Sistema Socio Sanitario
Regione Lombardia
ASST Nord Milano

Azienda Socio Sanitaria Territoriale Nord Milano

Deliberazione pubblicata all'Albo Informatico dell'Azienda
Dal 01/07/2021 al 22/07/2021
Il Responsabile U.O.C. Affari Generali
(dott.ssa Silvia Liggeri)

Deliberazione n. 575 del 28/06/2021

Tit. di Class. 1.1.02

A270
GR

OGGETTO: Regolamento Gestione incidenti e violazioni relativi alla sicurezza delle informazioni dell'Azienda Socio Sanitaria Territoriale Nord Milano in ottemperanza al Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27.04.2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati – Applicazione delle misure tecniche previste dall'Art. 32.

IL DIRETTORE GENERALE

PREMESSO che le norme introdotte dal Regolamento (UE) 2016/679 in data 27.04.2019 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, si traducono in obblighi organizzativi, documentali e tecnici che tutti i Titolari del trattamento dei dati personali devono considerare per consentire la piena e consapevole applicazione del nuovo quadro normativo in materia di protezione dei dati personali;

RICHIAMATI i precedenti atti deliberativi in ordine all'applicazione della normativa sul trattamento dei dati personali, ovvero:
- deliberazione n. 753 del 04/11/2020 approvazione del Regolamento informatico;
- deliberazione n. 659 del 24/12/2003 approvazione del Regolamento generale sul trattamento dei dati;

RICHIAMATO l'art. 32 del Regolamento Generale sulla protezione dei Dati (GDPR UE/2016/679) commi 1, 2 ,4, ai sensi del quale: "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio;

DATO ATTO della collaborazione in essere tra l'UOC Servizi Informatici Aziendali e l'UOS Affari Legali, Ufficio Privacy, finalizzata all'adozione delle più adeguate misure di sicurezza in ambito tecnico e organizzativo sul trattamento dei dati;

PRESO ATTO altresì, che in attuazione dell'art. 32 del Regolamento Generale sulla Protezione dei Dati (GDPR – UE/2016/679), e nell'ambito più generale delle azioni congiuntamente attuate dalle due Strutture aziendali citate, è stato predisposto il seguente Regolamento: Gestione incidenti e violazioni relativi alla sicurezza delle informazioni;

VISTO l'allegato testo del Regolamento in oggetto, come predisposto dalla UOC Servizi Informativi Aziendali in collaborazione con l'Ufficio Privacy (UOS Affari Legali) che aggiorna e sostituisce ogni altra disposizione in precedenza emanata con esso confliggente;

RITENUTO di approvare il testo del suddetto "Regolamento gestione incidenti e violazioni relativi alla sicurezza delle informazioni" allegato alla presente deliberazione quale parte integrante, unitamente ai suoi allegati;

ATTESO che dal presente provvedimento non derivano oneri a carico del bilancio aziendale, così come attestato dall'U.O.C. Bilancio e Risorse Finanziarie, nell'ultimo foglio allegato al presente provvedimento;

SU PROPOSTA del Responsabile della UOC Servizi Informativi Aziendali che attesta la legittimità e regolarità tecnico/amministrativa del presente provvedimento, come riportato nell'ultimo foglio;

PRESO ATTO del parere favorevole espresso, per quanto di rispettiva competenza, dal Direttore Amministrativo, dal Direttore Sanitario e dal Direttore Socio-sanitario;

- d e l i b e r a -

per le motivazioni esposte in premessa:

1. di prendere atto delle attività aziendali svolte, in applicazione della normativa nazionale ed europea in tema di "protezione dei dati personali", descritte negli atti deliberativi citati in premessa;

2. di approvare l'allegato "Regolamento gestione incidenti e violazioni relativi alla sicurezza delle informazioni" revocando contestualmente ogni altra disposizione in precedenza emanata confliggente con detto regolamento;

3. di dare atto che il Responsabile del procedimento relativo al presente provvedimento è il Responsabile dell'UOC SIA ing. Pietro Lanzoni;

