SOMMARIO

IL DOCUMENTO È STATO COMPLETAMENTE REVISIONATO

IL DOCUMENTO E' STATO APPROVATO CON PARERE FAVOREVOLE DAL DATA PROTECTION OFFICER (DPO) DELL'AZIENDA

STATO	DATA	FIRMA
Verificato		Dott.ssa Lucia Bortoluzzi
Approvato	04.04.2019	Dott.ssa Antonella Messori
Approvato	04.04.2019	Dott.ssa Federica Filippini
Approvato	04.04.2019	Ing. Luca Capitani
Data di applicazione: 02.05.2019		

1.0 GRUPPO DI REDAZIONE

Il presente documento nella prima versione, è stato redatto dal gruppo di lavoro composto da: F. Filippini (Ufficio Privacy), L. Capitani, E. Scanavini, M. Barani (Servizio ICT), P. Lambertini (Ingegneria clinica), L. Vigne, R. Baroni (Controllo di gestione). Gli aggiornamenti e le revisioni periodiche sono di responsabilità del Responsabile Privacy e del Responsabile ICT, cosi come sono il punto di riferimento per l'invio dei report di comunicazione interna di un data breach da prte del personale.
Il documento è stato condiviso e validato anche da F. Banorri Data Protection Officer (DPO) dell'Azienda al fine di garantire la coerenza con quanto definito nell'ambito dell'AVEC.

2.0 DOCUMENTI DI RIFERIMENTO

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 24 ottobre 2014 Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonchè dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese (GU Serie Generale n.285 del 09-12-2014)

IOA29 Istruzione Operativa Aziendale - Regolamento aziendale attuativo delle disposizioni in materia di protezione dei dati personali

3.0 DEFINIZIONI

Autorizzato al trattamento: la persona fisica, espressamente designata, che opera sotto l'autorità del titolare del trattamento, con specifici compiti e funzioni connessi al trattamento dei dati personali (art. 4, punto 10).
Coordinatore del GAP: il Dirigente aziendale deputato a coordinare le attività, gli adempimenti organizzativi e procedurali derivanti dalle nuove disposizioni normative in materia di protezione dei dati personali
Data Protection Officer: la persona fisica individuata come Responsabile della protezione dei dati personali ai sensi del GDPR (in particolare artt. 37, 38, 39).
Gruppo Aziendale Privacy (GAP): il gruppo di professionisti individuato dal Titolare con il compito di presidiare a livello aziendale gli adempimenti organizzativi e procedurali derivanti dalle nuove disposizioni normative in materia di protezione dei dati personali

Referente privacy: la persona fisica che, secondo l'organizzazione aziendale, ricopre un ruolo gestionale e di responsabilità all'interno dell'azienda sanitaria che determina specifiche modalità organizzative rispetto ad uno o più trattamenti.
Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (art. 4, punto 8).
Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4, punto 7). In questo contesto, sono titolari del trattamento le Aziende Sanitarie afferenti ad AVEN.
Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, punto 2).

4.0 CONTENUTO

Il documento descrive il percorso aziendale per la **notifica di violazione dei dati personali** all'autorità di controllo (art. 33 GDPR) e **comunicazione della violazione dei dati personali** all'interessato (art. 34 GDPR), nonché i casi non oggetto di notifica all'Autorità di controllo, ma comunque annotati nel Registro delle Violazioni.

4.1 IL 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, è 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, 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.

4.2 PERCORSO DI NOTIFICAZIONE DI UN DATA BREACH

In caso di accertamento di violazione che rientra nella definizione di Data Breach, gli step del percorso di notificazione da seguire sono i seguenti:

1. Acquisizione della notizia da parte dei soggetti preposti al ricevimento/raccolta della violazione (di seguito indicati) che provvederanno ad attivare i passi successivi
2. Analisi tecnica dell'evento
3. Contenimento del danno
4. Valutazione della gravità dell'evento
5. Notifica al Garante Privacy

6. Altre segnalazioni dovute
7. Comunicazione agli interessati, dove necessario
8. Inserimento dell'evento nel Registro delle Violazioni
9. Azioni correttive specifiche e per analogia

