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

REDAZIONE Caposervizio privacy e banche dati e RPD Provvidenza Mariella Stella	Data 20.01.2022	*Firma / Timbro* *Firmato in originale*
VERIFICA Responsabile Sistemi Informativi Fabio Bassotto RFSP Davor Perkovic Direttore Amministrativo Andrea Pauletti Direttore Sanitario Guido Sattin	 20.01.2022 24.01.2022 24.01.2022 24.01.2022	 *Firmato in originale*
APPROVAZIONE Amministratore Delegato Orianna Romanello	 26.01.2022	 *Firmato in originale*

Sommario

1. INTRODUZIONE

Il 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 (di seguito RGPD 2016/679 o Regolamento) all'articolo 4, punto 12 definisce la "violazione dei dati personali" (c.d. "data breach") come la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. In tal senso, si ha:

- "distruzione" dei dati, ogni qual volta gli stessi non esistono più o non esistono più in una forma che sia di qualche utilità per il titolare del trattamento;
- "danno" quando i dati personali sono stati modificati, corrotti o non sono più completi;
- "perdita" dei dati personali nel caso in cui i dati potrebbero comunque esistere, ma il titolare del trattamento potrebbe averne perso il controllo o l'accesso, oppure non averli più in possesso. Un esempio di perdita di dati personali può essere la perdita o il furto di un dispositivo contenente una copia della banca dati del titolare del trattamento; oppure il caso in cui l'unica copia di un insieme di dati personali sia stata crittografata da un ransomware (malware del riscatto) oppure dal titolare del trattamento mediante una chiave non più in suo possesso;
- "trattamento non autorizzato o illecito" quando viene effettuata una divulgazione di dati personali a (o l'accesso da parte di) destinatari non autorizzati a ricevere (o ad accedere a) i dati oppure quando viene svolta qualsiasi altra forma di trattamento in violazione del regolamento.

Come indicato all'articolo 4, punto 12, il Regolamento si applica soltanto nel caso in cui un incidente di sicurezza comporta la violazione di dati personali. La conseguenza di questo tipo di violazione è che il titolare del trattamento non è più in grado di garantire l'osservanza dei principi applicabili al trattamento dei dati personali (articolo 5 del sopracitato Regolamento: liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza).

In caso di violazione dei dati personali, il Regolamento 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 interessate. 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 RGPD 2016/679).

In ogni caso, il titolare del trattamento dovrà 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

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.

3. CAMPO D'APPLICAZIONE E DIVULGAZIONE

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, per gli obblighi di competenza, 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.

4. DEFINIZIONI

Azioni di Denial of Service - malfunzionamento dovuto ad un attacco informatico in cui si fanno esaurire deliberatamente le risorse di un sistema informatico che fornisce un servizio ai client, ad esempio un sito web su un web server, fino a renderlo non più in grado di erogare il servizio ai client richiedenti.

Data center – chiamato anche *CED* (Centro Elaborazione Dati) o *server farm*, ospita tutte le apparecchiature necessarie a governare il sistema informativo aziendale. Tra queste apparecchiature figurano server, storage, router e tutto ciò che serve per garantire la continuità operativa del business.

Escalation di privilegi - lo sfruttamento di una falla, di un errore di progetto o di configurazione di un software applicativo o di un sistema operativo al fine di acquisire il controllo di risorse di macchina normalmente precluse a un utente o a un'applicazione.

Grado di rischio – tipologia e livello di danno, fisico, materiale o immateriale che una violazione può comportare alle persone fisiche, 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.

Incidente e violazione – Sono eventi che compromettono la confidenzialità, l'integrità e la disponibilità del dato. E' necessario esplicitare la differenza terminologica tra incidente di sicurezza delle informazioni e violazione dei dati personali in quanto non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali. La violazione è una particolare tipologia di incidente di sicurezza delle informazioni, che coinvolge i dati personali.

Intercettazioni di rete rete (Man in The Middle) - attacco informatico in cui qualcuno segretamente ritrasmette o altera la comunicazione tra due parti che credono di comunicare direttamente tra di loro

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.

Ransomware - è un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (ransom in inglese) da pagare per rimuovere la limitazione. Ad esempio alcune forme di ransomware bloccano il sistema e intimano all'utente di pagare per sbloccare il sistema, altri invece cifrano i file dell'utente chiedendo di pagare per riportare i file cifrati in chiaro.

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.

5. TIPOLOGIA DI VIOLAZIONI E POSSIBILI CAUSE

Si considerano eventi di Data Breach quelli che comportano in modo accidentale o illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai

dati personali trattati dall'ORAS. Tali eventi comportano rischi per i diritti e le libertà degli interessati, e potrebbero avere un impatto indiretto sulla reputazione del titolare.

I principali rischi per i diritti e le libertà degli interessati sono i seguenti:

- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati degli interessati;
- limitazioni dei diritti/discriminazione;
- furto o usurpazione di identità;
- perdite finanziarie/danno economico o sociale o reputazionale (sia per l'interessato che per il Titolare);
- decifratura non autorizzata della pseudonimizzazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari);

o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. (Considerando 85 RGPD 2016/679).

Nelle tabelle esposte di seguito sono esplicitate a titolo indicativo e non esaustivo alcune tipologie di violazioni di dati personali (Tabella 1) e le possibili cause .

Tabella 1

TIPOLOGIE DI VIOLAZIONI DEI DATI PERSONALI **Le tipologie di violazioni di dati personali descritte nella colonna a sinistra se vengono commesse volontariamente, cambiano nel nome e nel significato**	
Accidentali	**Volontarie**
1. Accesso non autorizzato Qualcuno non poteva vedere certe informazioni, ma le ha viste. *Esempio: Comunicazione/consegna/invio per posta di documenti riservati e/o informazioni sulla salute a persona sbagliata*[1]*.* *Pubblicazione di documentazione sanitaria di un interessato su dse/fse di un'altra persona.*[2]	**1. Accesso non autorizzato = Spionaggio** *Esempio: accesso abusivo in ambienti di lavoro riservati, alle postazioni di lavoro (Pdl)*

[1] Autorità Garante per la Protezione dei Dati Personali, Provvedimento n. 123 del 2 luglio 2020
[2] [2] Autorità Garante per la Protezione dei Dati Personali, Provvedimento n.141 del 9 luglio 2020

