Azienda Ospedaliera Santa Maria – Terni

AZIENDA OSPEDALIERA SANTA MARIA TERNI

DELIBERAZIONE DEL DIRETTORE GENERALE
n. 0000554 del 17/06/2022

OGGETTO:

APPROVAZIONE PROCEDURA PER LA GESTIONE DI VIOLAZIONI DEL TRATTAMENTO DEI DATI PERSONALI O DATA BREACH.

VISTA

Proposta n. 0000598 del 17/06/2022 a cura di S.C. Affari Generali e Legali
Hash.pdf (SHA256):2452c800d43eb3dfe0256eef8a907fcafbcb9495a2d85c2a6471a5993fd6c129

firmata digitalmente da:

Il Responsabile del Procedimento
Responsabile P.O. Giuseppina Ferraro

Il Responsabile S.C. Affari Generali e Legali
f.f. Raffaella Ranchetti

IL DIRETTORE AMMINISTRATIVO
Parere: FAVOREVOLE
Anna Rita Ianni

IL DIRETTORE SANITARIO
Parere: FAVOREVOLE
Alessandra Ascani

DELIBERA

Di fare integralmente propria la menzionata proposta che allegata al presente atto ne costituisce parte integrante e di disporre così come in essa indicato.

IL DIRETTORE GENERALE
Pasquale Chiarelli

Premesso:

Che il regolamento (UE92016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati (in seguito per brevità "GDPR", General Data Protection Regulation), applicabile in tutti gli Stati membri dell'Unione Europea a partire dal 25 maggio 2018, nell'affrontare il tema tutela dei dati personali attraverso un approccio basato principalmente sulla valutazione dei rischi sui diritti e la libertà degli interessati, attribuisce ai Titolari del trattamento il compito di assicurare e di comprovare il rispetto dei principi applicabili al trattamento dei dati personali e di adottare le misure che ritiene a ciò più idonee ed opportune (c.d. principio di responsabilizzazione o accountability);

Che il richiamato GDPR detta una complessa disciplina di carattere generale in materia di protezione dei dati personali, prevedendo molteplici obblighi ed adempimenti a carico dei soggetti che trattano dati personali, ivi comprese le Aziende sanitarie, attribuendo al titolare il compito di decidere autonomamente le mobilità, le garanzie e i limiti del trattamento dei dati;

Che il Decreto Legislativo n. 101 del 10 agosto 2018 recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio Europeo, in attuazione dell'art. 13 della legge di delegazione europea 2016-2017 (legge 25 ottobre 2017, n.163) ha introdotto disposizioni per l'adeguamento della normativa nazionale alle disposizioni del GDPR, novellando il codice della privacy di cui al D.Lgs. n. 196/2003;

Che il nuovo approccio comporta il coinvolgimento di tutti i soggetti chiamati a trattare i dati personali all'interno della organizzazione aziendale, con assunzione delle relative responsabilità;

Atteso che nell'ambito delle attività svolte dal titolare del trattamento, è stata redatta una procedura per la gestione di violazione dei dati personali o Data Breach ex artt. 33 34 del GDPR;

Ritenuto pertanto di approvare la procedura per la gestione di violazione dei dati personali o data Breach ex artt. 33 e 34 del GDPR;

Preso atto che dall'adozione del presente provvedimento non derivano oneri aggiuntivi a carico del bilancio dell'Azienda Ospedaliera di Terni;

Dato Atto che la proposta è coerente con il Piano triennale Aziendale della Prevenzione della Corruzione e del Programma Triennale per la Trasparenza e l'Integrità;

Considerato che il Responsabile di P.O. ed il Dirigente della Struttura proponente attestano di non versare in alcuna situazione di conflitto di interesse, anche potenziale, tale da pregiudicare l'esercizio imparziale delle funzioni e compiti attribuiti, in relazione al procedimento indicato in oggetto ed attestano l'insussistenza di cause di conflitto di interesse, anche potenziale, ex art. 6-bis della legge n. 241/90e ss.mm.ii e art. 1, comma 9, lett. e) della Legge n. 190/2012 e l'inesistenza delle condizioni di incompatibilità di cui l'art. 35-bis del D. Lgs. n. 165/201;

SI PROPONE DI DELIBERARE

- **di approvare**, per le motivazioni esposte in premessa che si intendono tutte integralmente riportate, la procedura per la gestione di violazione dei dati personali o Data Breach ex artt.33 e 34 del GDPR;

- **di prendere atto** che dall'adozione del presente provvedimento non derivano oneri aggiuntivi a carico del bilancio dell'azienda Ospedaliera di Terni;

- **di trasmettere** copia del presente atto a tutti i designati del trattamento e a tutti i componenti del Gruppo Aziendale Privacy;

-**di stabilire** che il presente atto sarà pubblicato nel sito web aziendale in adempimento degli obblighi di pubblicazione ;

-**di individuare** quale responsabile del procedimento amministrativo, ai sensi della Legge 241/'90 la dott.ssa Giuseppina Ferraro, collaboratore amministrativo professionale senior ;

Il Responsabile P.O. Affari legali
Dott.ssa Giuseppina Ferraro

Il Dirigente Amministrativo
Dott.ssa Maria Rita Bruscolotti

Servizio Sanitario Nazionale
Regione Umbria

AZIENDA
OSPEDALIERA
SANTA MARIA
TERNI

PROCEDURA DA SEGUIRE IN CASO DI DATA BREACH

Via Tristano di Joannuccio, 1 - 05100 Terni (TR)
C.F.- P.I.: 00679270553 - Centralino: 0744/2051
P.E.C.: aospterni@postacert.umbria.it
www.aospterni.it

RIFERIMENTI NORMATIVI

- 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)"

- 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

- 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.

- Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015

- 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

- Decreto del Presidente del Consiglio dei Ministri 1 aprile 2008 "Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività" previste dall'articolo 71, comma 1-bis del decreto legislativo 7 marzo 2005, n. 82, recante il «Codice dell'amministrazione digitale» G.U. 21 giugno 2008, n. 144.

- Art. 13 del DPCM DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 24 ottobre 2014 Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese. (1409376) (GU Serie Generale n.285 del 09-122014)

DEFINIZIONE DATA BREACH

L'art. 33 del GDPR recita che: "In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di controllo competente a norma dell'art.55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, corredata dei motivi del ritardo".

Per "Data Breach" si intende un evento in conseguenza del quale si verifica una "violazione dei dati personali"., Nello specifico, l'articolo 4 p. 12 del GPDR definisce la violazione dei dati personali come 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 e conservati o comunque trattati.

Le 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 precisano la nozione di violazione come di seguito riportata: le violazioni possono essere classificate in base ai seguenti tre principi ben noti della sicurezza delle informazioni:

- "violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
- "violazione dell'integrità", in caso di modifica non autorizzata o accidentale dei dati personali; • "violazione della disponibilità", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

Va altresì osservato che, a seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

Ci si potrebbe chiedere se una perdita temporanea della disponibilità dei dati personali costituisca una violazione e, in tal caso, se si tratti di una violazione che richiede la notifica. L'articolo 32 del regolamento ("Sicurezza del trattamento") spiega che nell'attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, si dovrebbe prendere in considerazione, tra le altre cose, "la 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".

Di conseguenza, un incidente di sicurezza che determina l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche. Va precisato che l'indisponibilità dei dati personali dovuta allo svolgimento di un intervento di manutenzione programmata del sistema non costituisce una "violazione della sicurezza".

Come nel caso della perdita o distruzione permanente dei dati personali (o comunque di qualsiasi altro tipo di violazione), una violazione che implichi la perdita temporanea di disponibilità dovrebbe essere documentata in conformità all'articolo 33, paragrafo 5. Ciò aiuta il titolare del trattamento a dimostrare l'assunzione di responsabilità all'Autorità di Controllo, che potrebbe chiedere di consultare tali registrazioni. Tuttavia, a seconda delle circostanze in cui si verifica, la violazione può

richiedere o meno la notifica all'autorità di controllo e la comunicazione alle persone fisiche coinvolte.

Il titolare del trattamento dovrà valutare la probabilità e la gravità dell'impatto dell'indisponibilità dei dati personali sui diritti e sulle libertà delle persone fisiche. Conformemente all'articolo 33, il titolare del trattamento dovrà effettuare la notifica a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Questo punto dovrà chiaramente essere valutato caso per caso.

Va notato che, sebbene una perdita di disponibilità dei sistemi del titolare del trattamento possa essere solo temporanea e non avere un impatto sulle persone fisiche, è importante che il titolare del trattamento consideri tutte le possibili conseguenze della violazione, poiché quest'ultima potrebbe comunque dover essere segnalata per altri motivi.

La mancata notifica può comportare ulteriori accertamenti da parte del Garante poiché può rappresentare un indizio di carenze che, se accertate, possono dar luogo a sanzioni.

Tutti gli eventi di Data Breach, compresi quelli per cui non sono necessarie le notifiche, devono essere documentati (art. 33 par. 5 del GDPR) su un Registro delle Violazioni.

ACQUISIZIONE DELLA NOTIZIA

La segnalazione di un Data Breach può essere interna o esterna all'Azienda.

INTERNAMENTE:

- Da personale dipendente
- Da personale convenzionato/stagisti/tirocinanti, ecc.

ESTERNAMENTE

- Da parte degli organi Pubblici (Agid, Polizia, altre Forze dell'Ordine, giornalisti, ecc.)
- Da parte del DPO
- Da parte dei Responsabili esterni del trattamento
- Da parte degli interessati
- Da parte di ulteriori soggetti.

La segnalazione deve essere inoltrata ai soggetti preposti individuati quali Riceventi mediante:

- Posta elettronica;
- Avvertimento verbale/telefonico in ogni caso.

Dal momento in cui i soggetti preposti predetti, vengono a conoscenza dell 'evento, decorre il termine delle 72 ore previsto dalla normativa per l'invio della notifica all'Autorità di Controllo.
Tale termine è ridotto a 48 ore nel caso in cui i trattamenti oggetto dell'evento rientrino in quelli previsti dalle misure di sicurezza e modalità di scambio dei dati personali tra Amministrazioni Pubbliche - 2 luglio 2015 (Pubblicato sulla Gazzetta Ufficiale n. 179 del 4 agosto 2015).

