azienda sanitaria locale matera

SERVIZIO SANITARIO NAZIONALE

REGIONE BASILICATA

AZIENDA SANITARIA MATERA

PROCEDURA GENERALE SANITARIA

Cod. PGS-URP-04-15

Procedura

PROCEDURA GESTIONE VIOLAZIONI DATI PERSONALI - DATA BREACH

Elenco emissioni/approvazioni/revisioni

Rev.	Redazione		Verifica		Approvazione	
0.0	Data 16/12/2021	U.O.S.D- Medicina Legale e Gestione Rischio Clinico Dirigente Dr.ssa Valeria Bruno U.O.C Innovazioni Tecnologiche e Attività Informatiche – Ingegneria Clinica Dirigente Ing. Teresa Bendicovanni U.O.S.D. U.R.P.-Comunicazione – Ufficio Stampa – Privacy Dott.ssa Rosalba Mangiacotti Dott.ssa Angela Divincenzo I.D.F. Gestione Sistema Documentale della Qualità Dott.ssa Chiara Gentile (Con la consulenza di Liguria Digitale Spa)	Data 17/12/2021	Resp. U.O.S.D. U.R.P.-Comunicazione – Ufficio Stampa – Privacy Dott. Achille Spada Direttore SIC Medicina Legale e Gestione del Rischio Clinico Dr. Aldo Di Fazio Resp. SGQ Dott.ssa A. Brala Resp. I.D.F. Gestione Sistema Documentale della Qualità Dott.ssa Chiara Gentile DPO Ing. Maurizio Pastore MAURIZIO PASTORE 17.12.2021 15:35:07 GMT+00:00	Data 21/12/2021	GERLI MASSIMILIANO 2021.12.21 18:31:39 CN=GERLI MASSIMILIANO C=IT 2.5.4.4=GERLI 2.5.4.42=MASSIMILIANO RSA/2048 bits Direttore Amministrativo Aziendale Dr. Massimiliano Gerli Direttore Sanitario Aziendale Dr. Giuseppe Magno

Ratifica	Data: 22/12/2021	Direttore Generale Dr.ssa Sabrina Pulvirenti

Distribuzione:

■ copia originale

X copia in distribuzione controllata ___ copia in distribuzione non controllata

Note:

La responsabilità dell'eliminazione delle copie obsolete della Procedura è dei destinatari di questa documentazione. Le copie aggiornate sono presenti nella rete intranet aziendale

INDICE

1. PREMESSA

La presente procedura di gestione delle violazioni dei dati personali, o "Data Breach", ha lo scopo di fornire le indicazioni operative in caso di violazione dei dati personali di cui l'Azienda Sanitaria Locale di Matera è titolare del trattamento.
Una violazione dei dati personali (di seguito "data breach") può scaturire sia dall'interno che dall'esterno dell'Azienda e, qualora non affrontata tempestivamente e in maniera adeguata, può comportare pericoli significativi per la privacy degli interessati cui i dati si riferiscono (es. discriminazioni, furti di identità, perdite economiche, pregiudizi alla reputazione,ecc).
Le violazioni della privacy più comuni sono quelle derivanti dall'errore umano. Basti pensare alla consegna o alla comunicazione di documenti contenenti dati particolari alla persona sbagliata (es. referto del paziente Caio nella cartella del paziente Tizio; invio documentazione sanitaria a persona sbagliata, furto/smarrimento di agende, documentazione clinica, etc.).
I possibili scenari di violazione dei dati sono sicuramente aumentati con l'avvento della società digitale. Gli operatori devono, pertanto, sviluppare la capacità di riconoscere ed affrontare le potenziali conseguenze, ad esempio sulle cure di un paziente, di eventi pregiudizievoli quali un accesso non autorizzato (hacheraggio o cessione di credenziali, furto di appunti sulle password), una modifica erronea di un database, un malfunzionamento di uno strumento informatico o il furto o perdita di un dispositivo (smartphone o chiavetta USB, telefonino aziendale) contenente dati di estrema delicatezza (dati sullo stato di salute), o la comunicazione di dati attraverso strumenti a larga diffusione (invio massivo di email o pubblicazione dati sul web).
La presente procedura è valida per tutti quei trattamenti di cui l'Azienda è titolare.

2. SCOPO/OBIETTIVO

Scopo della presente procedura è pianificare anticipatamente la messa in atto di 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 e comunicarla alle persone fisiche interessate; definire i compiti, le responsabilità e le modalità operative in caso di violazione dei dati personali trattati da o per conto dell'Azienda Locale di Matera.
La suddetta procedura consente al Titolare del trattamento dei dati personali dell'ASM di Matera di porre in atto quanto previsto dagli articoli 33 e 34 del Regolamento (UE) 2016/679 e delle Linee Guida sulla notifica delle violazioni dei dati ai sensi del regolamento (UE) 2016/679, elaborate ed adottate dal Gruppo di lavoro ex art 29 della direttiva 95/46/CE. Nonchè le successive Guidelines 01/2021 on Examples regarding Data Breach Notification.
La ASM di Matera effettua taluni trattamenti nell'ambito del Decreto Legislativo 18 maggio 2018, n. 51 "Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorita' competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali", segnatamente qualora il proprio personale agisca nel ruolo di Ufficiale di Polizia Giudiziaria e/o provveda a comminare sanzioni

amministrative a carattere repressivo. In tali casi la notifica è dovuta sulla base dell'art. 26 del citato D.lgs. 51 e l'eventuale comunicazione agli interessati è prescritta dal successivo art. 27. Entrambi gli articoli fanno esplicito riferimento rispettivamente agli art. 33 e 34 del G.D.P.R. In tali casi nella notifica dovrà essere indicato il diverso riferimento normativo.
In particolare, la predisposizione della presente procedura consente di:

- definire i ruoli e le responsabilità organizzative per la gestione di un data breach;
- fornire a chi a diverso titolo tratta dati all'interno dell'Azienda Sanitaria Locale di Matera (di seguito ber brevità "Azienda"), nonché a chi tratta dati per conto dell'Azienda (Responsabili del Trattamento), indicazioni pratiche e modalità operative per riconoscere e gestire situazioni relative a violazioni di dati al fine di minimizzarne l'impatto e di prevenirne la reiterazione;
- fornire l'opportuna modulistica.

Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti; e la mancata osservanza di quanto in essa previsto potrà comportare l'adozione di provvedimenti disciplinari ovvero giusta causa di risoluzione dei contratti in essere a carico rispettivamente di dipendenti, collaboratori a vario titolo (specializzandi, tirocinanti, sumaisti, borsisti, ect), fornitori o terzi parti inadempienti.

3. CAMPO DI APPLICAZIONE

La presente procedura deve essere applicata in tutti i casi in cui si verifichi una potenziale ma attuale rischio di perdita, distruzione o diffusione indebita di dati personali, ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi che possono determinare pericoli significativi per la protezione dei dati degli interessati.
La presente procedura è destinata a tutte le Strutture dell'Azienda che trattano, a qualsiasi titolo (dipendenti, universitari, borsisti, tirocinanti,..) e in qualsiasi modalità (automatizzata, manuale, digitale, cartacea), dati all'interno dell'Azienda, nonché ai Responsabili che trattano i dati per conto dell'Azienda.
La procedura è destinata a tutti i dipendenti e collaboratori dell'Azienda individuati quali soggetti designati ai sensi dell'art. 2-quaterdecies del D.Lgs. 196/2003 come modificato dal D.lgs. 101 del 10 agosto 2018, e pertanto autorizzati a trattare dati personali di cui l'Azienda Sanitaria Provinciale di Matera è titolare.
La procedura è rivolta altresì a qualsiasi soggetto, persona fisica o giuridica, che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento effettua un trattamento di dati personali in qualità di Responsabile esterno del trattamento ex art. 28 G.D.P.R..

4. RIFERIMENTI NORMATIVI E DOCUMENTALI UTILI

- Regolamento (UE) 2016/679 del Parlamento Europeo del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in particolare gli articoli 33 (Notifica all'Autorità di Controllo), 34 (notifica agli interessati) e 28 (Responsabile del trattamento)

- D. Lgs. 196/2003 Codice per la protezione dei dati personali
- Decreto Legislativo 18 maggio 2018, n. 51 "Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorita' competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali"
- Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) – WP250, definite in base alle previsioni del Regolamento (UE) 2016/679
- Decreto Legislativo 10 agosto 2018 n, 101 "Disposizioni per l'adeguamento della Normativa Nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)"
- Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche – 2 luglio 2015, come modificata Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) – 30 luglio 2019 [9126951]
- Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) – 30 luglio 2019 [9126951]
- Provvedimento del 27 maggio 2021 – Procedura telematica per la notifica di violazioni di dati personali (data breach)
- https://servizi.gpdp.it/databreach/s/self-assessment
- https://servizi.gpdp.it/databreach/s/istruzioni
- https://servizi.gpdp.it/databreach/resource/1625230706000/DB_Istruzioni
- Linee guida in materia di valutazione d'impatto sulla protezione dei dati
- ENISA Raccomandazioni in merito a una metodologia di valutazione della gravità di una violazione dei dati personaliApertura sito esterno in una nuova scheda per Raccomandazioni in merito a una metodologia di valutazione della gravità di una violazione dei dati personali – Metodologia Enisa
- D.Lgs. 82/2005 Codice dell'Amministrazione Digitale (CAD)
- Artt. 331 e 361 del Codice di Procedura Penale (obbligo di denuncia da parte del pubblico ufficiale)
- Decreto 9 gennaio 2008 del ministero degli interni in attuazione della Legge 155/2005 sulle infrastrutture critiche
- Direttiva (UE) 2016/1148 (Direttiva NIS) del Parlamento europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione Europea
- Prescrizione del WP29 "Guidelines on Personal data breach notification under Regolation 2016/679", adottate il 03.10.2017 (ultima revision 06/02/2018)
- Prescrizioni dell'EDPB "Guidelines 01/2021 on Examples regarding Data Breach Notification"
- Decreto Legislativo 18 maggio 2018 n. 65, Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione

- Circolare 18 aprile 2017, n. 2/2017,recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del PCM 01.08.2015, pubblicata in G.U. Serie generale n. 103 del 5.5.2017
- Direttiva 95/46/CE del Parlamento Europeo e del Consiglio del 24 Ottobre 1995

5. ABBREVIAZIONI,DEFINIZIONI, TERMINOLOGIA

GLOSSARIO E ABBREVIAZIONI	
Terminologia, Abbreviazione	**Definizione**
G.D.P.R.	Regolamento (UE) 2016/679 del Parlamento Europeo del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in particolare gli articoli 33 (Notifica all'Autorità di Controllo), 34 (notifica agli interessati) e 28 (Responsabile del trattamento)
AGID	Agenzia per l'Italia Digitale
CAD	Codice dell'Amministrazione Digitale
NIS	Network and Information Security
RSPP	Responsabile Servizio Prevenzione e Protezione
WP29	Working Party Art. 29 - Gruppo di lavoro Art. 29 - dal 25/05/2018 EDPB (European Data Protection Board – Comitato Europeo per la Protezione dei Dati)
TITOLARE DEL TRATTAMENTO	L'Autorità Pubblica (Rappresentante Legale dell'Azienda Sanitaria Locale di Matera) che singolarmente o insieme ad altri, determina la finalità e i mezzi del trattamento dei dati personali
CONTITOLARE	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, insieme ad altri determina le finalità e i mezzi di trattamento dei dati personali
RPD (o D.P.O.)	Responsabile della Protezione dei Dati (o Data Protection Officer): la persona individuata dal Titolare del Trattamento dei dati quale responsabile della protezione dei dati all'interno dell'Azienda che determina specifiche modalità organizzative rispetto ad uno o più trattamenti
RESPONSABILE DEL TRATTAMENTO	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento
SUB RESPONSABILE	La persona fisica o giuridica designata dal responsabile del trattamento previa autorizzazione scritta del titolare del trattamento
TRATTAMENTO DEI DATI	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione
INTERESSATO	Persona fisica identificata o identificabile. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