2. Copia non autorizzata Qualcuno ha preso dei dati che non poteva prendere e li ha copiati da un'altra parte. Esempio: *nel regolamento aziendale e nelle istruzioni al personale c'è scritto che non si devono copiare i dati al di fuori del sistema di archiviazione aziendale, ma Antonio ha preso i dati e li ha copiati su una chiavetta USB. È una violazione.*	**2. Copia non autorizzata = Furto** *Esempio: sottrazione (analogica o digitale) volontaria di documenti, computer, supporti di memorizzazione e di altri dispositivi elettronici contenenti dati personali e sanitari, Furto di credenziali degli amministratori*
3. Divulgazione non prevista Qualcuno diffonde accidentalmente dei dati. *Esempio: Pubblicazione sui social network aziendali di foto di cene aziendali che possono compromettere la reputazione di alcuni interessati, anche in presenza di consenso*	**3. Divulgazione non prevista = Diffusione volontaria** Perdita di confidenzialità/riservatezza dei dati
4. Modifica non autorizzata Qualcuno ha modificato dei dati che non poteva modificare. *Esempio: modifica dei contenuti dei file di Excel/word condivisi nelle cartelle di rete e non bloccati anche se il Disciplinare aziendale lo vieta.*	**4. Modifica non autorizzata = Compromissione** *Esempio: Alterazione dei dati (crittografia da virus, scambio di anagrafiche sui dati sanitari).*
5. Perdita d'accesso Qualcuno perde delle informazioni, che diventano temporaneamente o definitivamente non disponibili. *Esempio: Indisponibilità temporanea dei dati e delle informazioni del data center aziendale.* *Perdita delle password di accesso a file protetti*	**5. Perdita d'accesso = Cifratura** *Esempio: infetto volontariamente con il CryptoLocker il computer che contiene tutti i dati personali dei dipendenti*
5. Cancellazione 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. *Esempio*: *Qualcuno cancella il file che conteneva delle informazioni che erano solo lì.*	**6. Cancellazione dei dati = distruzione volontaria.**

Tabella 2

Possibili cause di violazioni		
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	
2. Eventi con effetti sul data center aziendale	**accidentali/naturali** - Guasto fisico al sistema server - Anomalie software dei Sistemi Operativi - Anomalie nei sistemi di alimentazione elettrica - Anomalie nei sistemi di raffrescamento - Eventi naturali, (inondazioni, terremoti, ecc.)	**malevoli** - 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 malware - Errore di configurazione degli account utente e delle relative autorizzazioni - Utilizzo di credenziali amministrative, con maggiori privilegi, da parte degli utenti.
3. Eventi con effetti sull'integrità e/o riservatezza dei dati personali degli interessati	**Accidentali da errore umano o tecnologico** Errata identificazione dell'interessato Selezione di anagrafica sbagliata Errata configurazione e/o interoperabilità di sistemi software	

6. RESPONSABILITÀ

- 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 violazione di dati, potenziale o certa, sono obbligati a segnalare tempestivamente l'accaduto nelle modalità previste dalla presente procedura (paragrafo 8.1)

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

Direttori e 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.

- 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.

- 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.

- Titolare

Il titolare del trattamento non appena riceve una segnalazione di una violazione dei dati personali, potenziale o certa 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.

- 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).

7. PIANIFICAZIONE (prima dell'evento)

il Titolare, supportato dal RPD, in fase di stesura della presente procedura ha individuato e formalizzato la composizione di un "team di crisi", nel quale ogni soggetto coinvolto e/o un suo sostituto ha delle specifiche responsabilità e attività da svolgere, per la gestione di incidenti/violazioni. La presente procedura è condivisa con i membri del Team crisi all'atto della loro nomina

7.1. Team crisi

Il team crisi di ORAS è composto da:

- Rappresentante legale dell'ORAS, che è anche la funzione che ha la responsabilità di comunicare con organi di stampa, responsabile del team
- DPO
- ADS/Responsabile dell'ufficio Sistemi Informativi
- Responsabile Area Risorse Umane nel caso in cui l'evento coinvolga i dati dei dipendenti dell'ORAS
- Direttore Sanitario nel caso in cui l'evento coinvolga i dati dei pazienti/utenti di prestazioni sanitarie
- Direttore Amministrativo nel casi in cui l'evento riguardi i servizi esternalizzati dal titolare a Responsabili esterni del trattamento o per le attività/Servizi svolti dall'ORAS in qualità di responsabile del trattamento.

Fanno parte del Team anche altre funzioni aziendali (RFSP, RSPP, responsabili U.OO/Servizi/Aree Amministrative) o esterne (responsabile esterno e/o sub responsabile o Contitolare), che verranno di volta in volta coinvolte in base al tipo di evento,

7.1.1. Formazione del Team crisi

Prima della pubblicazione della presente procedura il Team crisi effettua una formazione mirata sulla applicazione della stessa; tale formazione è ripetuta quando necessario.

7.1.2. Responsabili esterni, Sub-responsabili, Contitolari

Nei contratti con i responsabili esterni, nei rapporti con i contitolari e nelle autorizzazione per i sub responsabili deve essere indicato in modo vincolante:

- la richiesta di valutazione della loro procedure di Data Breach
- la specificazione dei tempi di comunicazione di data breach all'ORAS che deve tener conto delle 72 ore a capo del Titolare per la segnalazione (es. 24 ore dalla rilevazione per i contitolari e responsabili e 12 ore per i sub-responsabili)
- le conseguenze nel caso di mancata o ritardata comunicazione
- la figura di riferimento per la comunicazione (Privacy Officer) ed i riferimenti per contattarla

7.1.3. Verbalizzazione delle attività

Tutte le attività e le riunioni del Team crisi debbono essere verbalizzate; i verbali sono conservati dal Responsabile del Team, nell'archivio "privacy" di ORAS per almeno 10 anni (o in relazione agli effetti che il Data Breach può avere sui diritti degli interessati). In ogni verbale (sottoscritto dai partecipanti alla riunione) deve essere indicato:

- chi partecipa (membro del Team/invitato all'incontro)
- decisioni assunte nel corso dell'incontro
- stato di avanzamento delle decisioni assunte nel corso di incontri precedenti

7.1.4. Disponibilità e posizione del Titolare del Trattamento

Il Titolare del trattamento è tenuto informato degli sviluppi in ogni fase dell'indagine; e, avvalendosi del supporto del RPD, ha il potere di imporre misure più restrittive a tutela dei diritti degli interessati nell'attuazione delle decisioni prese dal team di crisi.