4. di disporre la pubblicazione del Regolamento che si approva con il presente atto nella sezione amministrazione trasparente del sito web aziendale;

5. di dare atto che il presente provvedimento non comporta oneri di spesa;

6. di dare mandato al Responsabile del procedimento per tutti i necessari, successivi incombenti all'attuazione del presente provvedimento;

7. di dare atto che il presente provvedimento è immediatamente esecutivo ai sensi dell'art. 17, comma 6, della legge regionale 30 dicembre 2009, n. 33, e ss. mm.;

8. di disporre la pubblicazione del provvedimento all'Albo Pretorio on-line aziendale, ai sensi dell'art. 17, comma 6, della legge regionale 30 dicembre 2009, n. 33, e ss. mm.;

9. di trasmettere il presente provvedimento al Collegio Sindacale.

(atti n.2/2021 tit. 01/07/03)

Parere favorevole:

IL DIRETTORE SANITARIO
(d.ssa Anna Lisa Fumagalli)

IL DIRETTORE AMMINISTRATIVO
(dott. Giovanni Palazzo)

IL DIRETTORE SOCIOSANITARIO
(d.ssa Barbara Mangiacavalli)

IL DIRETTORE GENERALE
(d.ssa Elisabetta Fabbrini)

deliberazione del Direttore Generale n. 575 del 28 GIU. 2021, avente all'oggetto: "Regolamento Gestione incidenti e violazioni relativi alla sicurezza delle informazioni dell'Azienda Socio Sanitaria Territoriale Nord Milano in ottemperanza al Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27.04.2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati – Applicazione delle misure tecniche previste dall'Art. 32".

* * * * * * * * * * *

Il sottoscritto Responsabile della U.O.C. Servizi Informativi Aziendali e Responsabile del procedimento:

ATTESTA

la legittimità e regolarità tecnico/amministrativa del presente provvedimento;

DICHIARA

☒ che il presente provvedimento non comporta alcun onere.

Il Responsabile della U.O.C. Servizi Informativi Aziendali
e Responsabile del procedimento
(ing. Pietro Lanzoni)

Il Responsabile della U.O.C. Bilancio e Risorse Finanziarie conferma:

☐ la copertura economica del presente provvedimento e l'annotazione a bilancio sopra riportata

☒ che dal presente provvedimento non derivano oneri a carico del bilancio.

Il Responsabile della U.O.C. Bilancio e Risorse Finanziarie
(d.ssa Domenica Luppino)

Sistema Socio Sanitario

Regione Lombardia

ASST Nord Milano

REGOLAMENTO GESTIONE INCIDENTI E VIOLAZIONI RELATIVI ALLA SICUREZZA DELLE INFORMAZIONI

ai sensi degli art.33-34 e dell'art. 58, paragrafo 2, del Regolamento UE 2016/679

Sommario

SCOPO

Questo Regolamento nasce dalla considerazione che, per quanto efficace sia il Sistema di Gestione della Privacy e Sicurezza Informativa di cui è dotata l'Azienda, ci saranno sempre degli eventi, di origine casuale o deliberata, che potranno minacciare i diritti e libertà degli interessati o comunque la sicurezza delle informazioni.

L'obiettivo di questo documento è quindi di assicurare che tutti gli eventi che possono mettere a repentaglio la privacy e la sicurezza delle informazioni e tutti i punti di debolezza dei sistemi informativi siano segnalati, in modo tale da permettere tempestive azioni correttive per salvaguardare la disponibilità e l'integrità dei dati.

Tutti, dipendenti e non (consulenti, collaboratori temporanei e terze parti) devono essere consapevoli della loro responsabilità nel segnalare ogni evento il più rapidamente possibile e devono essere a conoscenza della procedura di segnalazione dei diversi tipi di eventi e delle debolezze che possono avere un impatto sulla sicurezza dei dati aziendali.