SOGGETTO DESIGNATO	I Direttori di Struttura Complessa, i dirigenti responsabili.
AUTORIZZATO	Per persona fisica, espressamente designata, che opera sotto l'autorità del Titolare del trattamento, con specifici compiti e funzioni connessi al trattamento dei dati personali. Art. 4.10 G.D.P.R.
INCIDENTE DI SICUREZZA	Evento singolo o una serie di eventi di sicurezza non voluti o inaspettati che hanno una significativa probabilità di compromettere il funzionamento di processi aziendali (ISO 27000)

6. PROCESSO/MODALITA' OPERATIVE

6.1. Definizione di violazione dei dati personali (Data Breach)

Un data breach è, secondo la definizione fornita dall'art. 4 par. 12 del Regolamento Generale sulla Protezione dei Dati (di seguito "G.D.P.R."), un incidente 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.
Le violazioni di dati personali possono accadere per un ampio numero di situazioni che, a titolo esemplificativo, possono includere:

- perdita, furto o violazione di documentazione cartacea
- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati
- il furto o la perdita di dispositivi informatici contenenti dati personali che appartengono all'Azienda
- 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 o altre calamità
- la divulgazione non autorizzata di dati
- l'alterazione o distruzione di banche dati senza autorizzazione rilasciata dal titolare o responsabile
- la violazione di una casella di posta elettronica aziendale.

Le violazioni, secondo le indicazioni fornite dal Gruppo di Lavoro art. 29 (della Direttiva 95/46/CE del Parlamento Europeo e del Consiglio del 24 Ottobre 1995), possono manifestarsi in diversi modi ed essere classificate in tre tipologie:

Tipologia di violazione	Evento/Minaccia
Violazione della riservatezza	Accesso o trattamento non autorizzato o illecito
	Divulgazione non autorizzata
Violazione dell'integrità	Modifica non autorizzata o accidentale
Violazione della disponibilità	Perdita o distruzione accidentale o illegale
	Indisponibilità temporanea o prolungata

A seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.
Il documento "Guidelines 01/2021 on Examples regarding Data Breach Notification" fornisce ulteriori esempi.
L'articolo 32 del "G.D.P.R." dispone che il Titolare del trattamento, nell'attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, deve tenere conto, tra le altre cose, *"della capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" e "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico".*
In caso di violazione dei dati personali, il Titolare del Trattamento deve, ex art. 33 del G.D.P.R., notificare all'autorità di controllo (Garante) la violazione senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, ma soltanto se ritiene probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati. Qualora la notifica all'Autorità di controllo non sia effettuata entro le 72 ore, la stessa è corredata dei motivi del ritardo. Ne deriva che la notifica dell'avvenuta violazione al Garante non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati. Se la probabilità del rischio è elevata, dovranno essere informati anche gli interessati.
Il criterio dirimente per valutare la necessità di avviare una procedura di notifica è pertanto la probabilità che l'incidente di sicurezza possa porre a rischio (per la notifica all'Autorità), o ad elevato rischio (per la comunicazione agli interessati) le libertà e i diritti degli individui.
Di conseguenza, un incidente di sicurezza che determina l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione da notificare al Garante e comunicare agli interessati solo qualora la mancanza di accesso alle informazioni può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche. Non configura invece una "violazione della sicurezza" l'indisponibilità dei dati personali dovuta allo svolgimento di un intervento di manutenzione programmata se accompagnata da opportune misure organizzative tese a salvaguardare i diritti e le libertà fondamentali.
Il Titolare ha il dovere di notificare al Garante nei seguenti casi:

- l'organizzazione è Titolare del/i trattamenti dei dati coinvolti nell'incidente
- l'organizzazione è Contitolare del trattamento con delega alla notifica
- l'organizzazione è Responsabile del trattamento con delega alla notifica.

Qualora la ASM Matera agisca come Responsabile del trattamento senza delega alla notifica dovrà informare immediatamente il Titolare (che ha nominato la ASM come Responsabile) ed offrire la necessaria assistenza.
Gli incidenti di sicurezza occorsi, anche se non notificati al Garante e non comunicati agli interessati, nonché l'indicazione delle circostanze e conseguenze in cui la violazione si è verificata ed i provvedimenti adottati in merito, dovranno essere comunque sempre annotati e documentati sul registro delle violazioni.

6.2. Fasi del Processo di Gestione del Data Breach

Il processo di gestione di una violazione concreta, potenziale o sospetta dei dati si articola nelle seguenti fasi:

1	Predisposizione strumenti
2	Rilevazione Evento- Acquisizione Notizia avvenuto incidente
3	Analisi preliminare e invio segnalazione
4	Gestione (contenimento del danno) e valutazione gravità dell'evento
5	Notifica al Garante Privacy
6	Altre segnalazioni dovute: (es. agli organi di Polizia e, nel caso di incidente informatico, a CERT-PA, all'autorità NIS competente)
7	Comunicazione agli interessati, ove necessario, e raccolta riscontro dell'avvenuta comunicazione
8	Inserimento dell'evento nel Registro delle Violazioni (Comprese le violazioni che non richiedono la notifica)
9	Azioni correttive specifiche e per analogia

6.2.1 Predisposizione degli strumenti (Fase 1)

Questa fase può essere definita come "Fase 1" in quanto diretta a garantire la sicurezza dei dati attraverso l'adozione di comportamenti e di misure tecniche per prevenire e/o ridurre il rischio di incidenti di sicurezza e/o gli effetti degli stessi.
In primo luogo la sicurezza del dato è garantita dalla rigorosa applicazione dei principi previsti all'art. 5 del G.D.P.R. (principi applicabili al trattamento dei dati) ed in particolare, esemplificando, da:

- principio di minimizzazione: i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati
- periodo di conservazione dei dati: es. conservare i dati per il periodo strettamente necessario per il conseguimento delle finalità per cui sono stati raccolti
- pertinenza delle informazioni gestite rispetto alle finalità
- numero di soggetti autorizzati al trattamento
- autorizzazione dei singoli al trattamento e alle relative procedure
- l'applicazione dei principi di protezione dei dati fin dalla progettazione (Privacy by design).