7.1.5. Ruolo di eventuali esperti esterni

Per le azioni previste dalla procedura possono essere coinvolti esperti esterni (in materia di cybersecurity e legale), che avranno un conferimento d'incarico nel rispetto delle procedure aziendali e previa sottoscrizione di un vincolo di riservatezza.

7.2. Modalità per la comunicazione di data breach

Nel sito di ORAS devono essere pubblicate, in modo visibile, le modalità per la comunicazione di un data breach, per rendere evidente e fruibile la consultazione agli interessati. Tra le informazioni riportate deve essere esplicitato il canale di comunicazione che l'interessato, il Garante per la protezione dei dati personali, i responsabili esterni (designati ai sensi dell'art. 28 del RGPD 2016/679) e l'indirizzo e-mail, (violazione.datipersonali@ospedalemotta.it) che i delegati e gli autorizzati possono utilizzare per questo tipo di eventi, in quanto costantemente presidiato.

La finalità è quella di comunicare anche all'esterno dell'ORAS come segnalare gli eventi che possono portare a situazioni anomale/sospette o Data Breach. La mail di contatto per le segnalazioni violazione.datipersonali@ospedalemotta.it è reindirizzata nella casella di posta elettronica dell'Amministratore Delegato, RPD e del Responsabile Sistemi Informativi.

In ORAS la responsabilità complessiva della gestione della comunicazione verso l'esterno è dell'Amministratore Delegato che definisce con i membri del team di crisi la strategia di comunicazione da attuare:

- Individuazione della/le forma/e di comunicazione da utilizzare
- stesura ed approvazione delle comunicazioni
- livello di coinvolgimento del Team crisi nella comunicazione verso l'esterno

7.2.1. Esempio di comunicazione esterna della modalità di gestione di data breach

Di seguito si riporta un esempio di contenuti per la comunicazione esterna delle modalità di gestione di un data breach:

«…L'ORAS, al fine di tutelare i dati personali dei propri utenti, ha predisposto una procedura aziendale per affrontare e gestire nel miglior modo possibile le eventuali violazioni dei dati personali.

Ciò, in quanto, una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, causare danni alla persona fisica.
La violazione dei dati personali può consistere nella distruzione, perdita, modifica, divulgazione non autorizzata o dall'accesso, in modo accidentale od illegale, a dati personali trasmessi, conservati o comunque trattati.
Riteniamo opportuno informare i nostri utenti, collaboratori, fornitori sui rischi che potrebbero derivare dalle violazioni sopra elencate.
Ai sensi del Regolamento europeo, infatti, i principali rischi per i diritti e le libertà di tutti gli interessati, a seguito dell'avvenuta violazione dei dati sono:

- *danni fisici, materiali o immateriali alle persone fisiche;*
- *perdita del controllo dei dati degli interessati;*
- *limitazioni dei diritti/discriminazione;*
- *furto o usurpazione di identità;*
- *perdite finanziarie/danno economico o sociale o reputazionale (sia per l'interessato che per il Titolare);*
- *decifratura non autorizzata della pseudonimizzazione;*
- *perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari);*
- *o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata*

Nel caso in cui si verifichi una violazione dei dati personali degli interessati l'ORAS ha previsto espressamente una procedura d'intervento che per trasparenza vuole comunicarle.

la informiamo che abbiamo costituito un Team crisi, così composto:

- *Rappresentante legale dell'ORAS, che è anche la funzione che ha la responsabilità di comunicare con organi di stampa, responsabile del team*

- *DPO*
- *ADS/Responsabile dell'ufficio Sistemi Informativi*
- *Responsabile Area Risorse Umane nel caso in cui l'evento coinvolga i dati dei dipendenti dell'ORAS*
- *Direttore Sanitario nel caso in cui l'evento coinvolga i dati dei pazienti/utenti di prestazioni sanitarie*
- *Direttore Amministrativo nel casi in cui l'evento riguardi i servizi esternalizzati dal titolare a Responsabili esterni del trattamento o per le attività/Servizi svolti dall'ORAS in qualità di responsabile del trattamento;*

Fanno parte del Team anche altre funzioni aziendali (RFSP, RSPP, responsabili UU.OO/Servizi/Aree Amministrative) o esterne (responsabile esterno e/o sub responsabile o Contitolare), che verranno di volta in volta coinvolte in base al tipo di evento,

Questo Team, in caso di data breach si occuperà di analizzare la gravità dell'evento prendendo in considerazione i dati, gli interessati coinvolti, la portata e l'arco temporale secondo precisi parametri individuati.

A seguito di tale analisi l'ORAS realizzerà un'approfondita valutazione del rischio al fine di comprendere l'effettiva sussistenza o meno della violazione.

In caso di esito positivo il Team procederà alla risoluzione del problema.

Deve sapere, inoltre, che in caso di violazione dei suoi dati potrebbe essere necessario dover comunicare al Garante Privacy l'evento entro 72 ore dall'accadimento.
Per tale ragione, qualora, della violazione ne sia venuto a conoscenza un nostro Responsabile esterno del trattamento o sub responsabile essi sono tenuti a comunicarci la violazione, il primo entro 24 ore, il secondo entro 12 ore dalla scoperta del fatto.
Qualora, la violazione dei suoi dati abbia cagionato un rischio elevato per i suoi diritti e le sue libertà fondamentali, saremo tenuti a darle un'opportuna comunicazione al fine di consentirle di adottare idonee precauzioni volte a ridurre al minimo il potenziale danno derivante dalla violazione.

Nella comunicazione siamo tenuti ad indicare:

- *il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;*
- *le probabili conseguenze della violazione dei dati personali;*
- *le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.*

Non siamo obbligati ad informarla nel caso in cui abbiamo messo in atto misure tecniche ed organizzative adeguate di protezione sui dati oggetto della violazione o quando abbiamo successivamente adottato misure atte a scongiurare nuovi rischi elevati per i suoi diritti ed inoltre, quando la comunicazione richiederebbe sforzi sproporzionati. In questo caso procederemo con una comunicazione pubblica o misura simile. In ogni caso valuteremo l'opportunità, anche se non strettamente obbligatoria di tenerla aggiornata/o.

