento dei dati violati
1.C	**COMUNICAZIONE DATA BREACH**	Il responsabile della struttura, insieme ai soggetti coinvolti nella violazione (compilazione modello predisposto a tale scopo - all.A)	• Titolare • Designato al trattamento • RPD	Appena ottenute informazioni sulla violazione e comunque entro e non oltre 12 ore	Utilizzando le vie più brevi per l'invio del modello A) debitamente compilato
2	**2.A ACCERTAMENTO** **2.B RACCOLTA INF.** **2.C DEFINIZIONE INTERESSATI** **2.D EVENTUALI AZIONI CORRETTIVE**	• Titolare • Designato al trattamento • Amministratore di sistema (per trattamenti informatizzati) • Responsabili delle strutture coinvolte • RPD	Ai soggetti incaricati di svolgere le relative attività	Appena Ricevuta la comunicazione	Devono essere indicate in dettaglio le operazioni da svolgere, i tempi di attuazione, la previsione di eventuali operazioni di verifica dell'efficacia delle misure correttive
3	**VALUTAZIONE D'IMPATTO**	• Titolare; • Designato al trattamento • Amministratore di sistema (per trattamenti informatizzati) • RPD		Appena ricevuta la comunicazione	Seguendo la metodologia indicata nel successivo par. **10.3**
4	**EVENTUALE NOTIFICA AL GARANTE PRIVACY (se necessaria)**	• Titolare con il supporto del RPD	GARANTE	Entro 72 ore dalla conoscenza del data breach	Mediante la modulistica predisposta dal Garante

F	ATTIVITA'	SOGGETTI TENUTI	DESTINATARI	TERMINE	MODALITA'
5	**SEGNALAZIONE AD ALTRE AUTORITA' (ORGANI DI POLIZIA, ECC.)**	Titolare	ALTRE AUTORITA'		
6	**EVENTUALE COMUNICAZIONE AGLI INTERESSATI (se necessaria)**	• Titolare Con il supporto del RPD	Alle persone fisiche i cui dati sono stati violati	Nei termini indicati nella valutazione d'impatto	Comunicazione diretta alle persone fisiche interessate delle eventuali conseguenze della violazione dei dati, ovvero mediante pubblicazione sul sito istituzionale della ASL BR
7	**REGISTRAZIONE DEL DATA BREACH**	RPD		• Al momento della comunica-zione; • al momento della chiusura; • al momento della ricezione della risposta del Garante	Registrazione della violazione/ aggiornamenti; Registrazione della risposta del Garante; Registrazione della prosecuzione/ chiusura dell'incidente
8	**RECEPIMENTO DELLA RISPOSTA DEL GARANTE ALLA NOTIFICA (SE EFFETTUATA**	• Titolare • RPD			Disposizioni per l'attuazione delle eventuali misure correttive indicate dal Garante; ulteriori indagini

10. DESCRIZIONE DELLE FASI

10.1 ACQUISIZIONE DEL DATA BREACH (RILEVAZIONE EVENTO, INVIO SEGNALAZIONE, RACCOLTA INFORMAZIONI E COMUNICAZIONE DATA BREACH)

Ogni Autorizzato al trattamento, qualora venga a conoscenza della concreta, sospetta e/o avvenuta violazione dei dati personali, la segnala immediatamente al Responsabile amministrativo della struttura di riferimento, al Designato al trattamento ed al RPD; compila, unitamente al Responsabile della struttura, il Modello A) allegato alla presente e lo invia al Titolare, al Designato al trattamento e al RPD entro 12 ore dalla conoscenza dei fatti.

10.2 GESTIONE TECNICA (ACCERTAMENTO, RACCOLTA INFORMAZIONI, DEFINIZIONE SOGGETTI COINVOLTI, EVENTUALI AZIONI CORRETTIVE)

Il Titolare, unitamente al Responsabile della Protezione dei Dati, al Designato al trattamento, all'Amministratore di sistema (per trattamenti informatizzati), avvia tempestivamente le attività sopra indicate ed in particolar modo le azioni correttive necessarie per gestire tecnicamente la violazione e per ripristinare, se del caso, la disponibilità e l'accesso dei dati personali (ad es. riparazione fisica di strumentazione; utilizzo dei file di back up per recuperare dati persi o

danneggiati; isolamento/chiusura di un settore compromesso della rete; cambio dei codici di accesso… ecc.).
Dovranno anche essere desunte informazioni circa la natura dell'incidente occorso, le misure preventive poste in essere per evitarlo e le misure adottate per minimizzarne le conseguenze.
Si dovranno comunicare al Titolare notizie aggiuntive, quali:
• la causa e la natura del disservizio o della rottura;
• tempi previsti per la riparazione;
• i tempi e le modalità per il ripristino della disponibilità dei dati;
• l'esistenza di misure adottate precedentemente all'evento per contrastare il rischio;
• l'eventualità di perdita di dati durante il ripristino, la loro tipologia, se i dati sono reperibili in altre aree dei sistemi o presso terzi e le tempistiche per il recupero.

