MODALITÁ DI GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI AI SENSI DEL REGOLAMENTO UE 2016/679

Sommario

REDAZIONE Gruppo di lavoro interaziendale responsabili privacy Responsabile protezione dati ORAS Dott.ssa Provvidenza Mariella Stella Responsabile protezione dati AOU Policlinico Consorziale Bari Dott. Gianni Lucatorto	Data	*Firma / Timbro*
VERIFICA Responsabile Sistemi Informativi P.I. Fabio Bassotto Direttore Amministrativo Dott Andrea Pauletti Direttore Sanitario Dott.ssa Alessandra Cappelletto		
APPROVAZIONE Amministratore Delegato Dott. Francesco Rizzardo		

1. INTRODUZIONE

Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. (Considerando 85 Regolamento generale UE 2016/679).

In caso di violazione dei dati personali, Il Regolamento generale Ue 2016/679 dispone che il titolare del trattamento notifichi la violazione all'Autorità Garante per la protezione dei dati personali (Autorità) 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, la stessa è corredata dei motivi del ritardo (art 33, par 1).

Pertanto, la notifica all'Autorità dell'avvenuta violazione è subordinata alla valutazione del rischio per i diritti e le libertà degli interessati che spetta al titolare.

In caso di rischi elevati per i diritti e le libertà, si dovranno informare della violazione anche gli interessati, sempre "senza ingiustificato ritardo" fatte salve alcune eccezioni (art. 34 paragrafo 3 Regolamento UE 2016/679). In ogni caso, tutti i titolari del trattamento dovranno documentare le violazioni dei dati personali subiti, anche se non notificate all'autorità di controllo e non comunicate agli interessati. Il titolare dovrà documentare accuratamente le circostanze, le conseguenze e le contromisure adottate al fine di impedire che un evento simile si verifichi in futuro. Il titolare è tenuto ad esibire la documentazione, su richiesta, all'Autorità Garante, in caso di accertamenti (Art. 33 paragrafo 5): "*Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo*".

2. SCOPO E CAMPO D'APPLICAZIONE E DIVULGAZIONE

La presente procedura disciplina la modalità di gestione delle violazioni di dati personali, ivi inclusi gli obblighi di notifica all'Autorità ed agli interessati, ove applicabile, e le modalità per documentare

le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati.

La presente procedura si applica a tutti i dipendenti dell'Ospedale Riabilitativo di Alta Specializzazione (ORAS), senza distinzione di ruolo e livello, al personale in comando, ai Liberi Professionisti e a tutti i collaboratori che a qualunque titolo svolgono la loro attività per conto dell'ORAS (es. tirocinanti, stagisti, studenti universitari, consulenti).

Il presente documento si applica anche ai dipendenti di società esterne affidatarie di servizi da parte dell'ORAS nominati Responsabili del trattamento ai sensi dell'art. 28 del Regolamento generale UE 2016/679.

la presente procedura è pubblicata nell'intranet aziendale e viene consegnata ai responsabili esterni di trattamento nominati ai sensi dell'art. 28 del Regolamento generale UE 2016/679 al momento della firma del contratto.

3. DEFINIZIONI

Violazione di dati personali - Per violazione dei dati personali (data breach) si intende la divulgazione (intenzionale o non), la distruzione, la perdita, la modifica o l'accesso non autorizzato ai dati trattati da aziende o pubbliche amministrazioni. La violazione dei dati personali, quindi, non è rappresentata solo da un attacco informatico, ma può essere anche un accesso abusivo, un incidente (es. un incendio o una calamità naturale), la semplice perdita di una chiavetta USB o la sottrazione di documenti con dati personali, il furto di un notebook di un dipendente. In sostanza la violazione dei dati personali racchiude un ventaglio molto ampio di eventi avversi che comprometterebbero i dati personali e di conseguenza la dignità e le libertà fondamentali dell'individuo a cui si riferiscono.

Incidente e violazione – Sono eventi che compromettono la confidenzialità, l'integrità e la disponibilità del dato. E' necessario esplicitare la differenza terminologica tra incidente e violazione dei dati personali, con l'incidente non si verifica il furto e la divulgazione di dati personali che invece si verifica con la violazione.