Se anche lei viene a conoscenza di una violazione dei dati personali può comunicarcela scrivendoci al seguente indirizzo mail violazione.datipersonali@ospedalemotta.it tale comunicazione verrà presa in esame dal team crisi, che procederà come sopra descritto…»

7.3. Tempistica

Il RGPD 2016/679 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. Il calcolo della tempistica decorre dal ricevimento di una segnalazione.

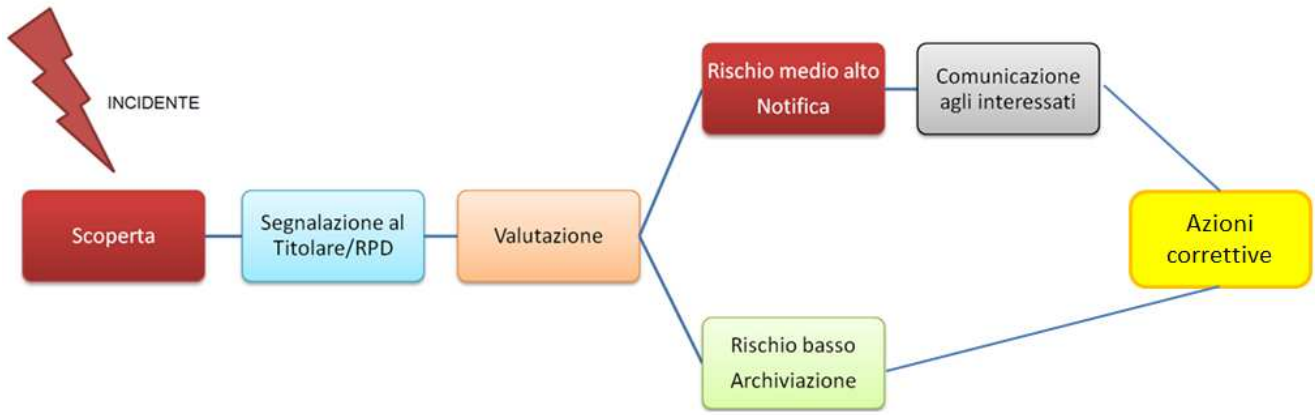
7.4. Rendicontazione delle attività del Team Crisi

Almeno annualmente il Titolare del trattamento/Responsabile Privacy predispone una relazione sulla attività del Team Crisi nel corso dell'anno. Tale relazione viene trasmessa all'Organo amministrativo di ORAS. La relazione, per quanto possibile è integrata da dati numerici per comprendere l'entità degli eventi ed i tempi di reazione.

8. GESTIONE EVENTO DI DATA BREACH (durante l'evento)

Di seguito vengono descritte le attività che dovranno essere espletate non appena si viene a conoscenza di un evento avverso/violazione dei dati personali, rappresentate schematicamente in figura 1.

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



Tutte le funzioni coinvolte devono prestare la massima collaborazione, attenzione e sensibilità alla gestione di evento di Data Breach.

8.1. Segnalazione

La segnalazione di un evento può provenire:

A. **dall'interno – personale che svolge l'attività lavorativa in ORAS**

Tutti i delegati privacy e autorizzati al trattamento che vengono a conoscenza di una violazione certa o presunta dei dati personali (compiuta dall'interno o dall'esterno) o siano a conoscenza di una comunicazione da parte di un interessato/terzo (anche esterno) devono:

- segnalare quanto appreso ad uno dei membri del Team di crisi in modo da attivare la procedura di valutazione dell'evento;
- la segnalazione può avvenire con qualsiasi forma, purché avvenga nel minor tempo possibile e, ove possibile utilizzando l'apposito modello UN0139;
- anche un solo sospetto deve essere comunicato perché si proceda con la valutazione.

B. **dall'esterno - interessato/Garante/media, stampa/soggetti terzi**.

In questi casi il RPD ed i componenti del team crisi:

- raccolgono le segnalazioni di possibile Data Breach provenienti dall'esterno in qualsiasi forma;
- consultano regolarmente il sito del Garante e gli organi di stampa specializzata per verificare eventuali situazioni di potenziale rischio che potrebbero riguardare anche l'ORAS;
- devono verificare l'autenticità della comunicazione ricevuta analizzando la fonte nota/registrata, informazione tramite canali regolari, messaggio con intestazione completa.

C. Dall'esterno - Responsabile esterno trattamento/subresponsabile/contitolare

Il responsabile privacy riceve le segnalazioni di possibile Data Breach provenienti da figure esterne con le quali è in essere un contratto di responsabile esterno/sub responsabile/contitolare; attraverso i canali definiti in tali contratti.

In tutti i casi il RPD comunica via mail con gli altri membri del Team crisi utilizzando la loro casella di posta e quella di violazione.datipersonali@ospedalemotta.it Tutte le comunicazioni che provengono da fonte interna o da Responsabili esterni devono essere identificate con l'orario (riportando, quando possibile un documento – es. mail – che l'attesta in modo univoco).

8.1.1. ID segnalazione

Ad ogni segnalazione è assegnato un numero univoco (ID) formato dal numero progressivo/anno. Questo numero permetterà di identificare in modo univoco tutta la documentazione che riguarda l'incidente e, per quanto possibile, deve essere sempre indicato.

Appena ricevuta la segnalazione deve essere avviata la compilazione, da parte del RPD del registro degli incidenti (modulo della piattaforma TESI gdpr)

8.2. Valutazione di pertinenza della segnalazione

Raccolta la segnalazione, attraverso le forme sopra indicate; il responsabile del Team crisi, convoca; in tempi brevi, entro massimo 12 ore dalla segnalazione[3], una riunione coinvolgendo tutti i membri ed eventuali altri soggetti potenzialmente coinvolti sulla base delle informazioni disponibili. Qualora qualche membro non fosse disponibile; si procede comunque con la riunione. Nel caso in cui dalla segnalazione si evince il coinvolgimento di un Responsabile esterno del trattamento (eventuale evento di Data Breach attribuibile al Responsabile), è necessario nel team valutare la presenza del Responsabile o assicurarsi la sua completa disponibilità.

Il team procede alla raccolta e annotazione delle informazioni per la gestione del Data Breach utilizzando il fac-simile per la notifica della violazione all'Autorità Garante per la Protezione Dati Personali (vedi allegato 1 alla presente procedura); se necessario, procede nella raccolta di eventuali ulteriori informazioni al fine di chiarire la veridicità, la portata e la reale sussistenza dell'evento segnalato.