10.3 VALUTAZIONE DI IMPATTO

Il Titolare, unitamente al Designato al trattamento e all'Amministratore di sistema (per trattamenti informatizzati) effettua una valutazione di impatto dell'evento verificatosi, consultandosi con il Responsabile della Protezione dei Dati ed avvalendosi, se nel caso, di eventuali altre professionalità necessarie per la corretta analisi della situazione.
In particolare:

A) identifica la violazione ed individua a quale categoria può appartenere (fra quelle identificate dal WP29:

- **di riservatezza**, quando si verifica una divulgazione o un accesso ai dati non autorizzato o accidentale;
- **di integrità,** quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
- **di disponibilità**, quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata.

B) Valuta il rischio connesso alla violazione.

Il livello di rischio è definito sulla base di due parametri, gravità e probabilità:

GRAVITA' rilevanza degli effetti pregiudizievoli che la violazione è in grado di produrre sui diritti e le libertà delle persone coinvolte	Impatto della violazione sui diritti e le libertà delle persone coinvolte: • Basso: nessun impatto • Medio: impatto poco significativo, reversibile • Alto: impatto significativo, irreversibile
PROBABILITA' grado di possibilità che si verifichino uno o più eventi temuti (es. la perdita di ogni traccia dei dati).	Possibilità che si verifichino uno o più eventi temuti • Basso: l'evento temuto non si manifesta • Medio: l'evento temuto potrebbe manifestarsi • Alto: l'evento temuto si è manifestato

Ai fini della identificazione dei valori da attribuire ai due parametri per la valutazione del rischio, occorre considerare anche i seguenti fattori:

- tipo di violazione,
- natura, sensibilità e volume dei dati personali;
- facilità di associare i dati violati ad una persona fisica;
- gravità delle conseguenze per gli interessati;
- particolarità degli interessati (es. minori);
- particolarità degli autorizzati al trattamento (es. personale sanitario);
- numero degli interessati esposti al rischio.

	GRAVTA’		
PROBABILITA’	A	M	B
	M		
	B		

C) appura se la violazione determina o meno l’obbligo di notifica e/o comunicazione al Garante, agli interessati e ad altre Autorità.

.

	DESCRIZIONE	NOTIFICA AL GARANTE	COMUNICAZIONE AGLI INTERESSATI
RISCHIO’	BASSO	NO	NO
	MEDIO	SI	NO
	ALTO	SI	SI

Nel caso in cui si constati l’assenza di rischi, il Responsabile della Protezione dei Dati è tenuto a registrare la violazione sul registro delle violazioni, annotando le motivazioni che hanno portato a non notificare l'evento al Garante Privacy.

10.4 NOTIFICA AL GARANTE

All’esito della valutazione, qualora si sia ritenuto probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche, il Responsabile della Protezione dei Dati predispone la notifica all’Autorità Garante, a firma del Titolare, utilizzando il modulo pubblicato sul sito www.garanteprivacy.it, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui il Titolare ne è venuto a conoscenza.
La notifica deve avere il **contenuto** previsto dall'art. 33 del GDPR e pertanto deve:

1. *descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione, nonché le categorie ed il numero approssimativo di registrazioni dei dati personali in questione;*
2. *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;*
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 per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.*

Oltre il termine delle 72 ore, la notifica deve essere corredata anche delle ragioni del ritardo.
E’ possibile comunicare successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il Titolare sia venuto a conoscenza, a seguito di ulteriori indagini.

10.5 SEGNALAZIONE AD ALTRE AUTORITA’

Il Titolare, qualora necessario, comunica la violazione di dati alle altre Autorità competenti (Autorità giudiziaria, ecc.), a mezzo gli Uffici ASL BR preposti.

10.6 COMUNICAZIONE AGLI INTERESSATI

Nel caso in cui si valuti che il *data breach* presenti un elevato rischio per i diritti e le libertà delle persone fisiche, occorre effettuare la comunicazione agli interessati della predetta violazione dei dati, da inviarsi nei tempi e nei modi più opportuni come specificato nell'art. 34 del GDPR e tenendo conto di eventuali indicazioni fornite dall'Autorità Garante.

In tal caso, nella eventuale comunicazione si dovranno indicare i seguenti dati:

a) la natura della violazione dei dati personali, descritta con linguaggio semplice e chiaro;
b) 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) le probabili conseguenze della violazione dei dati personali;
d) le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione. e, se del caso, per attenuarne i possibili effetti negativi.