Grado di rischio – tipologia e livello di danno, fisico, materiale o immateriale che una violazione può comportare alle persone fisiche quali ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, quali ad esempio: "discriminazione, furto o usurpazione

d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata". In assenza di ulteriori indicazioni, il considerando n. 85 del Regolamento offre alcuni criteri per delimitare il "rischio" che una violazione dei dati personali può comportare.

Pseudonimizzazione – il trattamento dei dati personali effettuato in modo tale che gli stessi non possano più essere 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.

4. TIPOLOGIA DI VIOLAZIONI E CAUSE

Di seguito sono esplicitate a titolo indicativo e non esaustivo le tipologie di violazioni e le possibili cause.

4.1. Tipologia di violazioni

4.1.1. Fisica

- Accesso abusivo in ambienti di lavoro riservati
- Lettura, copia e fotografia di documenti contenenti dati personali e sanitari;
- Sottrazione di documenti cartacei
- Sottrazione di computer, supporti di memorizzazione e di altri dispositivi elettronici contenenti dati personali

4.1.2. Logica

- Accesso abusivo alla postazione di lavoro (Pdl)
- Furto di credenziali degli amministratori
- Indisponibilità dei dati e delle informazioni del data center aziendale
- Alterazione dei dati (crittografia da virus, scambio di anagrafiche sui dati sanitari)
- Perdita di confidenzialità/riservatezza dei dati
- Perdita di memorie USB non cifrate sulle quali sono stati copiati dati personali e particolari di pazienti e/o di dipendenti;
- Supporti di memorizzazioni distrutti e/o rovinati.

4.2. Possibili cause di violazioni

4.2.1. Utilizzo scorretto della Postazione di lavoro, dei dispositivi mobili (notebook, tablet e smartphone) e dei supporti di memorizzazione (chiavette USB, CD)

- Postazione di lavoro incustodita e non bloccata (assenza del salvaschemo)
- Memorizzazione delle credenziali nei software
- Annotazione delle credenziali in prossimità della postazione di lavoro
- Scelta di password deboli (quali ad esempio nome, cognome, data di nascita, 12345678)
- Uso di un algoritmo noto per la creazione di password per gli utenti
- Lasciare incustoditi o perdere supporti di memorizzazione USB non protetti da password e non cifrati e contenenti dati personali e particolari

4.2.2. **Eventi con effetti sul data center aziendale**

- Guasto fisico al sistema servente
- Anomalie software dei Sistemi Operativi
- Anomalie nei sistemi di alimentazione elettrica
- Anomalie nei sistemi di raffrescamento
- Eventi naturali, (inondazioni, terremoti, ecc.)
- Azioni derivanti da maleware
- Azioni di Denial of Service
- Intercettazioni di rete (Man in The Middle)
- Utilizzo delle credenziali di default nei database
- Escalation dei privilegi derivante da maleware
- Errore di configurazione degli account utente e delle relative autorizzazioni
- Utilizzo di credenziali amministrative, con maggiori privilegi, da parte degli utenti.

5. RESPONSABILITÀ

5.1. Tutto il personale

Tutti coloro che trattano i dati personali e sanitari per conto dall'Ospedale Riabilitativo di Alta Specializzazione (ORAS), che vengono a conoscenza di una potenziale o violazione certa sui sopracitati dati, sono obbligati a segnalare tempestivamente l'accaduto al Direttore/Responsabile UU.OO/Servizio/Area amministrativa presso la quale operano.

5.2. Direttori e Responsabili delle UU.OO/Servizi/Aree amministrative

Secondo il modello organizzativo adottato, i Direttori ed i Responsabili delle UU.OO/Servizi/Aree amministrative devono segnalare tempestivamente al Titolare del trattamento e al Responsabile della Protezione Dati (RPD) l'evento avverso verificatosi nell'U.O./Area di responsabilità e collaborare alla corretta gestione dell'iter per la violazione.