L'Azienda, infatti, in base a quanto stabilito dal Regolamento UE 2016/679 (anche, nel testo, "GDPR") deve **senza indebiti ritardi** e, ove possibile, **entro 48 oppure 72 ore** dalla scoperta (in relazione alla tipologia dell'evento), deve notificare la violazione al Garante per la protezione dei dati personali, a meno che sia **improbabile** che la violazione dei dati personali comporti un **rischio** per i diritti e le libertà delle persone fisiche.

Anche il fornitore, in qualità di Responsabile esterno del trattamento, che viene a conoscenza di una eventuale violazione è tenuto a informare tempestivamente il titolare in modo che questi possa attivarsi, e ciò è previsto dal vigente modello di nomina a Responsabile del trattamento, ai sensi dell'art. 28 del GDPR.

Le notifiche al Garante effettuate oltre il termine delle 48/72 ore devono essere **accompagnate dai motivi del ritardo.**

Inoltre, se la violazione comporta un rischio elevato per i diritti delle persone, il Titolare deve darne comunicazione a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto.

L'Azienda, in qualità di Titolare del trattamento, a prescindere dalla notifica al Garante, è tenuta a **documentare** tutte le violazioni dei dati personali, ad esempio predisponendo un apposito registro. Tale documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa.

DESTINATARI

Sono destinatari del presente Regolamento:

- Responsabili del Trattamento Interni
- Personale interno autorizzato al trattamento
- Amministratori di Sistema.

DEFINIZIONI E TIPOLOGIE

Vengono fornite nel seguito alcune definizioni che sono utilizzate nel testo:

Incidente, Evento, Data Breach

- **Incidente relativo alla sicurezza delle informazioni**: uno o più eventi non voluti o inaspettati cha hanno una probabilità significativa di compromettere l'attività normale e minacciare la sicurezza delle informazioni.
- **Evento relativo alla sicurezza delle informazioni**: occorrenza di uno stato di un sistema, servizio o rete che indica una possibile violazione alla politica per sicurezza delle informazioni o un fallimento dei controlli o da una situazione sconosciuta in precedenza che può essere relativa alla sicurezza.
- **Data breach**, ossia l'effetto di un evento o di un'azione colposa o fraudolenta compiuta da un soggetto, che può compromettere o ha compromesso i diritti e le libertà delle persone fisiche interessate al trattamento.

FIGURE PROFESSIONALI COINVOLTE

Nell'ambito della gestione degli incidenti relativi alla sicurezza delle informazioni operano le seguenti figure professionali:

- **Segnalante.** È la persona che individua per primo l'incidente e provvede a segnalare al proprio Responsabile la dinamica degli eventi di cui è stato testimone.

- **UOS Attuazione normativa sulla riservatezza dei dati personali (c.d. "UOS Privacy").** È la Struttura aziendale che valuta le segnalazioni di incidenti che hanno impatto sulla privacy degli interessati e fornisce supporto ai Responsabili del trattamento per la loro corretta gestione. Sulla base dei rischi rilevati, fornisce indicazioni ai Responsabili per prevenire incidenti e violazioni nell'ambito di aree operative/processi più vulnerabili. Svolge anche funzioni di Gestione reclami privacy, per la prevenzione del contenzioso sulla riservatezza dei dati personali.

- **Responsabile dei Sistemi Informatici.** È la persona incaricata di vigilare sull'efficace gestione degli incidenti informatici; supporta l'UOS Privacy nel fornire indicazioni di natura tecnica per mitigare e prevenire i rischi correlati a incidenti di natura informatica.

- **Amministratore di Sistema.** È la figura che attraverso la propria attività manutentiva ordinaria previene disfunzioni dei sistemi informativi e gestisce operativamente gli incidenti informatici.

- **Nucleo Data Breach.** Composto da:
  - DPO;
  - Responsabile IT;
  - Responsabile UOS Privacy.
  - all'occorrenza, Responsabile del Trattamento del Processo coinvolto, o altre figure aziendali competenti ad esprimere un parere tecnico.

  Valuta le segnalazioni ritenute significative sotto il profilo privacy, proponendo le soluzioni adeguate al caso.