Tra le misure tecniche ed organizzative da predisporre rientrano:

- le azioni di sensibilizzazione e formazione del personale
- i sensori tecnici per individuare intrusioni di rete
- gli strumenti di supporto alla procedura in oggetto (es. gestione con canali di comunicazione in caso di blocco informatico)
- la predisposizione di questa procedura
- la predisposizione di procedure sulla continuità operativa
- gli audit periodici sui trattamenti e sul sistema informativo
- gli interventi di digitalizzazione dei processi previsto dal CAD nel quadro delle misure tecniche previste.

6.2.2 Rilevazione Evento - Acquisizione notizia avvenuto incidente (Fase 2)

Il verificarsi di un evento anomalo relativo alla sicurezza delle informazioni può essere rilevato da:

- qualsiasi soggetto interno (es. personale dipendente, personale convenzionato, stagisti, tirocinanti, borsisti, specializzandi etc.);
- soggetti esterni (cittadini, pazienti, utenti);
- .Responsabile/Contitolare, Titolare (nel caso in cui l'Azienda agisca in qualità di Responsabile con delega alla notifica).

Qualunque soggetto autorizzato al trattamento dei dati personali di cui l'Azienda è titolare (soggetti designati quali Responsabili del trattamento, autorizzati), qualora rilevi una concreta, potenziale o sospetta violazione dei dati personali, procede a dare comunicazione come indicato di seguito:

- i soggetti interni devono segnalare immediatamente quanto rilevato al Direttore/Dirigente della Struttura di afferenza, o a suo delegato/sostituto, verbalmente, tramite contatto telefonico, e via e-mail o altro mezzo scritto in caso di indisponibilità della posta elettronica. In considerazione dell'importanza della tempestività delle azioni, nel caso di incidente di sicurezza in orario notturno o in giornata festiva/prefestiva, l'evento – in aggiunta - deve essere segnalato al Dirigente Medico reperibile della Direzione Sanitaria di Presidio;
- i soggetti esterni quali cittadini, pazienti, utenti tramite segnalazione all'URP;
- i soggetti esterni quali i Responsabili e altre figure Privacy quali Titolari/Contitolari, verbalmente, tramite contatto telefonico ed invio di una PEC indirizzata al relativo DEC. E' ammessa, in casi eccezionali e se giustificata, la comunicazione da parte del Responsabile esterno entro le 48 ore dall'evento o dall'avvenuta conoscenza dello stesso.

6.2.3 Invio segnalazione (Fase 3)

Il Direttore della Struttura, o suo delegato, il Medico reperibile della Direzione Sanitaria di Presidio (nel caso di evento occorso nelle ore notturne o in giornate festive), il Responsabile dell'URP, i DEC, venuti a conoscenza dell'incidente di sicurezza, attivano il processo di segnalazione dell'evento:

- dandone prima comunicazione telefonica al D.P.O. e al Titolare del trattamento (Rappresentante Legale dell'Azienda Sanitaria) anche per il tramite dell'Ufficio Privacy;
- compilando e trasmettendo – via pec - il modulo per la segnalazione "Allegato A" al D.P.O. e al Titolare del trattamento (Rappresentante Legale dell'Azienda Sanitaria).

6.2.4 Valutazione gravità dell'evento (Fase 4)

Il D.P.O., ricevuto l'allegato A, o la comunicazione telefonica, esamina il caso e svolge una breve indagine sulla base di quanto comunicato e indicato nel suddetto modulo, avvalendosi – se ritenuto opportuno – di altre figure presenti in Azienda (es. Direzione Sanitaria, Ufficio Privacy, Innovazione Tecnologica: ingegneria clinica/servizi informatica o informativi, Medicina Legale e Gestione del Rischio Clinico, RSPP, etc.).

Sulla base delle informazioni raccolte il Responsabile della protezione dati (D.P.O.) procede alla valutazione finale del rischio sulla base dei parametri e criteri indicati nel modulo "Allegato B",

verificando, il tipo di violazione, la natura e il volume dei dati personali coinvolti, la facilità di identificazione delle persone fisiche, la gravità delle conseguenze per le persone fisiche, le caratteristiche particolari dell'interessato e il numero delle persone fisiche coinvolte. Il D.P.O., sempre nell'Allegato B, propone:

- L'archiviazione della segnalazione (qualora sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche) o
- La notifica all'autorità di controllo (qualora la violazione presenti un rischio per i diritti e le libertà delle persone fisiche)
- Comunicazione agli interessati qualora il rischio risulti elevato.

Il Titolare del trattamento, sulla base delle indicazioni riportate dal Responsabile della protezione dati (D.P.O.) nell'allegato B, conferma la gravità della violazione, ovvero la possibilità che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.
Qualora il Titolare del trattamento dei dati ed il D.P.O. abbiano opinioni discordanti circa l'insussistenza del rischio per i diritti e le libertà degli interessati, la decisione sull'opportunità di notificare la violazione dei dati personali all'autorità di controllo ricadrà unicamente sul Titolare del trattamento e dovrà essere debitamente motivata.
Qualora sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche e il titolare – in accordo con il D.P.O. - ritenga non opportuno procedere alla notifica della violazione, la procedura si conclude compilando il Registro delle violazioni con annotazione delle motivazioni e scelte operate. Potranno eventualmente essere avviate misure di miglioramento per incrementare ulteriormente la protezione dei dati.

Ai fini della valutazione della gravità del Data Breach occorre considerare se:

- i dati siano stati in precedenza resi anonimi oppure pseudonimizzati;
- i dati siano stati oggetto di cifratura e se fosse garantita, al momento della violazione, la riservatezza della chiave di decifratura;
- i dati violati non siano riconducibili all'identità di persone fisiche;
- i dati siano già stati oggetto di pubblicazione.

A titolo esemplificativo si riporta la tabella seguente contenente per ogni tipologia di violazione cosa verificare e alcuni esempi.