5.3. Responsabili esterni del trattamento (fornitori e manutentori)

I Responsabili del trattamento nominati ai sensi dell'Art. 28, devono, senza ingiustiticato ritardo, segnalare tempestivamente al Titolare del trattamento e al Responsabile della Protezione Dati (RPD) l'evento avverso verificatosi sui sistemi, e/o sui dati personali e particolari, trattati in virtù del rapporto contrattuale. In caso di una violazione sospetta o certa il Responsabile esterno del trattamento deve collaborare per la corretta gestione dell'incidente.

5.4. Contitolari

I contitolari del trattamento, ove presenti, devono determinare le rispettive responsabilità in merito all'osservanza del regolamento . Ciò includerà la determinazione di chi sarà responsabile di adempiere agli obblighi di cui agli articoli 33 e 34. In presenza di una violazione sospetta o certa il primo dei Contitolari che viene a conoscenza dell'evento avverso deve, senza ingiustiticato ritardo, segnalare tempestivamente all'altro Titolare del trattamento e al Responsabile della Protezione Dati (RPD) di competenza l'evento avverso verificatosi che ha visto coinvolti di dati personali e/o particolari in contitolarità, nel rispetto di quanto disciplinato nel rapporto contrattuale tra contitolari. Entrambi dovranno collaborare per la corretta gestione della violazione.

5.5. Titolare

Il titolare del trattamento non appena riceve una segnalazione di una potenziale o violazione certa dei dati personali ha la responsabilità di avviare e gestire l'iter per la violazione ponendo in essere:

- l'attività conoscitiva
- la valutazione del rischio e delle conseguenze per gli interessati
- la notifica della violazione all'Autorità ed agli interessati, ove applicabile, senza ingiustificato ritardo e ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza.
- il ripristino e la mitigazione del rischio.

Inoltre, il titolare ha la responsabilità di documentare le violazioni dei dati personali subite, anche se non notificate all'Autorità di controllo e non comunicate agli interessati.

5.6. Responsabile Protezione Dati

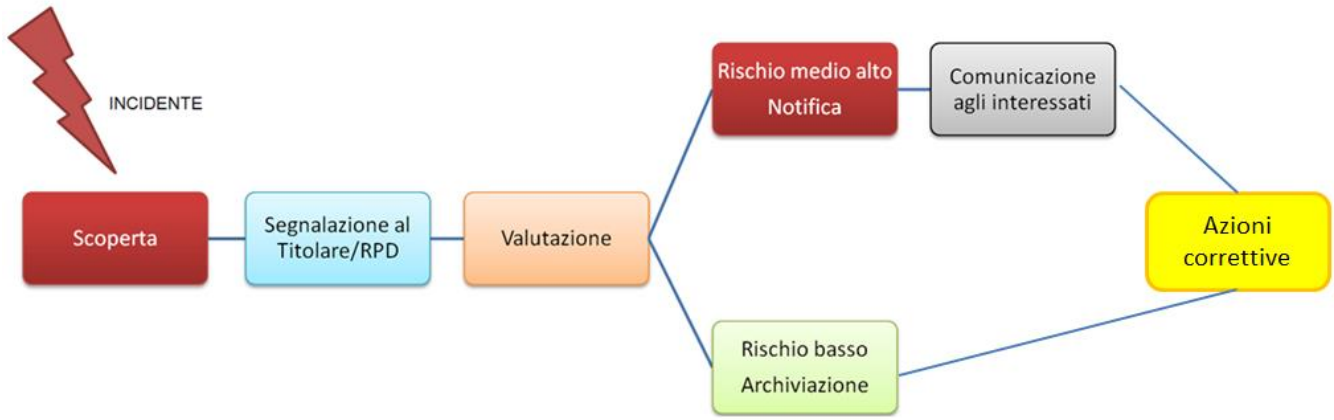
Il Responsabile della Protezione dati fornisce consulenza al titolare coadiuvandolo nella gestione dell'iter per la valutazione della violazione, sorvegliando l'osservanza del regolamento e fungendo da punto di contatto per l'Autorità (art.39 par1).