SCOPO DEL DOCUMENTO

L'Azienda Ospedaliera protegge la sicurezza e la riservatezza delle Informazioni Personali di qualsiasi Interessato (dipendenti, pazienti, fornitori, docenti in visita, partecipanti a corsi di formazione, etc.) e fornisce immediata risposta agli Incidenti di Sicurezza (da intendersi come qualsiasi incidente, a prescindere dall'eventuale interessamento di Dati Personali) nonché alle Violazioni dei Dati personali (da intendersi come ogni Incidente sulla sicurezza che coinvolge Dati Personali), come di seguito meglio definiti.
Qualsiasi Incidente sulla Sicurezza e qualsiasi Violazione dei Dati Personali, rilevato dai collaboratori o portato all'attenzione di tutti i collaboratori che operano, a vario titolo, presso l'Azienda, deve essere gestito secondo le modalità definite nelle pagine seguenti.

L'obiettivo del presente documento è:

-sensibilizzare i dipendenti sulle responsabilità in materia di protezione dei dati personali e sull'importanza della collaborazione nella tempestiva segnalazione e risoluzione degli Incidenti sulla Sicurezza (inclusi le Violazioni dei Dati Personali);

-definire processi per identificare, tracciare e reagire ad un Incidente sulla Sicurezza e a una Violazione dei Dati Personali, per valutarne il rischio, contenere gli effetti negativi e porvi rimedio nonché stabilire se, in caso di Violazione dei Dati Personali, si renda necessario procedere alla notifica al Garante e alla comunicazione agli Interessati;

-definire ruoli e responsabilità per la risposta agli Incidenti sulla Sicurezza e alle Violazioni dei Dati Personali;

-assicurare un adeguato flusso comunicativo all'interno dell'Azienda Ospedaliera tra le parti interessate.

Definizioni:

Altre informazioni	Informazioni diverse dalle Informazioni personali.
Comunicazione	Rivelazione di dati personali a uno o più enti identificati e diversi dal Soggetto Interessato, rappresentante del titolare del trattamento nel territorio statale, responsabile del trattamento e soggetti responsabili dell'elaborazione sotto qualsiasi forma, incluso il rendere disponibili o accessibili tali dati.
Dati biometrici	Dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
Dati comuni	Categoria non definita nella normativa. Fanno parte dei dati comuni il codice fiscale, il numero di partita IVA, la residenza, il numero di telefono, l'indirizzo e-mail.
Dati giudiziari	Dati personali idonei a rivelare provvedimenti di cui all'art. 3, comma 1, lettere da a) a o) e da r) a u) del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, ana afe delle sanzioni amministrative

	dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi de li art. 60 e 61 del codice di procedura penale.
Dati particolari	Dati personali idonei a rivelare origine razziale ed etnica, convinzioni religiose, filosofiche o di altro genere, opinioni politiche, adesione a partiti politici, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati genetici, biometrici e i dati idonei a rivelare lo stato di salute e la vita sessuale.
Dati personali	Qualunque informazione relativa ad una persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale (per es. n. di matricola), i dati relativi all'ubicazione, un identificativo on line. Si considera identificabile la persona fisica che può essere identificata anche tramite uno o più elementi della sua identità fisica, psichica, economica, culturale, sociale.
Dati relativi alla salute	Dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.
Diffusione	Rivelazione dei dati personali a enti non identificati, sotto qualsiasi forma, incluso il rendere disponibili o accessibili tali dati.
Garante	L'Autorità Garante per la protezione dei dati personali.
Incidente sulla sicurezza	Violazione della sicurezza che può anche non riguardare le Informazioni Personali.
Informazioni Personali	I Dati personali, i Dati comuni, i Dati particolari ivi inclusi i dati biometrici, i Dati relativi alla salute e i Dati giudiziari.
Interessato	Qualsiasi persona fisica a cui si riferiscono i dati personali.
Responsabile ICT	E il soggetto incaricato di gestire le violazioni dei dati personali e gli Incidenti di sicurezza.
Responsabile del trattamento	Persona fisica, persona giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal Titolare al trattamento dei dati personali.
Responsabile della protezione dei Dati o DPO	Soggetto individuato dal Titolare in funzione delle qualità professionali e della conoscenza specialistica della normativa e della prassi in materia di protezione dati che deve essere necessariamente coinvolta in tutte le questioni che riguardano la protezione dei dati personali.
Titolare del trattamento	Persona fisica, persona giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro Titolare, le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo di sicurezza.
Trattamento	Qualsiasi operazione o serie di operazioni eseguite con o senza l'ausilio di mezzi elettronici o automatici che riguarda la raccolta, registrazione, organizzazione, mantenimento, interrogazione, elaborazione, modifica, selezione, recupero, confronto, utilizzo, interconnessione, blocco, comunicazione, divulgazione, cancellazione e distruzione di dati, che questi siano o meno contenuti in una banca dati.
Violazione di dati o di dati personali	Violazione della sicurezza che comporta, in modo accidentale o illecito, la distruzione, perdita, alterazione, comunicazione non autorizzata di, o accesso a, dati personali trasmessi, conservati o altrimenti trattati. La violazione dei dati è quindi un incidente di sicurezza che riguarda le Informazioni Personali.