ESEMPI VALUTAZIONE RISCHI		
Descrizione	**Cosa verificare**	**Esempi**
Tipo di violazione	Il tipo di violazione verificatosi può influire sul livello di rischio presentato per le persone fisiche?	Una violazione della riservatezza che ha portato alla divulgazione di informazioni mediche a soggetti non autorizzati può avere conseguenze diverse per una persona fisica rispetto a una violazione in cui i dettagli medici sono stati persi e non sono più disponibili.
Natura e volume dei dati personali coinvolti	La natura dei dati personali compromessi dalla violazione: maggiore è il rischio di danni per gli interessati ove questi rientrino nelle categorie particolari di dati,. Fermo quanto precede, ai fini di una puntuale valutazione occorre prendere in considerazione anche altri elementi, posto che anche la semplice violazione di dati comuni potrebbe comportare un rischio rilevante ai fini della notifica e della comunicazione. Di norma una combinazione di dati personali ha un carattere più sensibile rispetto a un singolo dato personale. Analogamente, una piccola quantità di dati personali altamente sensibili può avere un impatto notevole su una persona fisica, mentre una vasta gamma di dettagli può rivelare molte più informazioni in merito alla stessa persona. Inoltre, una violazione che interessa grandi quantità di dati personali relative a molte persone può avere ripercussioni su un numero corrispondentemente elevato di persone.	Ad esempio, violazioni relative a dati sulla salute, documenti di identità o dati finanziari come i dettagli di carte di credito, possono tutte causare danni di per sé, ma se tali dati fossero usati congiuntamente si potrebbe avere un'usurpazione d'identità.
Facilità di identificazione delle persone fisiche	Un fattore importante da considerare è la facilità con cui un soggetto che può accedere a dati personali compromessi riesce a identificare persone specifiche o ad abbinare i dati con altre informazioni per identificare persone fisiche. A seconda delle circostanze, l'identificazione potrebbe essere possibile direttamente dai dati personali oggetto di violazione senza che sia necessaria alcuna ricerca speciale per	Ad esempio, i dati personali protetti da un livello appropriato di cifratura saranno incomprensibili a persone non autorizzate che non dispongono della chiave di decifratura. Inoltre, anche una pseudonimizzazione opportunamente attuata (definita all'articolo 4, punto 5 del G.D.P.R. come *"il trattamento dei dati personali in modo tale che i dati personali non possano più essere*

	scoprire l'identità dell'interessato, oppure potrebbe essere estremamente difficile abbinare i dati personali a una particolare persona fisica, ma sarebbe comunque possibile a determinate condizioni. L'identificazione può essere direttamente o indirettamente possibile a partire dai dati oggetto di violazione, tuttavia può dipendere anche dal contesto specifico della violazione e dalla disponibilità pubblica dei corrispondenti dettagli personali. Quest'ultima eventualità potrebbe essere più rilevante per le violazioni della riservatezza e della disponibilità.	*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*") può ridurre la probabilità che le persone fisiche vengano identificate in caso di violazione. Tuttavia, le tecniche di pseudonimizzazione da sole non possono essere considerate sufficienti a rendere i dati incomprensibili.
Gravità delle conseguenze per le persone fisiche	A seconda della natura dei dati personali coinvolti in una violazione, ad esempio categorie particolari di dati, il danno potenziale alle persone che potrebbe derivarne può essere particolarmente grave soprattutto nei casi di furto o usurpazione di identità, danni fisici, disagio psicologico, umiliazione o danni alla reputazione. Parimenti, se la violazione riguarda dati personali relativi a persone fisiche vulnerabili, queste ultime potrebbero essere esposte a un rischio maggiore di Il fatto che il titolare del trattamento sappia o meno che i dati personali sono nelle mani di persone le cui intenzioni sono sconosciute o potenzialmente dannose può incidere sul livello di rischio potenziale. Prendiamo una violazione della riservatezza nel cui ambito i dati personali vengono comunicati a un terzo o ad altri destinatari per errore. Una tale situazione può verificarsi, ad esempio, nel caso in cui i dati personali vengano inviati accidentalmente all'ufficio sbagliato di un'organizzazione o a un'organizzazione fornitrice utilizzata frequentemente. Il titolare del trattamento può chiedere al destinatario di restituire o distruggere in maniera sicura i dati ricevuti. In entrambi i casi, dato che il titolare del trattamento ha una relazione continuativa con tali soggetti e	Il fatto che il destinatario sia affidabile può neutralizzare la gravità delle conseguenze della violazione. Si dovrebbe altresì tener conto della permanenza delle conseguenze per le persone fisiche laddove l'impatto possa essere considerato maggiore qualora gli effetti siano a lungo termine.

	potrebbe essere a conoscenza delle loro procedure, della loro storia e di altri dettagli pertinenti, il destinatario può essere considerato "affidabile". In altre parole, il titolare del trattamento può ritenere che il destinatario goda di una certa affidabilità e può ragionevolmente aspettarsi che non leggerà o accederà ai dati inviati per errore e che rispetterà le istruzioni di restituirli. In caso di violazione di riservatezza occorre verificare che le misure di sicurezza (es.: cifratura dei dati) in vigore rendano improbabile l'identificazione degli interessati (non compromissione della chiave, algoritmo di cifratura o impronta senza vulnerabilità note). In caso di perdita di integrità o disponibilità di dati occorre valutare se è possibile il recupero degli stessi in tempi compatibili con i diritti degli interessati danni.	
- *Caratteristiche particolari dell'interessato*	Una violazione può riguardare dati personali relativi a minori o ad altre persone fisiche vulnerabili, che possono di conseguenza essere soggette a un rischio più elevato di danno. Altri fattori concernenti la persona fisica potrebbero influire sul livello di impatto della violazione sulla stessa.	Violazioni relative a dati sulla salute relative a determinate patologie (es. paziente affetto da sclerosi multipla, HIV, etc.) possono causare rischi di discriminazione per l'interessato.
Numero di persone fisiche interessate	Una violazione può riguardare solo una o poche persone fisiche oppure diverse migliaia di persone fisiche, se non molte di più. Di norma, maggiore è il numero di persone fisiche interessate, maggiore è l'impatto che una violazione può avere. Tuttavia, una violazione può avere ripercussioni gravi anche su una sola persona fisica, a seconda della natura dei dati personali e del contesto nel quale i dati sono stati compromessi.	Un interruzione di rete per più di una giornata può riguardare dati di molte persone, determinando un maggior impatto della violazione.