Il Team di crisi valuta prioritariamente eventuali azioni correttive per contenere gli effetti dell'evento. Le azioni definite vengono messe in atto dal team attivando le risorse necessarie, le decisioni assunte vengono descritte nei verbali delle attività e delle riunioni del team, e documentate attraverso la registrazione nell'apposita sezione della piattaforma TESI GDPR per la gestione del data breach.

Qualora si verificasse, anche dopo eventuali approfondimenti; la non sussistenza di situazioni che mettono a rischio i dati degli interessati; il Team descrive tale scelta e comunica la decisione al Titolare (che potrebbe comunque richiedere un ulteriore approfondimento). Il Team valuta la necessità di procedere ad una eventuale azione correttiva e registra tale decisione nell'apposita sezione della piattaforma TESI GDPR per la gestione del data breach.

Negli altri casi il Team procede a:

- valutare la conseguenze dell'evento, tipologia di dati personali colpiti, portata (n. e/o % interessati coinvolti e n. dati), arco temporale.

Sulla base degli elementi raccolti, valuta la presenza o meno della violazione, tenendo presente che il Team crisi, in caso di dubbio deve assumere un atteggiamento prudenziale a difesa dei diritti dell'interessato.

In caso di esito positivo procede con l'analisi del rischio.

L'esito della valutazione di pertinenza della segnalazione, incluse tutte le informazioni e le decisioni prese dal team di crisi, devono essere riportate, a cura del responsabile privacy nell'apposita sezione della piattaforma TESI GDPR per la gestione del data breach.

[3] Considerare che, nel caso di comunicazione da parte del sub responsabile (situazione più critica) l'azione si avvia entro 36 ore dalla sua rilevazione

8.3. Analisi del rischio

Nel valutare il rischio per le persone fisiche derivante da una violazione, il titolare del trattamento deve considerare le circostanze specifiche della violazione, inclusa la gravità dell'impatto potenziale e la probabilità che tale impatto si verifichi. Per tale attività si fa riferimento alle Linee guida sulla notifica delle violazioni dei dati personali del WP29 del 3 ottobre 2017 (emendate in data 6 febbraio 2018) ed al documento "Raccomandazioni per una metodologia di valutazione della gravità delle violazioni dei dati" elaborato dall'Agenzia Europea per la Sicurezza delle Reti e delle Informazioni (ENISA)" e alle recenti Linee Guida dell'European Data Protection Board (EDPB) 1/2021 "Esempi di notifica di violazione di dati personali" Adottate il 14 Dicembre 2021.

Il Team di crisi procede all'analisi del rischio ed alla sua documentazione compilando il modulo per la Gestione del Data Breach (TESI GDPR), tenendo conto nella valutazione del significato associato a:

- Riservatezza: stima del danno/impatto che la perdita di riservatezza riguardante l'asset comporterebbe per il business di ORAS/tutela interessato (1-4);
- Integrità: stima del danno/impatto che la perdita di integrità riguardante l'asset comporterebbe per il business di ORAS/tutela interessato (1-4);
- Disponibilità: stima del danno/impatto che la perdita di disponibilità riguardante l'asset comporterebbe per il business di ORAS/tutela interessato (1-4).

Per effettuare una valutazione della stima della perdita di Riservatezza, Integrità e Disponibilità che tenga conto sia del danno per l'organizzazione che dell'impatto sugli interessati, viene utilizzata la seguente tabella (fonte www.cesaregallotti.it).

Tabella 3 (Gallotti)

Liv	R- Riservatezza	I - Integrità	D- Disponibilità
1 – Basso	**Organizzazione** I dati non presentano particolari requisiti di riservatezza. I dati sono pubblici.	**Organizzazione** I dati non presentano particolari requisiti di integrità. I dati gestiti non fanno parte di transazioni economiche, finanziarie o sanitarie.	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente non comporta multe o penali rilevanti.
	Interessati La mancanza di riservatezza ha impatti lievi (p.e. fastidio) sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici;	**Interessati** La mancanza di integrità ha impatti lievi (p.e. fastidio) sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici;	**Interessati** La mancanza di disponibilità ha impatti lievi (p.e. fastidio) sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici;

	- stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	- stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	- stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.
2 - Medio	**Organizzazione** I dati devono essere riservati per ragioni di business (concorrenza sleale, danni all'immagine), ma un'eventuale loro diffusione non ha elevati impatti sul business dell'organizzazione, sul rispetto della normativa vigente o sull'immagine dell'organizzazione.	**Organizzazione** I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un'impresa. La mancanza di integrità dei dati non ha elevati impatti sulle attività operative o sul rispetto della normativa vigente.	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali non particolarmente rilevanti.
	Interessati La mancanza di riservatezza ha impatti, non critici (p.e. perdita di tempo, perdita limitata di serenità), sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Interessati** La mancanza di integrità ha impatti, non critici (p.e. perdita di tempo, perdita limitata di serenità), sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Interessati** La mancanza di disponibilità ha impatti, non critici (p.e. perdita di tempo, perdita limitata di serenità), sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.
3 - Alto	**Organizzazione** I dati devono essere riservati per ragioni di business (concorrenza sleale, danni all'immagine) e un'eventuale loro diffusione ha elevati impatti sul business dell'organizzazione, sul rispetto della normativa vigente o sull'immagine dell'organizzazione.	**Organizzazione** I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un'impresa. La mancanza di integrità dei dati ha elevati impatti sulle attività operative o sul rispetto della normativa vigente.	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali rilevanti.

3 - Alto	**Interessati** La mancanza di riservatezza ha elevato impatto sulla vita sociale (p.e. sconvolgendola) o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Interessati** La mancanza di integrità ha elevato impatto sulla vita sociale (p.e. sconvolgendola) o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Interessati** La mancanza di **disponibilità** ha elevato impatto sulla vita sociale (p.e. sconvolgendola) o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.
4 - Critico	**Organizzazione** La diffusione delle informazioni ha elevati impatti sul business dell'organizzazione o sul rispetto della normativa vigente o sull'immagine dell'organizzazione tali da compromettere la sostenibilità dell'organizzazione.	**Organizzazione** La mancanza di integrità delle informazioni ha elevati impatti sul business aziendale o sul rispetto della normativa vigente tali da compromettere la sostenibilità dell'organizzazione.	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali che mettono in pericolo la sostenibilità economica e di immagine o hanno impatti sulla sicurezza delle persone fisiche.
	Interessati La mancanza di riservatezza ha impatto sulla sopravvivenza degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Interessati** La mancanza di integrità ha impatto sulla sopravvivenza degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Interessati** La mancanza di disponibilità ha impatto sulla sopravvivenza degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.