4.3 GESTIONE OPERATIVA del DATA BREACH DA PARTE DEL TITOLARE DEL TRATTAMENTO

Ogni operatore aziendale autorizzato a trattare dati (personale autorizzato), qualora venga a conoscenza di un potenziale caso di data breach, anche tramite segnalazioni esterne dei cittadini, deve avvisare tempestivamente il referente privacy della struttura a cui afferisce. Quest'ultimo, valutato l'evento, se confermate le valutazioni di potenziale data breach, lo segnala tempestivamente al Responsabile Privacy/Coordinatore del GAP. A tal fine può essere utilizzato il report di comunicazione interna/notifica di un data breach (R01/IOA98) inviandolo per mail a: federica.filippini@aosp.bo.it; luca.capitani@aosp.bo.it; ufficio.privacy@aosp.bo.it.; mauro.barani@aosp.bo.it. Se è il referente privacy a venire direttamente a conoscenza del potenziale caso di data breach la procedura di comunicazione da seguire è la medesima.

Il Responsabile Privacy/Coordinatore del GAP, effettua una prima valutazione dell'evento, avvalendosi dei componenti del Gruppo Aziendale Privacy competenti alla trattazione del caso specifico e di eventuali altre professionalità necessarie per la corretta analisi del caso e comunica l'esito dell'analisi preliminare effettuata al DPO, al fine di avvalersi della sua consulenza.

Il Responsabile Privacy/Coordinatore del GAP, completata l'istruttoria avverte il titolare del trattamento comunicandogli l'esito della valutazione eseguita dal GAP in collaborazione con il DPO al fine di metterlo a conoscenza del potenziale caso di data breach.

Il titolare assume le proprie determinazioni, disponendo la necessità o meno di notifica.
Il Responsabile Privacy/Coordinatore del GAP predispone l'eventuale comunicazione all'Autorità Garante da sottoporre al DPO e al titolare del trattamento. Il titolare, per il tramite del Responsabile Privacy/ Coordinatore del GAP, trasmette la comunicazione all'Autorità Garante, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il titolare abbia un ragionevole grado di certezza della verifica di un incidente di sicurezza che riguardi dati personali.
Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.

E' comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi).

L'avvenuta notificazione al Garante viene documentata dal Responsabile Privacy/Coordinatore del GAP nel Registro delle violazioni (R02/IOA98) dallo stesso curato e tenuto. Tale registro ha durata annuale e contiene tutte le segnalazioni ricevute e gestite durante l'anno ed entro il 31 dicembre deve essere chiuso. Entro il 31 gennaio dell'anno successivo il Responsabile Privacy/Coordinatore del GAP provvede ad inviarlo al titolare del trattamento ed al DPO con nota protocollata, ai fini della conservazione ai sensi di legge.

Si precisa che anche i casi non ritenuti dal Titolare da notificare e le motivazioni sottese devono essere documentate nel medesimo registro.

4.4 GESTIONE OPERATIVA del DATA BREACH DA PARTE DEL RESPONSABILE DEL TRATTAMENTO

Ogni qualvolta l'azienda si trovi ad affidare il trattamento di dati ad un soggetto terzo/responsabile del trattamento, è tenuta a stipulare con tale soggetto uno specifico contratto che lo vincoli al rispetto delle istruzioni impartitegli dal titolare in materia di protezione dati.

A tal fine è necessario che la presente procedura di segnalazione di data breach sia resa nota a tutti i Responsabili del trattamento con l'obiettivo fornirgli le istruzioni per informare il titolare del trattamento senza ingiustificato ritardo, di ogni potenziale evento di data breach.
Pertanto il Responsabile del trattamento, qualora venga a conoscenza di un potenziale caso di data breach, deve avvisare, senza ingiustificato ritardo, e nel rispetto dei tempi previsti nell'atto di nomina, il DPO all'indirizzo pec protocollo@pec.ausl.bologna.it o tramite raccomandata A/R all'indirizzo Via castiglione, 29 – 40124- Bologna utilizzando il report per la segnalazione di un sospetto caso di data breach (R03/IOA98 per responsabile esterno).
Il DPO inoltra la notifica di data breach al Responsabile Privacy/Coordinatore del Gruppo Aziendale Privacy (federica.filippini@aosp.bo.it; ufficio.privacy@aosp.bo.it) e a luca.capitani@aosp.bo.it;.; mauro.barani@aosp.bo.it; da questo momento vengono eseguiti i medesimi steps della procedura illustrata al punto 4.2 (attraverso la necessaria collaborazione del Responsabile del trattamento).