Nel caso in cui si accerti che la violazione abbia compromesso dati contenuti in un sistema informatico, spetta ai Sistemi Informativi/Informatici procedere all'analisi tecnica dell'evento e all'individuazione delle azioni da porre in essere per il contenimento degli eventuali danni e il ripristino dei dati.

6.2.5 Notifica al Garante Privacy (Fase 5)

Ai sensi dell'art. 33 del G.D.P.R., la notifica del Data Breach all'Autorità di controllo (Garante della Privacy) è obbligatoria, salvo i casi in cui sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

La notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/ . Nella stessa pagina è disponibile un modello facsimile (https://servizi.gpdp.it/databreach/resource/1629905132000/DB_Istruzioni), da NON utilizzare per la notifica al Garante ma utile per vedere in anteprima i contenuti che andranno comunicati al Garante .

Ai sensi dell'art. 33 del GDPR, in caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza (decorrenti dal momento in cui gli Autorizzati, i Designati, i Responsabili e gli altri soggetti facenti parte dell'organizzazione "allargata" sono ragionevolmente certi che si è verificato un incidente di sicurezza che ha comportato una compromissione di dati), 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, essa dovrà essere corredata dei motivi del ritardo.

Se non fosse possibile fornire tutte le informazioni contestualmente, queste ultime potranno essere inviate in fasi successive senza ulteriore ingiustificato ritardo, avendo cura di dare evidenza delle motivazioni per cui tali informazioni non sono disponibili e significando che questa è l'inizio di una notifica in fasi. Si può valutare di fare una notifica cumulativa se una stessa compromissione ha riguardato la stessa tipologia di dati con le stesse modalità.

6.2.6 Altre segnalazioni dovute (es. agli organi di Polizia e, nel caso di incidente informatico, a CERT-PA, all'autorità NIS competente) (Fase 6)

Il Titolare, per il tramite del Responsabile della protezione dati (D.P.O.), provvede ad informare, ricorrendone i presupposti, altri organi quali:

- CERT-PA (in caso di incidenti informatici ai sensi della Circolare Agid n. 2/2017 del 18.04.2017);
- Organi di Polizia (in caso di violazioni di dati conseguenza di comportamenti illeciti o fraudolenti), tra cui la Polizia Postale e delle comunicazioni
- CNAIPC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche)
- al Gestore di Identità Digitale e ad Agid nel caso in cui si individui un uso anomalo di un'identità SPID (Sistema Pubblico di Identità Digitale)
- All'Autorità Competente NIS (Network and Information System – Dlgs n. 65 del 18.5.2018).

6.2.7 Comunicazione agli interessati, ove necessario, e raccolta riscontro dell'avvenuta comunicazione (Fase 7)

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

In tal caso il Titolare provvede ad informare, senza ingiustificato ritardo, gli interessati sul fatto avvenuto, sui dati violati e sulle procedure necessarie a ridurre il rischio, utilizzando il Modulo "Allegato C".

La comunicazione deve contenere, con linguaggio semplice e chiaro (art.34.2 G.D.P.R.), almeno le seguenti informazioni:

- la natura della violazione dei dati personali;
- i dati di contatto del D.P.O. o altro referente competente a fornire informazioni necessarie;
- le probabili conseguenze della violazione;
- 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.

Ai sensi dell'art. 34, paragrafo 3, non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

a) il Titolare del trattamento ha messo in atto 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) 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.

Tenuto conto della tipologia della violazione o del numero di interessati coinvolti, qualora la segnalazione ai singoli interessati comporti sforzi sproporzionati il Titolare coinvolge immediatamente l'Ufficio Stampa e l'Ufficio Relazioni con il Pubblico per procedere ad una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Possono tornare utili in questa fase i documenti dell'EDPB ("Guidelines 01/2021 on Examples regarding Data Breach Notification") e lo strumento di autovalutazione predisposto dal Garante.
https://servizi.gpdp.it/databreach/s/self-assessment

Il comma 4 dell'art. 32 del G.D.P.R. prevede che 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 (Art. 32 del G.D.P.R.) è soddisfatta.

6.2.8 Inserimento dell'evento nel Registro delle Violazioni (Comprese le violazioni che non richiedono la notifica) (Fase 8)

L'Azienda documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. A tal riguardo l'Azienda predispone un registro interno delle violazioni e delle segnalazioni di violazione dei data breach e ciò indipendentemente dalle notifiche all'autorità di controllo.

Il Registro delle violazioni dovrà contenere le informazioni di seguito riportate: (I) data della violazione; (II) data della segnalazione; (III) nominativo del segnalante; (IV) luogo della violazione; (V) descrizione della violazione; (VI) dispositivo/applicativo oggetto di violazione; (VII) categorie di dati personali coinvolti; (VIII) tipologia di violazione; (IX) categorie e numero approssimativo di soggetti interessati dalla violazione; (X) categorie e numero approssimativo di registrazioni dei dati; (XI) probabili conseguenze della violazione; (XII) valutazione del rischio per i diritti e le libertà delle persone fisiche; (XIII) misure e provvedimenti adottati; (XIV) se sia stata effettuata o meno notifica all'autorità di controllo; (XVI) se sia stata effettuata o meno la comunicazione agli interessati; (XVII) note e commenti.
Il Registro delle violazioni è tenuto in formato elettronico dal Titolare (anche per il tramite dell'Ufficio Privacy) e dal Responsabile della protezione dei dati (D.P.O.) e da questi continuamente aggiornato. Esso viene messo a disposizione del Garante per la protezione dei dati personali qualora l'Autorità chieda di accedervi.