6. MODALITÀ PER LA GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI

Il Regolamento Europeo per la Protezione dei Dati Personali individua perentoriamente il termine massimo di 72 ore entro il quale deve essere comunicato all'Autorità di controllo l'evento avverso verificatosi sui dati personali e le potenziali conseguenze della violazione sui diritti e le libertà fondamentali degli individui a cui si riferiscono i dati.

Di seguito vengono descritte le attività che dovranno essere espletate non appena si viene a conoscenza di un evento avverso/violazione dei dati personali raggruppate in quattro fasi.

Figura 1: Rappresentazione schematica dell'iter per la gestione della violazione



6.1. Fase 1 Segnalazione al Titolare e al RPD

Tutti coloro che vengono a conoscenza di una violazione certa o presunta dei dati personali dovranno tempestivamente segnarlo al Direttore/Responsabile dell'U.O/Servizio/Area amministrativa presso la quale operano.

Il Direttore/ Responsabile dell'U.O/Servizio/Area amministrativa, dovrà tempestivamente segnalare l'accaduto al Titolare e al RPD utilizzando il modello di comunicazione della violazione dei dati personali, allegata alla presente procedura e segnalando, obbligatoriamente, le seguenti informazioni necessarie ad avviare l'istruttoria:

- Denominazione della/e banca/banche dati oggetto di violazione e una breve descrizione di quanto accaduto e dei dati personali coinvolti
- Data e ora dell'evento
    - Un eventuale intervallo di tempo nel quale si è verificato l'evento (se noto)
    - Se l'evento è ancora in corso
    - Oppure se non si riesce a determinare l'esatta insorgenza dell'evento avverso
- Descrizione del luogo in cui si è verificato l'evento specificando se è avvenuto in seguito ad uno smarrimento di un dispositivo elettronico, una memoria USB, o semplicemente lo smarrimento o sottrazione di un documento cartaceo
- Indicazione del tipo di esposizione al rischio e se si sia verificata il seguente tipo di violazione
    - Lettura (presumibilmente i dati non sono stati copiati)
    - Copia (i Titolare è ancora in possesso dei dati)
    - Alterazione (i dati sono presenti ma sono stati alterati)
    - Cancellazione/distruzione (i dati non sono più posseduti dal titolare e non li ha neppure l'autore della violazione)
    - Furto (i dati non sono più posseduti dal titolare, sono ora in possesso dell'autore della violazione)
- Indicazione del dispositivo oggetto della violazione
    - Computer
    - Rete
    - Dispositivo mobile
    - File o parte di un file

- Strumento di backup
- Documento cartaceo

6.2. Fase 2 rilevazione/accertamento della violazione (attività conoscitiva)

Il Titolare, supportato dal RPD, individua un team per la gestione dell'incidente, nel quale ogni soggetto coinvolto ha delle specifiche responsabilità. L'assegnazione dei ruoli deve quindi essere sufficientemente precisa da consentire l'identificazione univoca di specifici gruppi di persone che eseguono ciascuna azione (nella maggior parte dei casi un soggetto responsabile e un sostituto devono essere identificati) .

Pertanto, il team per la gestione dell'incidente deve essere composto in funzione della tipologia della violazione e delle rispettive responsabilità.

Se l'evento riguarda una violazione fisica quale ad esempio il furto o lo smarrimento di documenti cartacei contenenti dati personali, faranno parte del team per la gestione dell'incidente:

- il Titolare coadiuvato dall'RPD
- il Direttore/Responsabile dell'U.O/Servizio/Area amministrativa. in cui si è verificato l'evento
- il Direttore Sanitario o Amministrativo, o un suo delegato, a seconda se l'U.O. interessata è Sanitaria o Amministrativa
- il Responsabile della Prevenzione e Protezione
- i Responsabili esterni nominati ai sensi dell'art. 28 del Regolamento generale UE 2016/679.

L'istruttoria sarà focalizzata sulle misure di sicurezza fisiche e sulle misure organizzative adottate nell'U.O/Servizio/Area amministrativa e sulle eventuali azioni di mitigazione già in corso, evidenziandone l'attuazione in un arco temporale.