  - **Responsabile della Protezione dei Dati personali (anche "DPO, Data Protection Officer").** Insieme ai componenti del Nucleo Data Breach, affianca la Direzione Generale nella valutazione del data breach e la supporta nelle conseguenti decisioni.

- **Legale rappresentante (Direttore Generale).** In base all'impatto sugli eventuali interessati coinvolti, e con il supporto tecnico delle figure citate, valuta la necessità di procedere alla notifica al Garante e agli interessati stessi della violazione subita.

Tipologia degli incidenti

Gli incidenti che possono costituire una minaccia alla privacy e sicurezza delle informazioni e che pertanto devono essere segnalati, si possono suddividere nelle seguenti tipologie:

Tipologia	*Descrizione*
Intrusione	L'accesso, sia logico che fisico, a archivi cartacei, reti, sistemi, applicazioni, dati o altre risorse tecnologiche da parte di un soggetto non autorizzato.
Denial of Service (DoS)	Attacco informatico in cui si cerca di portare il funzionamento di un sistema al limite delle prestazioni fino a renderlo non più in grado di erogare il servizio.
Codice malevolo (*malware*)	Virus, worm, trojan, backdoor, spyware o qualsiasi altro software creato con il solo scopo di causare danni più o meno gravi ad un sistema informatico. Anche un eccesso di "spam" può essere incluso in questa tipologia.
Malfunzionamento	Il guasto di un componente hardware o software, oppure il degrado

Tipologia	Descrizione
	delle performance. Deve essere considerato come incidente alla sicurezza solo se di media o alta gravità (vedi il paragrafo successivo). Il malfunzionamento software, anche apparente, deve essere preso in considerazione perché può essere l'indizio di una infezione che può minacciare l'integrità dei dati custoditi nei sistemi e potenzialmente diffondersi nella rete aziendale.
Uso improprio	Utilizzo dei dati per scopi e secondo modalità non conformi alle procedure vigenti e normative esterne.
Dato personale errato	Errata compilazione/registrazione del dato personale da parte di uno o più soggetti. È da considerarsi incidente solo se l'evento, determinato per colpa o dolo da parte dell'autore, ha un impatto significativo sui diritti, reputazione, servizi assicurati all'interessato.
Eventi naturali o innescati dall'uomo	Qualsiasi evento distruttivo naturale o provocato direttamente o indirettamente dall' azione dell'uomo come un incendio, un corto circuito, allagamento, degrado dell'ambiente ecc che influenza direttamente l'operatività dei sistemi informativi o compromette l'integrità degli archivi.

Gravità di un incidente

Un incidente deve essere classificato secondo la seguente scala di gravità:

Danno a sistemi				
Significativo (4)	4	8	12	16
Medio (3)	3	6	9	12
Lieve (2)	2	4	6	6
Trascurabile (1)	1	2	3	4
	Trascurabile (1)	Lieve (2)	Medio(3)	Significativo (4)
	Danno alle persone			

Significativo -> Azione urgente
Medio -> Valutare un intervento
Minimo -> Monitor

Danno ai sistemi

Tipologia	Descrizione
Significativo	I servizi o i sistemi sono gravemente compromessi. I beni aziendali hanno subito danni rilevanti. I tempi di ripristino sono elevati con impatti notevoli sulla continuità del servizio.
Medio	I servizi e i beni aziendali hanno subito danni non trascurabili. I tempi di ripristino non compromettono pesantemente la continuità del servizio.
Lieve	I danni sono limitati solo ad una parte ridotta o minima dei sistemi. La continuità del servizio non subisce impatti.
Trascurabile	I sistemi continuano a erogare i servizi.

Danno alle persone

Tipologia	*Descrizione*
Significativo	Perdita permanente delle informazioni, danno oggettivo alla reputazione, danno materiale all'interessato.
Medio	Mancata erogazione del servizio o potenziale alla reputazione, danno materiale (imminente) sull'interessato.
Lieve	Temporanea indisponibilità del servizio nella modalità usuale. L'interessato continua a ricevere il servizio o svolgere il proprio lavoro secondo procedure alternative.
Trascurabile	Non procura nessun effetto sui servizi o accordi di lavoro.