AMBITO DI APPLICAZIONE

La presente procedura si applica a tutte le Informazioni Personali e alle altre informazioni che, pur non costituendo Informazioni Personali, sono raccolte o gestite o comunque trattate dall'Azienda Ospedaliera siano esse dati contenuti su dispositivi elettronici, accessibili via rete o web, contenuti su dispositivi mobili o portatili ovvero su supporti cartacei.

RUOLI E TIPOLOGIE DI VIOLAZIONI DEI DATI PERSONALI

La tempestività è un fattore determinante nella risposta agli Incidenti sulla sicurezza e alle violazioni dei dati personali ed è dovere di ciascun soggetto, nell'ambito del proprio ruolo nella struttura e nella catena di comunicazione, non ritardare iniziative di reazione all'incidente e rispettare le procedure e le tempistiche di comunicazione individuate dal presente documento.

Coerentemente con il concetto di sicurezza (Riservatezza, Disponibilità e Integrità), gli incidenti possono avere per oggetto uno o più di questi attributi. Laddove interessino uno solo dei sotto indicati attributi, questi vengono classificati in:

1. Violazione dei Dati Personali sulla Riservatezza: violazione della riservatezza delle Informazioni Personali (a titolo esemplificativo: quando si verifica una comunicazione non dovuta o un accesso non autorizzato o accidentale ai dati personali);
2. Violazione dei Dati Personali sulla Disponibilità: quando i dati personali non sono disponibili perché si verifica una loro perdita accidentale o una distruzione (a titolo esemplificativo viene smarrita la chiave di decriptazione dell'unica copia di dati criptati e non è disponibile una copia di backup). La perdita di disponibilità può anche essere temporanea (e configurare, comunque, una Violazione dei Dati Personali), vista l'importanza di avere informazioni disponibili in un dato momento;
3. Violazione dei Dati Personali sull'Integrità: quando si verifica un'alterazione non autorizzata o accidentale dei dati personali.

PROCEDURE A TUTELA DELLA SICUREZZA DEI DATI

Presso L'Azienda Ospedaliera "S. Maria" di Terni sono state attivate procedure a tutela della sicurezza dei dati, tra cui:

— **l'adozione di misure organizzative e tecniche** per garantire un livello di sicurezza adeguato al rischio connesso al trattamento dei dati personali e alle altre informazioni trattate, comprese misure volte al tempestivo ripristino della disponibilità in caso di Incidente sulla sicurezza;

— **l'organizzazione, a cadenza periodica, di corsi di formazione** per i dipendenti/collaboratori sui principi cardine della normativa sul trattamento dati, sulla sicurezza dei Dati Personali e dei Sistemi;

— **la predisposizione di un sistema di protezione**, mediante apposite misure tecniche (firewall, antivirus,) dell'accesso a Internet ai dispositivi elettronici.

Il personale e i collaboratori che prestano attività in Azienda, ove dovessero venire a conoscenza di un Incidente sulla sicurezza o di elementi che fanno sospettare (anche a seguito di segnalazione di terzi) che si sia verificato o possa verificarsi un tale incidente, sono tenuti a seguire la procedura di seguito descritta:

Titolare del trattamento dati: Azienda Ospedaliera "S. Maria" di Terni
Responsabile della Protezione dei dati (RPD): Dott.ssa Giuseppina Ferraro

Attività di segnalazione, raccolta informazioni, valutazione notifica della violazione

Step	Attività	Chi	A Chi	Quando	Come
1	**Rilevazione segnalazione data breach**	Tutto il personale, collaboratori, fornitori, responsabili esterni	Responsabile della struttura di riferimento (Dirigente amministrativo, Dirigente S.C. Tecnico patrimoniale, Dirigente S.C. Economato e Provveditorato, Responsabile ufficio informatico, Dirigente S.C. Economico Finanziaria, Direttori e responsabili strutture e servizi sanitari, Direttore S.C. di riferimento...) o al suo sostituto o al Manager Privacy	Appena se ne viene a conoscenza	Utilizzando le vie più brevi (telefono, di persona, e-mail)
2	Raccolta informazioni sulla violazione	Il Responsabile della Struttura o il sostituto o il Manager Privacy insieme ai soggetti coinvolti nella violazione Responsabile nel caso non		Appena ricevuta la comunicazione	Utilizzando il modello fornito e raccogliendo informazioni dai soggetti coinvolti nella segnalazione e nel trattamento dei dati violati