Nel caso di eventi avversi riguardanti i dati e i documenti informatici (software gestionali, dossier sanitario elettronico, videosorveglianza ecc.) faranno parte del team per la gestione dell'incidente:

- il Titolare coadiuvato dall'RPD
- il Responsabile dell'Ufficio Sistemi Informativi e l'Amministratore di Sistema dell'infrastruttura violata
- il Direttore/Responsabile dell'U.O/Servizio/Area amministrativa in cui si è verificato l'evento
- il Direttore Sanitario o Amministrativo, o un suo delegato, a seconda se l'U.O/Servizo/Area interessata è Sanitaria o Amministrativa
- il Responsabile della videosorveglianza, ove applicabile

- i Responsabili esterni nominati ai sensi dell'art. 28 del Regolamento generale UE 2016/679.

Se la violazione è avvenuta sui dispositivi informatici presenti nelle UU.OO/Servizi/Aree amministrative l'istruttoria sarà focalizzata sulle misure di sicurezza informatiche e sulle misure organizzative adottate dalle stesse.

Nell'eventualità che la violazione sia stata perpetrata nei confronti dell'infrastruttura informatica aziendale le attività per l'individuazione delle cause e conseguenze saranno svolte a cura del Responsabile dell'Ufficio Informatico e dell'Amministratore di sistema di competenza. Saranno, inoltre, prese in considerazione le eventuali azioni di mitigazione già in corso, evidenziandone l'attuazione in un arco temporale.

6.3. Fase 3 Analisi della violazione, valutazione dei rischi connessi e notifica

In questa fase ogni componente del team per la gestione dell'incidente, per quanto di competenza, deve acquisire e valutare le evidenze al fine di individuare il livello di gravità della violazione nei confronti dei dati personali e determinare le conseguenze per i diritti e le libertà degli interessati.

Al fine di calcolare il livello dell'impatto e la gravità delle conseguenze derivanti da una violazione dei dati personali, si fa riferimento alle raccomandazioni elaborate dall'Agenzia Europea per la Sicurezza delle Reti e delle Informazioni (ENISA).

6.3.1. Violazione di dati: assenza di rischio

Nel caso in cui la violazione dei dati personali non determini alcuna compromissione ai diritti e alla libertà fondamentali degli interessati non è obbligatoria la notifica all'Autorità ma è comunque necessario comprovare l'assenza dei rischi. Inoltre, è necessario registrare la violazione in un apposito registro.

6.3.2. Violazione di dati: presenza di rischi e notifica all'autorità di controllo

In presenza di rischi per gli interessati il Titolare per il tramite del RPD, notifica la violazione entro 72 ore all'Autorità Garante per la Protezione dei Dati Personali utilizzando l'apposita modulistica Qualora la notifica non sia effettuata entro 72 ore, la stessa è corredata dai motivi del ritardo, ove applicabile, e con quale mezzo.

6.4. Fase 4 – avvio delle azioni correttive

I componenti del team per la gestione dell'incidente impegnati nella gestione della violazione devono individuare tempestivamente:

- le strategie per ripristinare il servizio o i dati personali compromessi

- mitigare il rischio ed individuare le misure correttive in tal senso.

7. ARCHIVIAZIONE DEI DOCUMENTI

La documentazione relativa alla gestione delle violazioni dei dati personali su supporto cartaceo viene conservata in doppia copia presso la Direzione generale e l'ufficio protezione dei dati personali.

La documentazione relativa alla gestione delle violazioni dei dati personali riguardanti i dati ed i documenti informatici viene conservata in triplice copia presso la Direzione generale, l'ufficio Informatico e l'ufficio protezione dei dati personali.

Il Registro delle violazioni, se non ancora informatizzato, deve essere custodito da parte dell'Ufficio protezione dati personali ed a disposizione dell'Autorità Garante per la protezione dei dati personali.

8. STORIA DELLE MODIFICHE

Revisione	Data Emissione	Esito
00	novembre 2018	Prima emissione

9. ALLEGATI

Allegato 1: Modello di comunicazione di incidente/violazione dei dati personali al Titolare/RPD