Categorie di eventi

Gli eventi si possono raggruppare in due categorie:

- **Eventi indicativi**: evidenziano che l'incidente alla sicurezza si è già verificato oppure è in corso. Esempi: crash di un server, allarme dell'antivirus, tentativi di accesso non autorizzato registrati dai log, reclami.
- **Eventi preventivi:** indicano che un incidente potrebbe verificarsi in futuro. Esempi: avvisi di vulnerabilità del software, vulnerabilità ricavate dai file di log (I/O error), comportamenti non conformi alle istruzioni riscontrati in fase di controllo.

Origine degli eventi

Gli eventi possono essere segnalati da:

- **Notifiche di allerta dei software di protezione**: Anti-Virus, Anti-Spyware, Anti-Spam, Intrusion Detection System, Backup, attivazione UPS ecc.
- **Sistemi di allarme generici**
- **Log files**: applicazioni, rete, OS, ecc.
- **Informazioni**: notizie di nuove vulnerabilità di sistemi operativi, ecc.
- **Personale**: mail, contatti telefonici, controlli sul campo.

Procedura di gestione di un incidente

La procedura di gestione di un incidente di sicurezza è suddivisa nelle seguenti fasi:

- Rilevazione
- Identificazione e analisi
- Contenimento, raccolta delle evidenze, rimozione e ripristino
- Chiusura incidente

Rilevazione

Quando viene rilevato un incidente o punto di debolezza da cui potrebbe scaturire un potenziale incidente del tipo descritto precedentemente, il dipendente / collaboratore ha due possibilità:

- caso A: contattare l'Help Desk del Sistema informativo per i casi di malfunzionamento o violazione di natura informativa (attacchi virus ecc)
- caso B: contattare l'Ufficio Privacy: ufficio.privacy@asstnordmilano.it per i casi di violazione della riservatezza; perdita di informazioni personali; errori nella registrazione dei dati personali; trattamenti dei dati per scopi non consentiti; utilizzo dei dati senza consenso.

L'ufficio che riceve la segnalazione deve annotare subito tutti i dettagli più importanti nell' Allegato 1_Incident Report – Fase 1.

La fase termina con la presa in carico dell'incidente da parte dei Responsabili dei due punti di contatto citati (Servizi Informatici e Privacy).

Identificazione e analisi

La fase di analisi dell'incidente ha inizio nel momento in cui l'ufficio destinatario della segnalazione la prende in carico e prosegue fino a quando, viene documentata l'analisi dell'incidente rilevato.

L'obiettivo di tale fase del processo è:

- stabilire se l'incidente ha un impatto solo sul funzionamento dei sistemi informativi oppure coinvolge anche i dati personali degli interessati;
- stabilire il danno potenziale connesso all'evento segnalato.

Alla fase di analisi succede il **processo di contenimento,** descritto nel paragrafo successivo.

Se l'analisi dell'incidente consente di stimare un impatto significativo sugli interessati l'ufficio coinvolto è tenuto a convocare tempestivamente il **Nucleo Data Breach** composto:

- DPO
- Responsabile dei Sistemi Informatici
- Responsabile UOS Privacy
- all'occorrenza, Responsabile del Trattamento del Processo coinvolto, o altre figure competenti ad esprimere un parere tecnico.

Alla convocazione del Nucleo deve corrispondere l'intervento immediato delle figure interpellate, che sono tenute a collaborare fornendo con la massima tempestività tutte le informazioni e pareri richiesti.

Valutati gli elementi della segnalazione, il Nucleo, dove fosse rilevata una violazione ad alto rischio per gli interessati, previa approvazione del Legale Rappresentante, provvede a compilare il **Modello di Registrazione delle violazioni e Notifica al Garante** (Allegato 2) e lo invia a:

- Garante per la protezione dei dati personali, all'indirizzo **protocollo@pec.gpdp.it**

e per conoscenza al Responsabile della Protezione dei Dati Personali.