		Possa essere immediatamente disponibile, deve dare istruzioni precise alla persona che l'ha contattato per iniziare subito la raccolta delle informazioni, indicando dove reperire il modello predisposto a tale scopo			
3	**Comunicazione del Data Breach**	Il Responsabile della struttura di riferimento (Dirigente amministrativo, Dirigente S.C. Tecnico patrimoniale, Dirigente S.C. Provveditorato e Servizi alberghieri, Responsabile ufficio informatico, Dirigente S.C. Economico Finanziaria, Dirigente Servizi sanitari, Direttore S.C. di riferimento.. o al suo sostituto o il Manager Privacy (in mancanza di tali figure la stessa persona che ha rilevato la violazione.	Al Titolare (da specificare quale organo è incaricato della notifica della violazione al Garante), RPD, esperti ICT	Appena ottenute informazioni di base sulla violazione	Utilizzando le vie più brevi
4	**Valutazione d'impatto**	Titolare, RPD, esperti ICT, soggetti coinvolti		Appena ricevuta la comunicazione	Utilizzando la metodologia indicata

5	**Individuazione delle azioni correttive**	RPD, esperti ICT, soggetti coinvolti		Appena terminata la valutazione d'impatto	Analizzando i risultati della valutazione d'impatto
6	**Comunicazioni delle valutazioni effettuate e delle azioni da intraprendere**	RPD, Responsabile della Struttura o sostituto o Manager Privacy	Al Titolare		Tramite una breve relazione anche orale
7	**Notifica della violazione (se è necessaria)**	Titolare	Al Garante	Entro 72 ore dalla rilevazione	Mediante la modulistica predisposta dal Garante
8	**Comunicazione agli interessati coinvolti (se è necessaria)**	Titolare	Alle persone fisiche i cui dati sono stati violati	Nei termini indicati nella valutazione d ' impatto	Comunicazione diretta alle singole persone o mediante pubblicazione in sito a loro accessibile delle eventuali conseguenze della violazione sulle categorie di persone fisiche interessate
9	**Disposizioni per l'attuazione delle misure correttive (se individuate)**	Responsabile delle strutture coinvolte	Ai soggetti incaricati di svolgere le attività	Nei termini indicati nella valutazione d'impatto	Devono essere indicate in dettaglio le operazioni da svolgere, chi è l'incaricato, i tempi di attuazione; prevedere eventuali operazioni di verifica dell'efficacia delle misure correttive
10	Recepimento della risposta del Garante alla notifica (se effettuata)	Titolare, RPD, responsabili delle strutture coinvolte, esperti ICT			Disposizioni per l'attuazione delle eventuali misure correttive indicate dal Garante; effettuazione di ulteriori indagini per approfondire le informazioni raccolte

Attività relative alla registrazione dell'incidente

Step	Attività	Chi	Quando	Come
1	**Registrazione della violazione/aggiornamenti**	Ufficio RPD	Appena ricevuta la comunicazione	Compilando l'apposito registro con la descrizione della violazione, delle azioni intraprese e annotando i successivi aggiornamenti
2	**Registrazione della risposta del Garante**	Ufficio RPD	Al momento della ricezione	Annotando sul registro gli estremi della risposta del Garante e le eventuali prescrizioni in essa contenute
3	**Registrazione della prosecuzione/chiusura dell'incidente**	Ufficio RPD	In seguito alle indicazioni del RPD	Registra la chiusura dell'incidente se non necessita di ulteriori indagini o riporta le istruzioni per le ulteriori inda ini

Attività inerenti la prosecuzione delle indagini

Da eseguire nel caso sia necessario acquisire ulteriori informazioni

Step	Attività	Chi	A Chi	Quando	Come
1	**Prosecuzione delle indagini**	RPD, Responsabile della Struttura o sostituto o Manager Privacy, soggetti coinvolti nella violazione e nei trattamenti di dati violati, esperti ICT		A seguito di indicazione da parte del Garante o del Titolare; se previsto nella prima valutazione d'impatto; nel caso che le informazioni raccolte risultino incomplete o mancanti	Raccogliendo le informazioni mancanti, o approfondendo quelle note per rilevare eventuali impatti non riscontrati nella prima indagine
2	**Esecuzione di una nuova valutazione d 'impatto**	Titolare, RPD, ICT, soggetti coinvolti		Al momento che si ritiene di aver raccolto tutte le informazioni possibili sulla violazione	

Comunicazione dei risultati del proseguimento delle indagini	RPD, responsabile della struttura o sostituto o Manager Privacy	Al Titolare	Appena terminato il lavoro	Tramite relazione sintetica sui risultati della valutazione d'impatto e sulle azioni necessarie, allegando il materiale informativo raccolto
Aggiornamento della notifica al Garante (se necessario)	Titolare	Al Garante	Appena sono disponibili i nuovi dati o secondo i termini stabiliti dal Garante	Mediante la modulistica predisposta o come indicato dal Garante
Comunicazioni agli interessati (se necessario)	Titolare		Nei tempi stabiliti nella valutazione d' impatto	Contattando direttamente gli interessati oppure rendendo nota la violazione e le possibili conseguenze mediante pubblicazione accessibile alle categorie di interessati

Tutti gli Incidenti di sicurezza e le violazioni dei dati personali devono essere trattati con il massimo livello di riservatezza: le informazioni devono essere condivise esclusivamente con il personale identificato nella

presente procedura e solo quando strettamente necessario. Eventuali comunicazioni a soggetti non coinvolti nella gestione dell'Incidente dovranno limitarsi all'indicazione che si è verificato un problema e che lo stesso è in fase di gestione.