8.3.1. Valutazione del livello di gravità

La valutazione del livello di gravità deve essere effettuata attraverso la compilazione del modulo per la Gestione del Data Breach (TESI GDPR) che utilizza la seguente formula:

Gravità della violazione (SE) = Contesto di trattamento (DPC) x facilità di identificazione *EI + circostanze della violazione (CB).*

Il risultato rientra in un intervallo di valori che corrisponde ad uno dei quattro livelli di gravità della violazione, tenendo conto dell'impatto sugli individui.

Tabella 4

Gravità di una violazione dei dati		
Valore del rischio		**Impatto sui soggetti interessati**
0 < 2	**Basso**	Gli individui non saranno interessati o potrebbero riscontrarne alcuni inconvenienti, che supereranno senza alcun problema (tempo speso reinserire informazioni, fastidi, irritazioni, ecc.).
2 < 3	**Medio**	Gli individui possono incontrare notevoli inconvenienti, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, negazione di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici irrilevanti, ecc.).
3 < 4	**Alto**	Gli individui possono andare incontro a conseguenze significative, che dovrebbero riuscire a superare seppur con serie difficoltà (appropriazione indebita di fondi, blacklist delle banche, danni materiali, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
≥ 4	**Molto alto**	Gli individui possono incontrare significativi, o addirittura irreversibili, conseguenze, che non possono superare (disagio finanziario come debito sostanziale o incapacità di lavorare, psicologici a lungo termine o malattie fisiche, morte, ecc.).

8.4. Esito della analisi del rischio e decisioni

Il risultato del calcolo del rischio (gravità) deve essere interpretato come di seguito esposto (vedi tabella 5), considerando che, in base ai criteri assegnati il valore minimo è minore di 2 ed il massimo è uguale o maggiore di 4.

Tabella 5

Gravità della violazione e decisioni			
Casistica	**Valore del rischio**		**Misure**
A	**0 < 2**	**Basso**	• Nessuna notifica • Eventuali azioni correttive

B	**2 < 3**	**Medio**	• Notifica all'Autorità Garante • Nessuna comunicazione agli interessati • Eventuali azioni correttive
C	**3 < 4**	**Alto**	• Notifica all'Autorità garante • Comunicazione agli interessati • Gestione dell'evento • Eventuali azioni correttive
D	**≥ 4**	**Molto alto**	

Nel caso in cui il valore anche di uno solo tra **riservatezza, integrità e disponibilità** sia uguale o superiore a 2 il team crisi deve valutare se le misure corrispondenti siano adeguate.

I risultati dell'esito della analisi del rischio vanno riportati nel MODULO Gestione del Data Breach al massimo entro 4 ore[4], dall'inizio della riunione del Team crisi. Dell'esito della decisione si informa il Titolare del trattamento.

Tutte le informazioni riguardanti l'evento, riportate sul sopracitato modulo del sistema software, e l'esito della valutazione effettuata confluiscono nel registro degli incidenti.

8.5. Azioni a seguito delle decisioni

Sulla base della casistica in cui si ricade, debbono essere svolte le seguenti azioni:

- **CASO A** - si verifica e completa la compilazione della valutazione del rischio (MODULO Gestione del Data Breach); l'evento si chiude; non vengono effettuate ulteriori comunicazioni.
- **CASO B** - si aggiorna il MODULO Gestione del Data Breach; si procede con le eventuali azioni correttive (AC); si comunica internamente al Responsabile dell'area interessata dall'evento l'adozione del trattamento dell'evento (vedi paragrafo 8.7)
- **CASO C** - si aggiorna il MODULO Gestione del Data Breach; si procede all'adozione di trattamento dell'evento (vedi paragrafo 8.7), con le azioni correttive (AC); si comunica internamente Responsabile dell'area interessata dall'evento; si NOTIFICA all'autorità di controllo (vedi paragrafo 8.9.1). Il Titolare del trattamento, responsabile della comunicazione aziendale, coadiuvato dal RPD prepara un comunicato stampa. Il Titolare del trattamento comunica all'Organo amministrativo di ORAS
- **CASO D** – implica, oltre a quanto previsto dal caso C anche la comunicazione obbligatoria agli interessati coinvolti preparata a cura del Il Titolare del trattamento, responsabile della comunicazione aziendale, coadiuvato dal RPD. Il Titolare del trattamento comunica all'Organo amministrativo di ORAS spa

[4] Considerare che, nel caso di comunicazione da parte del sub responsabile o contitolare (situazione più critica) l'azione si conclude entro 52 ore dalla sua rilevazione

Le comunicazioni (notifica e comunicazione obbligatorie agli interessati) per i casi C e D debbono avvenire massimo entro 8 ore[5] dalla decisione presa.

Per le comunicazioni agli interessati ed al Garante vedi paragrafo.8.9

Il trattamento dell'evento senza l'avvio di azioni correttive (AC) deve essere considerata una situazione eccezionale: di norma contenere semplicemente la violazione e continuare con lo *status quo*, non è accettabile.

8.6. Indicizzazione sui motori di ricerca

Nel caso in cui il data breach abbia riguardato la pubblicazione di dati in rete (ad esempio pubblicazione on line di pagine per errore), deve essere verificato, sui i principali motori di ricerca che le pagine contenenti tali dati non siano stati indicizzati e, nel caso in cui fosse avvenuto, richiedere, ai motori di ricerca. la rimozione (diritto all'oblio). Tale indagine deve essere fatta sia appena a monte del data breach sia ripetuta a distanza di una settimana, due settimane ed un mese dall'evento.

8.7. Trattamento dell'evento

Quando è previsto un trattamento dell'evento, ovvero una o più azioni volte a minimizzare gli impatti per gli interessati e ripristinare la situazione precedente all'evento (laddove possibile) il Team crisi definisce: modalità, responsabilità e tempi. Il Team tiene sotto controllo lo stato di avanzamento delle azioni di trattamento previste e tiene aggiornato il MODULO Gestione del Data Breach (prevedendo l'inserimento della data di completamento del trattamento). Tra le azioni di trattamento da tenere sotto controllo anche quelle eventualmente imputabili al Responsabile esterno del trattamento.