Le informazioni raccolte vengono riportate anche in un apposito **Registro delle Violazioni** (Allegato 3), conservato presso la UOS Privacy, precisando:

- data
- tipo di violazione e le circostanze ad esse relative
- le sue conseguenze
- provvedimenti adottati per porvi rimedio
- eventuali notifiche al Garante
- eventuale comunicazione agli interessati
- firma del Responsabile della Protezione dei Dati Personali.

Ad ogni utilizzo, la sezione del Registro impiegata viene trasmessa in copia al Titolare.

Contenimento

La fase di contenimento ha lo scopo di limitare e ridurre i danni provocati dall'incidente di sicurezza e/o violazione, evitando che questi si propaghino in altri settori dell'azienda o produca degli effetti sugli interessati irrimediabili. Le azioni intraprese in questa fase dipendono molto dalla tipologia e dalla gravità dell'incidente. Esempi: disconnettere i sistemi coinvolti, disabilitare gli account e/o i servizi compromessi o a rischio, disconnettere l'intera rete aziendale. Tutte le azioni intraprese in questa fase devono essere documentate nella Fase 3 dell'Allegato1.

Raccolta delle evidenze e possibili conseguenze

Sin dalla fase di identificazione e analisi può nascere l'esigenza di raccogliere delle evidenze o prove. Questa attività può essere necessaria per accertare le responsabilità, per potere effettuare successivamente delle indagini più approfondite, per una valutazione più completa dei danni o anche per le possibili conseguenze legali.

Bisogna tenere sempre in considerazione che le prove potrebbero essere distrutte, incidentalmente o intenzionalmente, prima di avere compreso la serietà dell'incidente e quindi procedere in tutte le fasi previste dal Regolamento con la massima tempestività.

A seguito dell'incidente, potrebbe essere necessaria un'azione legale civile o penale contro una persona fisica o giuridica, o, viceversa, potrebbero esserci le premesse per essere oggetto di

azione legale: in questi casi, tutta la documentazione sarà trasmessa in copia all'Ufficio Legale per quanto di competenza.

Rimozione e Ripristino

Durante l'attività di rimozione si cerca di eliminare le cause che hanno determinato il verificarsi dell'incidente. Le attività in questo caso sono influenzate dalla tipologia di incidente e dai guasti provocati e possono andare dal semplice utilizzo di strumenti di rimozione del malware fino alla reinstallazione del sistema operativo e/o delle applicazioni da copie di backup, all'accordo con l'interessato stesso, all'identificazione di misure organizzative più restrittive.

Valgono le regole:

- solo il personale autorizzato può avere accesso ai sistemi coinvolti nell'incidente
- tutte le azioni intraprese vanno documentate in dettaglio, inclusi i tempi necessari al ripristino
- l'obiettivo è di ottenere il ripristino della normale attività nel più breve tempo possibile

L'attività di ripristino, infine, ha il compito di riportare i sistemi coinvolti nelle condizioni in cui erano prima del verificarsi dell'incidente.

Chiusura dell'incidente

La chiusura dell'incidente viene formalizzata con la compilazione del Rapporto degli Incidenti da parte di Responsabile dei Sistemi Informatici e della Responsabile Privacy, che permette di attestare l'efficace chiusura dell'incidente. Una volta chiuso l'incidente, il documento dovrà essere riposto e conservato nel Cartella Incidenti nella Intranet Aziendale, visibile solo al Nucleo Data Breach.

In questa fase di valutazione degli incidenti relativi alla sicurezza delle informazioni, può nascere la necessità di migliorare o aggiungere dei controlli per prevenire il ripetersi dell'evento o limitare la frequenza, il danno e i costi di potenziali eventi futuri.

Sempre in sede di chiusura dell'incidente si deve valutare se vi sono dei feed back sulle procedure utilizzate e quindi vi sia la necessità di una loro revisione o, più in generale, di una revisione della politica della sicurezza e privacy aziendale.

Tutte queste osservazioni essere riassunte nel Registro degli incidenti e violazioni (Allegato 3).