6.2.9 Azioni correttive specifiche e per analogia (Fase 9)

Il Titolare, al termine dell'analisi dell'incidente, individua le aree vulnerabili, promuovendo l'adozione delle seguenti azioni di miglioramento:

- audit specifico e tempestivo sui trattamenti coinvolti da parte del D.P.O.
- adozione di nuovi sistemi tecnici di prevenzione/protezione e/o di sistemi di controllo/monitoraggio/allarme
- individuazione di controlli e misure di sicurezza che diminuiscano la probabilità dell'incidente o i relativi impatti sul sistema colpito e su sistemi analoghi
- valutazione su possibilità di copertura assicurativa
- programmazione azioni informative rivolte ai dipendenti
- revisione delle relazioni con Clienti e Fornitori
- pianificazione test periodici per verificare la validità della presente procedura
- revisione della procedura, se necessaria, e di eventuali altri documenti collegati.

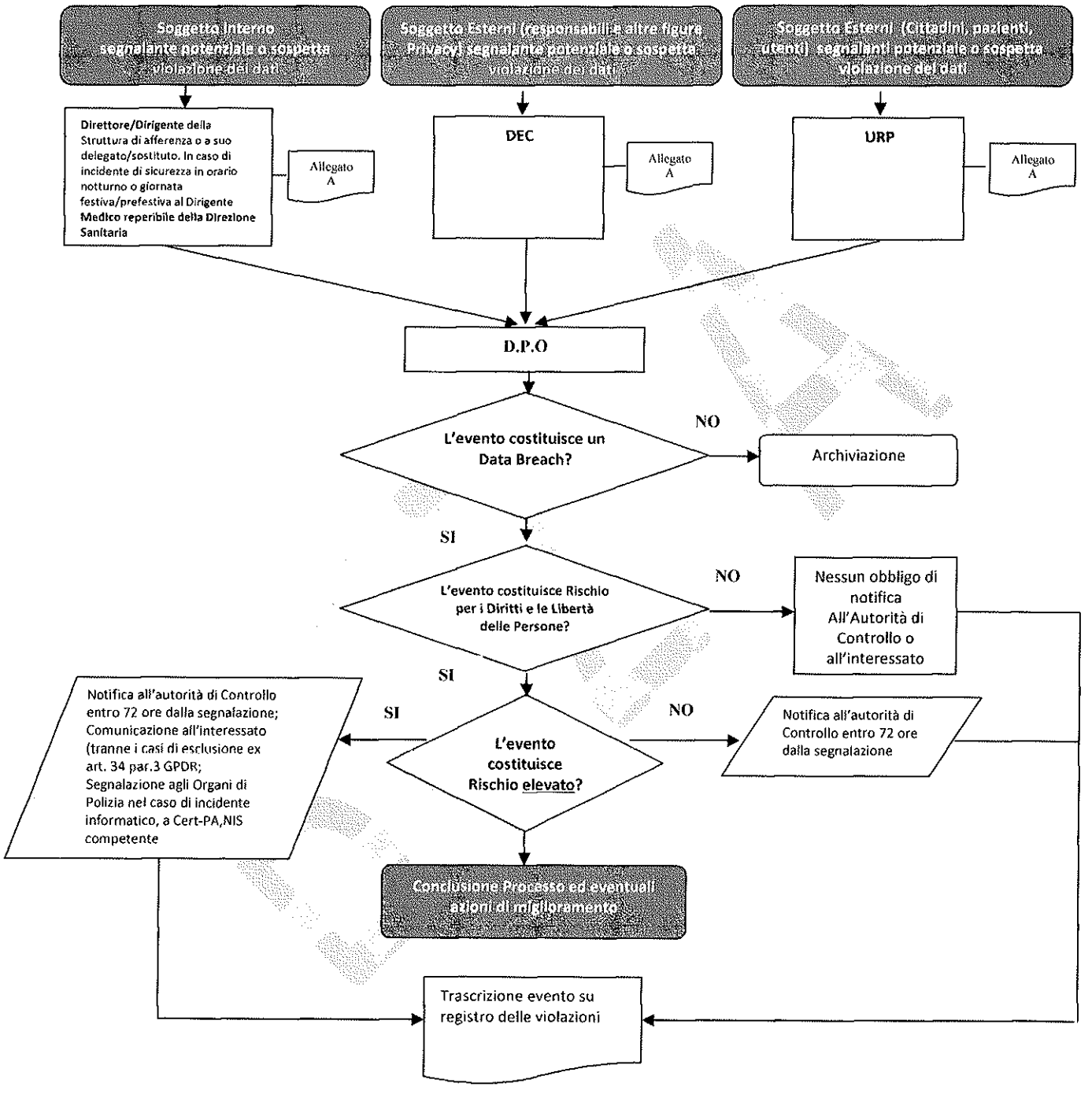
7 MATRICE DELLE RESPONSABILITA'

RACI					
Attività	**Soggetto abilitato al trattamento di dati personali (interno/esterno)**	**Direttore Struttura/ Dirigente Direzione Sanitaria di Presidio reperibile/DEC/URP**	**D.P.O.**	**Titolare trattamento dati**	**Ufficio stampa**
Rilevazione evento	R	I			
Attivazione del processo di segnalazione dell'evento		R	I	I	
Compilazione allegato A	C	R	I	I	
Valutazione gravità evento		C	R	I R	
Compilazione allegato B			R	R	
Notifica violazione dati Garante Privacy			C	R	
Notifica violazione dati altre Autorità (CERT-PA, CNAIP, AGID, Gestore Identità Digitale, Organi di Polizia, NIS)			C/R	R	

Comunicazione interessati (allegato C)			C	R	C
Compilazione registro violazioni			R	R	
Messa in atto azioni correttive	C	C	C	R	

Legenda: R: Responsabile - **C:** Coinvolto - **I:** Informato

8 DIAGRAMMA DI FLUSSO SULLE SOLE VALUTAZIONI DI ORDINE TECNICO



9 INDICATORI

Criterio	Indicatore	Standard
Tempestività	Numero ore da accertamento violazione a notifica	Entro 72 ore
Sicurezza	Numero di incidenti segnalati	Crescente
Sicurezza	Gravità degli incidenti segnalati	Decrescente
Sicurezza	Numero di violazioni annue	Tendente a zero
Sicurezza	Numero di notifiche al Garante rispetto al numero di violazioni da notificare	100%
Sicurezza	Numero di comunicazioni agli interessati rispetto al numero di violazioni ad alto rischio	100%

La finalità delle rilevazioni sulla base dei succitati indicatori è diretta ad adottare le più adeguate misure tecniche e organizzative volte alla riduzione del rischio.