Calcolo del livello di rischio

Per effettuare la predetta valutazione, vengono utilizzati i criteri di seguito elencati, tenendo conto della probabilità di accadimento del danno e della gravità delle conseguenze. Tali criteri rappresentano una mera esemplificazione, fermo restando che la valutazione andrà condotta sul caso specifico e con riguardo al contesto di riferimento.

Tipologia di Data Breach	Viene valutato se il dato si dovrà valutare se è relativo alla confidenzialità, disponibilità e/o integrità dei dati. Si consideri che una violazione concernente la confidenzialità dei dati riguardanti la carriera di uno studente può avere un livello di rischio e un impatto diverso (e minore) rispetto alla perdita o distruzione definitiva dei predetti dati.
Natura, tipologia e sensibilità dei dati violati	Generalmente, maggiore è la sensibilità dei dati violati maggiore è il rischio di lesione dei diritti e delle libertà degli individui (per esempio, la violazione della confidenzialità dei dati sulla salute ha delle conseguenze più gravi della violazione della confidenzialità dei dati anagrafici di un soggetto).
Facilità d'identificazione diretta o indiretta dei soggetti interessati	Ove l'incidente riguardi dati che non permettono la diretta identificazione degli Interessati, il livello di rischio è minore (per es. la violazione di dati criptati o de identificati è sicuramente meno grave della violazione di dati in chiaro o accompagnati dagli identificativi diretti de li Interessati .
Gravità delle conseguenze per i soggetti interessati	Ad esempio, il rischio dovrà essere valutato elevato ove dalla violazione possa derivare un furto di identità, un danno materiale, un danno di immagine. Analogamente, deve considerarsi elevato il rischio qualora siano stati violati i diritti e le libertà fondamentali dei soggetti interessati quando il Titolare è consapevole che i dati personali sono stati violati e si ritiene che il soggetto che li detiene abbia intenzioni sospette o malevoli.
Categorie dei soggetti interessati	In caso di violazione di Informazioni Personali concernenti minori o soggetti vulnerabili (ad esempio soggetti con disabilità etc...) il rischio si considera più elevato.
Numero di soggetti coinvolti	Generalmente, maggiore è il numero di soggetti interessati, più elevato è il rischio.

Il rischio (R) è calcolato mediante la seguente formula:

R = Probabilità della minaccia X Impatto

Il rischio è tanto maggiore quanto più è probabile che accada l'incidente e tanto maggiore è la gravità del danno arrecato (impatto). Una volta determinati gli indici di rischio sarà possibile individuarne la significatività e definire quindi le priorità d'intervento. In base ai valori attribuibili alle due variabili "Probabilità della Minaccia" e "Impatto", il rischio è numericamente definito con una scala crescente dal valore 1 al valore 12 secondo la matrice riportata nella seguente tabella

TAB. "A"

	IMPATTO			
PROBABILITA' DELLA MINACCIA	BASSO (1)	MEDIO (2)	ELEVATO (3)	MOLTO Elevato (4)
BASSO 1	1	2	3	4
MEDIO (2)	2	4	6	8
ALTO 3	3	6	9	10

La probabilità è misurata mediante la ponderazione delle variabili che influenzano il trattamento del dato come: le risorse tecniche utilizzate, i processi e le procedure e la tipologia di trattamento svolto. Per maggiori dettagli si rinvia al documento dell'ENISA denominato "Guidelines for SMEs on the security of personal data processing" del dicembre 2016, pagg. da 24 a 30.

L'impatto della violazione viene misurato in base ai soggetti coinvolti nel trattamento.

TAB. "B"

LIVELLI DI IMPATTO	
Nullo/Basso	I soggetti interessati non vengono colpiti o subirebbero disagi minimi, superabili senza alcun problema (tempo necessario per reinserire le informazioni, fastidio, irritazione etc...
Medio	I soggetti interessati subiscono notevoli disagi risolvibili con qualche difficoltà (costi extra, negazione accesso a servizi aziendali, timori, difficoltà di comprensione, stress, indisposizione fisica, etc...
Elevato	I soggetti interessati subiscono notevoli disagi risolvibili con serie difficoltà (appropriazione indebita di fondi, inserimento nella black list dei cattivi pagatori da parte delle banche, danni a proprietà, perdita dell'impiego, citazione a comparire, peggioramento dello stato di salute, etc...
Molto Elevato	I soggetti interessati subiscono notevoli conseguenze, perfino irreversibili, e impossibili da risolvere (difficoltà finanziarie quali ingenti debiti, impossibilità a lavorare, problemi fisici o psicologici a lungo termine, morte, etc...

Violazioni della presente procedura

La violazione di quanto previsto nella presente Policy espone il Titolare del trattamento al rischio di responsabilità civile, penale e a sanzioni amministrative. Il soggetto autore delle violazioni potrà incorrere in responsabilità disciplinare e conseguentemente nei provvedimenti sanzionatori, secondo quanto previsto dalla normativa vigente e dal CCNL di riferimento applicabile.