Segnalazione delle debolezze e di potenziali falle nel sistema

Nuove minacce alla sicurezza nascono quotidianamente e le vulnerabilità di un sistema possono essere il risultato di debolezze nel disegno del sistema o nella sua gestione o nella formazione del personale addetto; una notevole fonte di informazioni sono sicuramente *focus group community* e le *newsletter* inviate da vari enti, organizzazioni partner e diffuse in Azienda dalla UOS Privacy.

La conoscenza delle debolezze e delle potenziali falle permette di affrontarle subito in modo adeguato e di mantenere quindi il livello di sicurezza del sistema ad un livello accettabile: tutti quindi sono tenuti a segnalare le debolezze e le potenziali vulnerabilità il più velocemente possibile per evitare la possibilità di incidenti alla sicurezza delle informazioni.

Chi scopre una debolezza o una falla deve astenersi dal compiere delle operazioni, che seppur dettate dalla volontà di verificare o contenere la minaccia rilevata, potrebbero aggravare i rischi per l'Azienda.

Il medesimo comportamento deve essere tenuto da/verso i soggetti individuati quali Responsabili esterni.

La segnalazione di una debolezza deve essere fatta descrivendo e documentando le criticità rilevate.

Il modello di Incident Report sarà disponibile sul sito aziendale, nell'Area riservata, unitamente alle Istruzioni per la compilazione.

INCIDENT REPORT

N: .....ANNO/ _____

FASE 1: RILIEVO

Data: _____ **Ora** _____

Segnalatore: _____ **Funzione aziendale** _____

Utenza Coinvolta(Interna/esterna): _____

Apparati informatici i nteressati

☑ **HW (server, rete, VDI, ...)** ☐ SW (applicativo)

Ambiti NON informatici i interessati

_____

Contenuti della Segnalazione: _____

_____

FASE 2: ANALISI DELL'INCIDENTE

Analisi dell'incidente	
Tipologia	Danno stimato al momento della segnalazione
Accesso non autorizzato ☐ **Denial of Service** ☐ **Malware** ☐ **Malfunzionamento** ☐ **Uso improprio** ☐ **Disastro naturale** ☐ **Dato errato** ☐	**Danno stimato alle persone** **Significativo** ☐ **Media** ☐ **Lieve** ☐ **Trascurabile** ☐ **Danno stimato ai sistemi** **Significativo** ☐ **Media** ☐ **Lieve** ☐ **Trascurabile** ☐
Sistemi, utenti e servizi coinvolti	
Descrizione dettagliata	
Dettagli tecnici	

☐ totale ☐ parziale

Entità disservizio

Significativo	
Medio	
Lieve	
Trascurabile	

Descrizione disservizio:

Durata:
Data e ora (presunta) inizio disservizio: _____
Data e ora segnalazione: _____
Data e ora presa in carico: _____

FASE 3: CONTENIMENTO DELL'INCIDENTE

Data e ora risoluzione: _____

Descrizione intervento effettuato:

Chi ha effettuato l'intervento:

Suggerimenti atti a prevenire il ripetersi di eventi analoghi

FASE 4: CHIUSURA DELL'INCIDENTE

Efficacia dell'intervento ☐ totale ☑ parziale

(Se parziale, riportare di seguito le ragioni e le raccomandazioni suggerite)_____

Suggerimenti atti a prevenire il ripetersi di eventi analoghi

Data_____

Firma del Responsabile_____

Modello di Registrazione
delle Violazioni e Notifica al Garante

DATI SOCIETARI

Società titolare del trattamento

.....

Denominazione o ragione sociale

.....

Provincia, Comune, Cap, Indirizzo

.....

Nome e Cognome Titolare del Trattamento

.....

Nome e Cognome persona fisica addetta alla comunicazione .....

Funzione rivestita

.....

Indirizzo PEC e/o EMAIL per eventuali comunicazioni .....

Recapito telefonico per eventuali comunicazioni

.....

Eventuali Contatti (altre informazioni)

.....