10 DOCUMENTI COLLEGATI

Documenti e Individuazione dei soggetti "Designati" e dei dipendenti "Autorizzati" al Trattamento dei dati personali.

11 ALLEGATI

Allegato A – Modello per la segnalazione di violazione dei dati personali
Allegato B -Scheda di valutazione della violazione dei dati personali (Data breach) Parte prima – Valutazione del Responsabile della Protezione dei dati
Allegato C - Modello di comunicazione del data breach all'interessato

Allegato A – Modello per la segnalazione di violazione dei dati personali

Al Direttore Generale/Commissario Straordinario
Al Responsabile della protezione dei dati personali (DPO)
Azienda Sanitaria Locale di Mtera
Pec: asmbasilicata@cert.ruparbasilicata.it

Il sottoscritto .....

Contatto telefonico ..... e mail .....

In qualità di ☐ soggetto designato/incaricato del trattamento presso l'U.O. di.....
☐ Responsabile esterno del trattamento

Comunica la seguente violazione dei dati personali:

Data e ora della presunta violazione: ...../...../..... **Ore** .....
In un tempo non ancora determinato.....
E' possibile che sia ancora in corso.....
Descrizione della violazione:

.....

.....

Tipologia di violazione:

☐ Distruzione /Perdita/furto/violazione di PC desktop ☐Distruzione/ Perdita/furto/violazione di PC portatile

☐ Distruzione/Perdita/furto di dispositivi di memoria☐Distruzione/Perdita/furto/violazione documenti cartacei

☐ Virus o attacchi informatici ai sistemi aziendali ☐ Violazione di casella di posta elettronica aziendale

☐ Altro.....

Categoria di dati personali coinvolti nella violazione:

☐ Dati comuni ☐ Dati particolari ( )

Tipo di dati coinvolti (anagrafici/codice fiscale, dati di accesso e di identificazione, relativi a minori, dati che rilevino l'origine razziale, le convinzioni religiose e filosofiche, l'appartenenza sindacale, dati genetici, biometrici, relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, dati relativi a condanne penali e reati) .....
Probabili conseguenze della violazione: .....

.....

E' stata effettuata segnalazione alle Forze di polizia: ☐Si (N.B. allegare copia della denuncia), ☐ No

Altre notizie .....

.....

Data ..... . Firma.....

Allegato B -Scheda di valutazione della violazione dei dati personali (Data breach)

Parte prima – Valutazione del Responsabile della Protezione dei dati

Descrizione ed oggetto della violazione:.....

.....

Notizie raccolte successivamente alla segnalazione pervenuta: .....

.....

Tipo di data breach:

☐ Distruzione ☐Perdita ☐ Modifica

☐ Divulgazione non autorizzata ☐Accesso non autorizzato ☐ Indisponibilità temporanea del dato

Misure tecniche e organizzative applicate ai dati oggetto di violazione: .....

.....

.....

Persone coinvolte dalla violazione:

☐ N. certo di persone..... ☐N.presunto di persone..... ☐ Numero sconosciuto

Probabili rischi per i diritti e le libertà delle persone:.....

.....

Livello di gravità della violazione:

☐ Basso/trascurabile ☐Medio ☐ Alto/Molto alto

Azioni che si propone di intraprendere:

☐ Archiviazione ☐Comunicazione all'interessato

☐ Notifica all'autorità di controllo

Per le seguenti motivazioni:.....

.....

.....

Misure tecniche e azioni di miglioramento proposte:.....

.....

.....

Data ..... Il Responsabile della Protezione dei Dati

.....

Allegato B -Scheda di valutazione della violazione dei dati personali (Data breach)

Parte seconda – Valutazione del Titolare del trattamento

Probabili rischi per i diritti e la libertà delle persone:

.....

.....

Livello di gravità della violazione:

☐ Basso/trascurabile ☐ Medio ☐ Alto/Molto alto

Azioni e misure adottate:

☐ Archiviazione

☐ Notifica all'autorità di controllo

Data ed estremi della notifica all'autorità di controllo:

.....

.....

☐ Comunicazioni all'interessato:

Data ed estremi della comunicazione resa all'interessato:

.....

.....

Principali motivazioni alla base delle azioni e misure adottate:

.....

.....

Misure tecnologiche ed organizzative adottate per contenere la violazione e prevenire analoghe future violazioni:

.....

.....

.....

Note:

.....

.....

.....

Data .....

Il Titolare del trattamento

.....

Allegato C - Modello di comunicazione del data breach all'interessato

Gentile (*nome e cognome dell'interessato*),

Con la presente si comunica che l'Azienda Sanitaria Locale di Matera in data _____ è venuta a conoscenza di un evento che potrebbe aver coinvolto i Suoi dati personali.

In particolare, è accaduto quanto di seguito descritto.

Inserire breve descrizione dell'incidente in relazione al quale si ritiene necessaria la comunicazione all'interessato ed indicazione dei dati personali violate.

Dall'analisi dei fatti sopra riportati, in considerazione della natura della violazione e della tipologia di dati personali coinvolti, si comunicano le possibili conseguenze dell'evento:

Inserire descrizione delle probabili conseguenze del data breach

L'Azienda, venuta a conoscenza dell'incidente, ha tempestivamente posto in essere le seguenti misure tecniche ed organizzative:

Descrizione delle azioni già poste in essere o di cui si propone l'adozione per porre rimedio o attenuare gli effetti del data breach

Come previsto dall'art. 33 del Regolamento UE 2016/679 l'Azienda ha provveduto a notificare questa violazione al garante Privacy.

Per ricevere ulteriori conformazioni, può contattare:

Pec: asmbasilicata@cert.ruparbasilicata.it

Distinti saluti

Il Titolare del Trattamento