Allegato A: ESEMPI DI DATA BREACH E COMUNICAZIONI

Caso	Notificare l'autorità di controllo?	Notificare la persona interessata?	Note/raccomandazioni
Un titolare del trattamento ha memorizzato un backup di archivio dati personali cri tati su una chiavetta	No	No	Fintanto che i dati sono criptati con un algoritmo di ultima generazione, che esistono dei backup dei dati che possono
SB. La chiavetta UBS viene rubata durante un furto con scasso.			essere recuperati in tempi rapidi, e che la chiave univoca non sia stata compromessa, non si tratta di una violazione da notificare. Tuttavia, se successivamente compromessa, la violazione va notificata.
Un titolare del trattamento offre un servizio online. Durante un attacco informatico a tale servizio vengono prelevati dei dati personali di individui. Il titolare del trattamento ha clienti in un singolo Stato membro.	Sì. Notificare l'autorità di controllo competente in presenza di potenziali conseguenze per singoli individui.	Sì. Notificare gli individui a seconda della natura dei dati personali interessati, e nel caso in cui vi siano alte potenziali conseguenze per gli individui.	Se il rischio non è elevato, è consigliabile che il titolare del trattamento informi la persona interessata, a seconda delle circostanze del caso. Potrebbe ad esempio non essere necessario informare nel caso di violazione di una newsletter relativa a un programma televisivo, tuttavia la notifica potrebbe essere necessaria se la newsletter può influenzare il punto di vista politico sull'argomento trattato.
Una breve interruzione di corrente elettrica della durata di qualche minuto presso il call center del titolare del trattamento non ha consentito ai clienti né di chiamare il titolare del trattamento né di accedere ai propri archivi.	No.	No.	Non si tratta di una violazione di dati personali notificabile, sebbene si tratti comunque di un incidente registrabile ai sensi dell'articolo 33. Il titolare del trattamento deve assicurare la registrazione del caso.

Caso	Notificare l'autorità di controllo?	Notificare la persona interessata?	Note/raccomandazioni
Un titolare del trattamento viene fatto oggetto di un attacco con richiesta di riscatto in seguito al quale tutti i dati vengono criptati. Non sono disponibili backup e non è possibile ripristinare i dati. In seguito ad accertamenti emerge con certezza che l'unico scopo dell'attacco era quello di criptare i dati, e che non vi è alcun altro malware presente nel sistema.	Sì. Notificare l'autorità di controllo competente se vi sono potenziali conseguenze per le persone poiché ciò rappresenta una mancanza di disponibilità.	Sì. Notificare i soggetti a seconda della natura dei dati personali interessati, del possibile effetto della mancanza di disponibilità dei dati, nonché di altre possibili conseguenze.	Nel caso vi sia un backup disponibile e i dati possano essere ripristinati in breve tempo, non necessario segnalare l'evento all'autorità di controllo o alle persone, in quanto non vi si configura una mancanza permanente di disponibilità né di riservatezza. Tuttavia, le autorità di controllo potrebbe ritenere necessaria un'indagine per valutare la conformità con i requisiti di sicurezza generali di cui all'art. 32.
Un dipendente smarrisce una cartella clinica/referto con relativi dati personali del paziente. Il titolare del trattamento svolge una breve indagine (entro le 24 ore) e stabilisce con ragionevole certezza che vi è stata una violazione di dati personali.	Si.	Si Vanno notificate soltanto le persone interessate, se vi è un alto rischio e se risulta evidente che non siano stati coinvolti altri.	

Caso	Notificare l'autorità di controllo?	Notificare la persona interessata?	Note/raccomandazioni
Un dipendente smarrisce lo smartphone aziendale su cui sono memorizzati messaggi di posta elettronica della casella aziendale	Si.		Non è necessaria se esiste copia dei dati e se siamo certi che lo smartphone
Un' azienda di web hosting (un responsabile del trattamento) identifica un errore nel codice che controlla l'autorizzazione utenti. Il risultato è che ogni utente può accedere ai dettagli dell'account di qualsiasi altro utente.	Come responsabile del trattamento l' azienda di web hosting deve immediatamente notificare i propri clienti (i titolari del trattamento) interessati. Dato per scontato che l'azienda di web hosting abbia condotto una propria indagine, i titolari del trattamento interessati devono essere ragionevolmente sicuri se abbiano o meno subito una violazione e, pertanto, se possano ritenersi "a conoscenza" una volta informati dall'azienda di web hosting (responsabile del trattamento). A questo punto il titolare del trattamento deve informare l'autorità di controllo.	Se è probabile che non vi sia un elevato rischio per le persone, queste non devono essere notificate.	L' azienda di web hosting (responsabile del trattamento) deve tenere in considerazione eventuali altri obblighi di notifica, ad es. in base alla Direttiva sulla sicurezza delle reti e dei sistemi informativi (MS). Se non vi è alcuna evidenza che questa vulnerabilità venga sfruttata dal titolare del trattamento, una violazione notificabile potrebbe non essersi verificata. Tuttavia è probabile che sia registrabile ovvero che configuri una non conformità ai sensi dell'art. 32.
A causa di un attacco informatico in un ospedale le cartelle cliniche non sono disponibili per un arco di 30 ore	Si. L'ospedale è tenuto a segnale un potenziale elevato rischio per il benessere la privacy dei pazienti	Si. Notificare i soggetti colpiti	