DENOMINAZIONE DELLA/E BANCA/BANCHE DATI OGGETTO DI DATA BREACH E BREVE DESCRIZIONE DELLA VIOLAZIONE DEI DATI PERSONALI IVI TRATTATI

.....
.....
.....
.....
.....

QUANDO SI È VERIFICATA LA VIOLAZIONE DEI DATI PERSONALI TRATTATI NELL'AMBITO DELLA BANCA DATI?

- ☐ Il .....
- ☐ Tra il e il .....
- ☐ In un tempo non ancora determinato
- ☐ E' possibile che sia ancora in corso

DOVE È AVVENUTA LA VIOLAZIONE DEI DATI? (SPECIFICARE SE SIA AVVENUTA A SEGUITO DI SMARRIMENTO DI DISPOSITIVI O DI SUPPORTI PORTATILI)

.....
.....
.....
.....
.....

MODALITÀ DI ESPOSIZIONE AL RISCHIO

.....
.....
.....
.....
.....

TIPO DI 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

- ☐ Rete
- ☐ Dispositivo mobile
- ☐ File o parte di un file
- ☐ Strumento di backup
- ☐ Documento cartaceo
- ☐ Altro :.....

SINTETICA DESCRIZIONE DEI SISTEMI DI ELABORAZIONE O DI MEMORIZZAZIONE DEI DATI COINVOLTI, CON INDICAZIONE DELLA LORO UBICAZIONE:

.....

.....

.....

.....

.....

QUANTE PERSONE SONO STATE COLPITE DALLA VIOLAZIONE DEI DATI PERSONALI TRATTATI NELL'AMBITO DELLA BANCA DATI?

- ☐ N. persone .....
- ☐ Circa persone .....
- ☐ Un numero (ancora) sconosciuto di persone

CHE TIPO DI DATI SONO OGGETTO DI VIOLAZIONE?

- ☐ Dati anagrafici/codice fiscale
- ☐ Dati di accesso e di identificazione (user name, password, customer ID, altro)
- ☐ Dati relativi a minori
- ☐ Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
- ☐ Dati personali idonei a rivelare lo stato di salute e la vita sessuale
- ☐ Dati giudiziari
- ☐ Copia per immagine su supporto informatico di documenti analogici
- ☐ Ancora sconosciuto
- ☐ Altro :.....

LIVELLO DI GRAVITÀ DELLA VIOLAZIONE DEI DATI PERSONALI TRATTATI NELL'AMBITO DELLA BANCA DATI (SECONDO LE VALUTAZIONI DEL TITOLARE)?

- ☐ Basso/trascurabile
- ☐ Medio
- ☐ Alto
- ☐ Molto alto

MISURE TECNICHE E ORGANIZZATIVE APPLICATE AI DATI OGGETTO DI VIOLAZIONE

.....

.....

.....

.....

LA VIOLAZIONE È STATA COMUNICATA ANCHE AGLI INTERESSATI?

Sì, è stata comunicata il

No, perché _____

QUAL È IL CONTENUTO DELLA COMUNICAZIONE RESA AGLI INTERESSATI?

.....

.....

.....

.....

QUALI MISURE TECNOLOGICHE E ORGANIZZATIVE SONO STATE ASSUNTE PER CONTENERE LA VIOLAZIONE DEI DATI E PREVENIRE SIMILI VIOLAZIONI FUTURE?

.....

.....

.....

.....

Data

Firma del Legale Rappresentante

Registro Violazioni

SEGNALATORE	TIPO DI INCIDENTE	GRAVITA'	CONSEGUENZE	AZIONE DI MITIGAZIONE INTRAPRESA	NOTIFICA AL GARANTE (SI/NO E DATA)	COMUNICAZIONE ALL'INTERESSATO (SI/NO E DATA)	FIRMA DEL RESPONSABILE PROTEZIONE DATI
	Accesso non autoriz. ☐ Denial of Service ☐ Malware ☐ Malfunzionamento ☐ Uso improprio ☐ Dato Errato ☐ Disastro ☐ Data Breach	☐Significativo -> Azione urgente ☐Medio -> Valutare un intervento ☐Minimo -> Monitorare					