A norma dell'art. 34, comma 3, non è richiesta la comunicazione all'interessato se:

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;
c) nel caso in cui la comunicazione diretta richieda uno sforzo ritenuto sproporzionato, si potrà utilizzare una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

10.7 REGISTRAZIONE DELLA VIOLAZIONE

Il Responsabile della Protezione dei Dati, in caso di una violazione dei dati, deve procedere alla registrazione del *data breach* nell'apposito Registro delle violazioni (art.33, comma 5 del GDPR), da compilare secondo il modello allegato alla presente ed identificato come **allegato B),** documentando qualsiasi violazione dei dati personali, comprese le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.
In caso di assenza di rischi per i dati personali, deve annotare e documentare i motivi della mancata notifica al Garante Privacy in modo da comprovare la effettiva assenza dei rischi.
Tutta la documentazione relativa alle segnalazioni deve essere archiviata.

10.8 RECEPIMENTO DELLA EVENTUALE RISPOSTA DEL GARANTE

Il Titolare dispone ulteriori indagini o eventuali misure correttive, secondo le disposizioni ricevute dal Garante.

11. GESTIONE DEL DATA BREACH ESTERNO ALLA ASL BR

Il Responsabile del Trattamento ex art. 28 del GDPR è tenuto ad osservare la presente procedura di gestione del *data breach* e ad informare il Titolare del trattamento senza ingiustificato ritardo di ogni potenziale evento di violazione dei dati.
Per "ingiustificato ritardo" si considera la notizia pervenuta al Titolare al più tardi entro 12 ore dalla conoscenza iniziale da parte del responsabile.
La segnalazione del *data breach* dovrà essere inviata agli indirizzi indicati nell'atto di nomina a Responsabile del trattamento.

12. DIFFUSIONE DELLA PROCEDURA

La presente procedura dovrà essere divulgata in modo capillare e dovrà essere pubblicata sul sito internet istituzionale della ASL BR nella sezione privacy.

ALLEGATO A

MODULO DI COMUNICAZIONE DATA BREACH

Da inviare a: E-mail: responsabileprotezionedati@asl.brindisi.it;
direzionegenerale@asl.brindisi.it;
Pec: protocollo.asl.brindisi@pec.rupar.puglia.it

Data dell'incidente	○ Data_____ ○ Tra il_____ed il _____ ○ In un tempo non ancora determinato ○ Ancora in corso
Data della scoperta della violazione	
Luogo della violazione **(Indicare la Struttura/il reparto/l'ufficio..)**	○ Luogo _____ ○ Struttura _____ ○ Reparto/Ufficio _____
Nome della persona che ha riferito della violazione	
Dati di contatto della persona che ha riferito della violazione (indirizzo e-mail, numero telefonico)	
Breve descrizione della violazione di dati personali	
Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili, ecc.	
Denominazione della/e banca/che dati oggetto di Data Breach	
Modalità di esposizione al rischio **Tipo violazione**	○ Lettura (presumibilmente i dati non sono stati copiati) ○ Copia (i dati sono ancora presenti sui sistemi del titolare) ○ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati) ○ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione) ○ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione) ○ Altro:

Dispositivo oggetto della violazione	○ Computer ○ Dispositivo mobile ○ Documento cartaceo ○ File o parte di un file Strumento di backup ○ Rete ○ Altro:
Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione	
Categoria e numero approssimativo degli Interessati colpiti dalla violazione di dati personali	○ Categoria _____ ○ N._____di persone ○ Circa_____persone ○ Un numero (ancora) sconosciuto di persone
Tipologia di dati coinvolti nella violazione	○ Dati anagrafici ○ Numero di telefono (fisso o mobile) ○ Indirizzo di posta elettronica ○ Dati di accesso e di identificazione (user name, password, customer ID, altro) ○ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro) ○ Altri dati di personali (sesso, data di nascità, età, ...), ○ dati sensibili e giudiziari ○ Ancora sconosciuto
Livello di gravità della violazione dei dati personali (secondo le valutazioni dell' Area/Ufficio)	○ Basso/trascurabile ○ Medio ○ Alto
Finalità del trattamento	
Misure tecniche e organizzative applicate ai dati colpiti dalla violazione	

Luogo, Data,

FIRMA_____

ALLEGATO B

REGISTRO DATA BREACH

N°prog.	Data della violazione	Luogo della violazione (Struttura…)	Descrizione della violazione	Tipologia della violazione	Categorie di interessati e numero approssimativo	Categorie di dati personali e numero approssimativo	Cause della violazione	Conseguenze della violazione	Misure correttive, responsabilità e data di attuazione	Gravità	Probabilità	Rischio	Necessità di notifica al Garante e data	Necessità di comunicazione agli interessati e data	Motivazioni della mancata notifica o comunicazione	Verifica attuazione misure e data di	Verifica efficacia misure e data di verifica