Caso	Notificare l'autorità di controllo?	Notificare la persona interessata?	Note/raccomandazioni
Ho trovato che è stata forzata la serratura di un armadio contenente archivi cartacei relativi alle carriere del personale, dati dei pazienti, studenti, ma sembra non manchi nulla.	Sì, notificare l'autorità di controllo.	Sì, notificare gli individui a seconda della portata e della tipologia di dati personali coinvolti e della gravità delle possibili conseguenze.	
E' stato rubato un portatile da un ufficio, reparto, aula didattica, nel quale erano contenuti dati personali di pazienti dipendenti, studenti	Si	Sì, notificare gli individui a seconda della portata e della tipologia di dati personali coinvolti e della gravità delle possibili conseguenze	
Non so chi devo informare di una violazione di dati personali che ho trovato su una pagina del sito web dell'Azienda	Si .La segnalazione deve essere effettuata al responsabile della propria struttura di afferenza, il quale avvierà la procedura per la comunicazione al Titolare		
Il computer è stato formattato in seguito ad un guasto. Devo fare la segnalazione?	No se esiste un backup dei dati personali contenuti nel computer.		
Per errore ho inviato un messaggio di posta elettronica contenente una lista di studenti iscritti ad un corso con indicazione di matricola ed indirizzo e-mail a più destinatari	Si è necessaria la segnalazione		

Allegato B: MODELLO DI NOTIFICA DATA BREACH AL GARANTE PRIVACY

1. Titolare che effettua la comunicazione:
   a. Denominazione o ragione sociale
   b. Sede del Titolare
   c. Persona fisica addetta alla comunicazione
   d. Funzione rivestita e. Indirizzo e-mail per eventuali comunicazioni
   f. Recapito telefonico pe eventuali comunicazioni

2. Natura della comunicazione:
   a. Nuova comunicazione (inserire contatti per eventuali chiarimenti, se diversi da quelli sub 1.)
   b. Seguito di precedente comunicazione (inserire numero di riferimento) bl. Inserimento ulteriori informazioni sulla precedente comunicazione b2. Ritiro precedente comunicazione (inserire le ragioni del ritiro)

3. Denominazione della/e banca/banche dati oggetto di Data Breach e breve descrizione della violazione dei dati personali ivi trattati

4. Quando si è verificata la violazione di dati personali?
   a. il (data)
   b. tra il (data) e il (data)
   c. in un tempo non ancora determinato
   d. È possibile che sia ancora in corso

5. Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smaltimento di dispositivi o di supporti portatili).

6. Modalità di esposizione al rischio: a. tipo di violazione:
   a. 1. lettura (presumibilmente i dati non sono stati copiati)
   a.2. copia (i dati sono ancora presenti sui sistemi del Titolare)
   a.3. alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
   a.4. cancellazione (i dati non sono più sui sistemi del Titolare e non li ha neppure l'autore della violazione)
   a.5. furto (i dati non sono più sul sistema del Titolare e li ha l'autore della violazione)
   a.6. altro (specificare)

   b. dispositivo oggetto della violazione:
   b. l. computer
   b.2. dispositivo mobile
   b.3. documento cartaceo
   b.4. file o parte di un file
   b.5. strumento di backup
   b.6. rete
   b. 7. altro (specificare)

7. Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione.

8. Quante persone sono state colpite dalla violazione di dati personali?
   a. (numero esatto) persone
   b. circa (numero) persone
   c. un numero (ancora) sconosciuto di persone

9. Che tipo di dati sono coinvolti nella violazione?
   a. Dati anagrafici
   b. Numeri di telefono
   c. Indirizzi di posta elettronica
   d. Dati di accesso e di identificazione (username, password, customer ID, altro)
   f. Altri dati personali (sesso, data di nascita/età ecc.) dati sensibili e giudiziari
   g. Ancora sconosciuto
   h. Altro (specificare)

10. Livello di gravità della violazione di dati personali (secondo le valutazioni del Titolare):
   a. Basso/trascurabile
   b. Medio
   c. Alto
   d. Molto alto

11. Misure tecniche e organizzative applicate ai dati colpiti dalla violazione.

12. La violazione è stata comunicata anche a contraenti (o ad altre persone interessate)?
   a. Sì, e stata comunicata il (data)
   b. No, perché (specificare)

13. Qual è il contenuto della comunicazione ai contraenti (o alle persone interessate)? (riportare il testo della comunicazione)

14. Quale canale è utilizzato per la comunicazione ai contraenti (o alle altre persone interessate)?

15. Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

16. La violazione coinvolge contraenti (o altre persone interessate) che si trovano in altri Paesi EU?

17. La comunicazione è stata effettuata alle competenti Autorità di altri Paesi EU? a. No b. Sì (specificare)