Per il trattamento di eventi che riguardano la sicurezza dei sistemi informatici (tenere in considerazione i documenti ENISA - Agenzia dell'Unione Europea per la Cybersicurezza e le Linee guida sulla notifica delle violazioni dei dati personali 1/2021del EDPB.

8.8. Azione correttiva

Quando sono previste una o più azioni correttive volte a rimuovere la causa dell'evento, il Team crisi definisce: modalità, responsabilità e tempi. Il Team tiene sotto controllo lo stato di avanzamento delle azioni e l'efficacia delle stesse. Viene valutata la necessità di aggiornare l'analisi dei rischi ed eventualmente la DPIA se prevista per i trattamenti coinvolti e la documentazione (es. procedure di riferimento nomina a responsabile esterno del trattamento), Il Team crisi tiene aggiornato il modulo Gestione del Data Breach (prevedendo l'inserimento della data di completamento della/e Azione/i correttiva/e). Tra le azioni di correttive da tenere sotto controllo anche quelle eventualmente imputabili al Responsabile esterno del trattamento.

[5] Considerare che, nel caso di comunicazione da parte del subresponsabie (situazione più critica) l'azione si conclude entro 60 ore dalla sua rilevazione

8.9. Notifica al Garante e comunicazione agli interessati

A seguito di un evento di Data Breach deve essere effettuata la comunicazione al Garante (art. 33 co1) «…*a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà fondamentali degli interessati*» e, nel caso in cui il rischio è alto, anche agli interessati. La comunicazione è coordinata dal Team Crisi. Le evidenze di tutte le comunicazioni debbono essere conservate.

8.9.1. Notifica al Garante

La notifica deve essere fatta utilizzando la procedura telematica adottata dall'Autorità garante con il provvedimento n. 209 del 27 maggio 2021. Sul sito istituzionale al seguente link https://servizi.gpdp.it/databreach/s/ sono presenti tutte le informazioni per l'utilizzo della modalità telematica per la notifica delle violazioni dei dati personali (in allegato alla presente procedura il fac- simile del modello di notifica).

La procedura prevede la possibilità di allegare nelle diverse sezioni documenti che contengono ulteriori informazioni. In ogni caso è importante allegare l'analisi del rischio e l'eventuale comunicazione inviata agli interessati.

8.9.2. Comunicazioni al Garante per evento imputabile al Responsabile del trattamento

La notifica all'Autorità di controllo è sempre a carico del Titolare del trattamento anche nel caso in cui la responsabilità del Data Breach fosse attribuibile al Responsabile esterno. Deve essere valutato, di concerto con il Responsabile del trattamento la comunicazione al Garante nel caso in cui la violazione abbia interessato più Titolari che fanno ricorso ai servizi di uno stesso Responsabile del trattamento che ha originato il Data Breach.

8.9.3. Comunicazione agli interessati

La comunicazione agli interessati può avvenire con modalità diverse tra cui:

- comunicazione diretta agli interessati (mailing list, posta elettronica, sms, news alert)
- comunicato stampa
- comunicazione tramite sito WEB/social media

La comunicazione deve essere congruente con quanto indicato nella modalità di comunicazione di Data Breach pubblicata sul sito aziendale (vedi paragrafo 7.2).

Il Team crisi decide la strategia di comunicazione da mettere in atto, sia durante l'evento di Data Breach ed anche successivamente quando l'evento è stato risolto.

Di seguito le linee guida da considerare per la redazione delle comunicazioni verso gli interessati

Aspetti generali:

- definire il tono della comunicazione che può essere più informale (comunicato) o più formale (dichiarazione ufficiale)
- fornire un titolo "giornalistico" che per quanto possibile rassicuri gli interessati o perlomeno riduca il livello di allarme, utilizzare parole chiave facilmente rintracciabili sui motori di ricerca qualora venissero ricercate informazioni sui motori di ricerca
- le comunicazioni potrebbero non riguardare solo il Data Breach (rilevazione) ma anche le informazioni sull'andamento dello stesso nel tempo
- assicurare forme di comunicazione oneste, concrete e trasparenti
- fare riferimento al Team crisi, il suo ruolo ed il suo impegno
- mettere in evidenza la storia, l'impegno della azienda nell'assicurare l'attenzione al tema, gli investimenti fatti, le misure applicate
- descrivere l'evento in modo facilmente comprensibile, quale impatto ha avuto sui dati (o quale impatto presumibile può avere – informazioni perse, violate, comunicate a terzi non autorizzati, diffuse, ecc), come lo si sta affrontando/è stato affrontato, specificare cosa l'azienda sta facendo concretamente per proteggere i dati degli interessati
- indicare come e quando è stato coinvolto il Garante della Protezione dei dati
- inserire un contatto diretto per contattare l'organizzazione
- considerare di attivare un numero verde per rispondere agli interessati

Aspetti specifici per il comunicato stampa/dichiarazione ufficiale:

- prevedere link alla pagina del sito web dove è reperibile ulteriore informazioni sul Data Breach ed anche lo stato dell'andamento dello stesso nel tempo

Aspetti specifici per la comunicazione tramite sito WEB/social media:

- nel caso di violazioni gravi valutare la possibilità di pubblicare un video di scuse/spiegazioni coinvolgendo il cda e/o, prevedendo il coinvolgimento di un esperto in tale ambito per evitare errori o creare più allarme del necessario.
- considerare di attivare una APP dedicata all'evento

La modalità di invio della comunicazione ed i riferimenti degli interessati coinvolti deve essere documentata nel MODULO per la gestione del Data Breach (TESI GDPR)

Comunicazione diretta agli interessati

La comunicazione agli interessati deve contenere almeno i seguenti elementi:

Mittente:ORAS spa

Destinatario: [Nome e indirizzo dell'interessato colpito]

Introduzione: In data [gg/mm/aaaa] abbiamo riscontrato una violazione dei suoi dati personali.

Come conseguenza della sopra menzionata violazione, i suoi dati personali potrebbero essere stati:

- Divulgati

- Distrutti
- Persi
- Modificati
- È stato eseguito l'accesso
- Altro [specificare]

da persone non autorizzate.

La informiamo che la violazione dei dati personali potrebbe avere le seguenti conseguenze: [elencare]

Per affrontare la violazione dei dati sono state/saranno implementate le seguenti misure:

- ..
- …

Se avete quesiti in merito alla violazione dei dati, potete contattare [nome] via mail all'indirizzo […@....], o via posta all'indirizzo [indirizzo fisico].

Comunicazione indiretta agli interessati

La comunicazione indiretta agli interessati può avvenire tramite:

- comunicato stampa/dichiarazione ufficiale
- sito WEB/social media
- comunicazione delle precedenti modalità

Di seguito esempio di comunicazione (Fonte Materiale didattico Il Sole 24 ore Business School)

Comunicato stampa

AAA, una APP per la pianificazione della pubblicazione di messaggi sui social media, è stata hackerata nell'ottobre del 20xx ma l'azienda è riuscita a gestire in modo esemplare la situazione perché ha tempestivamente avvertito direttamente i clienti prima che la notizia andasse sui media.

Il livello di sincerità, proattività e commitment nella comunicazione via mail ai clienti ha determinato un effetto di fedeltà e fiducia presso i clienti salvando l'azienda da una pericolosa perdita di reputazione. L'azienda non ha avuto paura di rivelare il Data Breach e ha strategicamente gestito la crisi per informare direttamente ed in modo costante i clienti. Hanno espresso vero rammarico e preso la situazione con grande serietà. La prima cosa che ha fatto l'azienda immediatamente dopo il Data Breach è stata quello di mandare una mail, direttamente dal CEO e Fondatore BBB, che si è scusato in modo sincero ed ha rassicurato gli interessati dichiarando l'impegno di tutta l'azienda 24/7 per gestire la situazione.

Comunicazione agli interessati

Siamo spiacenti di comunicarvi di aver accertato in data….che abbiamo subito una violazione dei dati personali che la riguardano. L'accaduto si è verificato in data….nonostante tutte le misure di

sicurezza adeguate poste in essere a seguito della nostra analisi dei rischi. La informiamo che il nostro Team di crisi dedicato, come da procedura, sta procedendo agli interventi conseguenti e necessari al fine di porvi rimedio Vi suggeriamo di ….(es non aprire le e-mail inviate dal seguente indirizzo…., non aprire i link, etc) Vi chiediamo di ….(es controllare i vs account, etc). Stiamo pubblicando continui aggiornamenti sul nostro sito che potrà verificare al seguente link….

Vi rassicuriamo che in nessun modo i vs dati… (ex dati sensibili, etc) sono stati oggetto del presente attacco. Stiamo lavorando ininterrottamente per risolvere quanto prima questo spiacevole evento. Per ogni ulteriori chiarimento, restiamo a vostra completa disposizione potendoci contattare al seguente indirizzo e mail….

Nome referente e il team AAA.

8.10. Comunicazione all'Organo amministrativo

A seguito di un evento che ricade nei casi C (rischio medio) e D (rischio alto/critico), ed in ogni caso qualora il Titolare del trattamento lo ritenesse opportuno, deve essere tenuto aggiornato il consiglio di amministrazione di ORAS. Tale attività è a cura del Titolare del trattamento e deve avvenire con modalità, per quanto possibili tracciabili.

8.11. Polizza assicurativa

Il Titolare deve valutare l'opportunità di sottoscrivere preventivamente una polizza assicurativa che copra i danni da responsabilità civile per eventi riconducibili a violazioni di dati personali.

8.12. Situazioni anomale o di emergenza

In caso di segnalazioni in situazioni anomale o di emergenza, quali:

- mancanza di figure apicali del Team crisi
- mancanza di collegamenti (es. internet)/energia/situazioni di emergenza dovute a cause di forza maggiore/eventi naturali/pandemia)

Devono essere considerate le seguenti misure:

- Per ogni membro/ o per una parte dei membri è individuato un sostituto e deve essere pianificato l'allontanamento dall'ufficio in modo alternato eventuale coinvolgimento del Titolare nel Team crisi e/o di rappresentanti della società
- Le riunioni del Team possono essere effettuate anche tramite strumenti digitali che consentano il collegamento da luoghi diversi dalla sede di ORAS
- Nel caso in cui vi sia l'indisponibilità del server o altri eventi che possono non garantire il presidio dei sistemi deve essere prevista una comunicazione nella sezione Data Breach del sito internet
- Condividere i numeri di telefono e creare una chat dedicata tra i membri del Team crisi.

9. AZIONI SUCCESSIVE

9.1. Attività proattiva a cura del Team Crisi

Il team crisi potrebbe prevedere delle attività proattive: annunci, audit, analisi dei dati sviluppo della sicurezza di applicazioni web (*penetretion* test), servizi di rilevamento di intrusioni, simulazioni di eventi, divulgazioni di informazioni relative alla sicurezza; istruzione e formazione. Se si valutasse di aggiungere tale attività sarebbe opportuno inserire nella presente procedura un rimando ad una procedura da predisporre "ad hoc" descrivendo nella stessa anche le mansioni delle funzioni coinvolte in tale attività.

9.2. Relazione annuale all'Organi di Governo

Nell'ambito della rendicontazione delle attività svolta dal RPD (o dal Titolare del trattamento) all'Organo di Governo di ORAS, un paragrafo è dedicato al tema del Data Breach. Nello specifico sono comunicati:

- una sintesi degli eventi occorsi nel corso dell'anno e delle azioni messe in atto (NC e AC)
- eventuali rilevanti modifiche alla presente procedura
- risultati degli audit sulla applicazione della presente procedura
- risultati dell'analisi dei dati
- eventuali impatti emersi dall'analisi dei rischi a seguito di eventi di Data Breach
- altre informazioni utile che si ritiene condividere con l'Organo di Governo

10. ALLEGATI

Fac-simile del modello di notifica di una violazione di dati personali all'Autorità Garante per la Protezione dei Dati Personali

11. ARCHIVIAZIONE DEI DOCUMENTI

Il registro delle violazioni in ORAS è un report prodotto digitalmente dal modulo per la gestione del data breach (tesi GDPR). Tutta la documentazione riguardante la gestione delle violazioni su supporto cartaceo viene conservata in doppia copia presso la Direzione generale e l'ufficio privacy e banche dati a disposizione di eventuali visite ispettive dell'Autorità Garante per la protezione dei dati personali

12. STORIA DELLE MODIFICHE

Revisione	Data di emissione	Esito
00	Novembre 2018	Prima emissione
01	Marzo 2021	Revisione del paragrafo 3 e cambio codifica
02	Gennaio 2022	Revisione complessiva