4.5 ANALISI TECNICA DELL'EVENTO E VALUTAZIONE DELLA GRAVITÀ DELL'EVENTO

Il Gruppo Aziendale Privacy identificato come competente in relazione alla tipologia della violazione da analizzare, sotto la supervisione del Responsabile Privacy/Coordinatore del GAP, è responsabile dell'analisi tecnica dell'evento, delle azioni da mettere in atto tempestivamente per il contenimento del danno, avvalendosi della funzione consulenziale del DPO.
In particolare, una volta verificato che l'evento segnalato si configuri effettivamente come un "Data Breach" (Analisi Preliminare), verranno svolte tutte le operazione necessarie a raccogliere gli elementi per una valutazione dell'evento (Analisi Approfondita) ai fini della notifica al Garante della Privacy. Si sottolinea inoltre che anche nel caso in cui dall'Analisi Preliminare emerga che la segnalazione non abbia i caratteri del Data Breach, è necessario registrarla nel Registro delle Violazioni.
Durante l'Analisi Approfondita, dovranno essere accertate le circostanze della violazione, le conseguenze e i relativi rimedi.
Si precisa che l'art. 33 paragrafo n. 4 del DGPR recita "Qualora nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo". Pertanto, sarà fondamentale raccogliere il maggior numero di informazioni e, anche in caso queste non siano per il momento ritenute esaustive, effettuare la notificazione, c.d. notifica per fasi.
Nello specifico verrà effettuato:
- il riconoscimento della categoria della violazione (se di riservatezza, di integrità o di disponibilità) o altro evento (cfr Linee Guida sulla notifica delle Violazioni dei dati personali ai sensi del Regolamento UE 2016/79 WP 250 Par. 1 . punto 2)
- l'identificazione dei dati violati/distrutti/compromessi e relativi trattamenti;
- l'identificazione degli interessati;
-il contenimento del danno come di seguito descritto:
    - limitazione degli effetti dell'incidente,
    - raccolta delle prove forensi nel caso sia ipotizzato un reato,
    - determinazione delle azioni possibili di ripristino,
    - valutazione delle eventuali vulnerabilità collegate con l'incidente,
    - individuazione delle azioni di mitigazione delle vulnerabilità individuate,
    - valutazione dei tempi di ripristino,
    - gestione della comunicazione con gli interessati, i media (se di impatto notevole),
    - ripristino dei dati, dei sistemi, dell'infrastruttura e delle configurazioni,
    - verifica dei sistemi recuperati.

L'art. 33 paragrafo n. 1 chiarisce che non vi è obbligo di notifica della violazione quando è "improbabile" che questa comporti un rischio per i diritti e le libertà delle persone fisiche, ovviamente il giudizio che determina l'improbabilità del rischio deve essere riportato nel Registro delle Violazioni.
A questo proposito, i Garanti europei nelle loro linee guida, precisano che la mancata comunicazione può essere sanzionata, ma che nessuna sanzione è prevista nel caso di comunicazione incompleta o di comunicazione non necessaria.
Nella fase di Valutazione, sulla base delle informazioni acquisite, occorre innanzitutto stabilire se nell'incidente sono coinvolti i dati personali. In caso di risposta positiva occorre valutare l'impatto sugli

interessati. Se si tratta di una violazione di riservatezza occorre verificare che le misure di sicurezza (es.: cifratura dei dati) in vigore rendano improbabile l'identificazione degli interessati (non compromissione della chiave, algoritmo di cifratura o impronta senza vulnerabilità note). In caso di perdita di integrità o disponibilità di dati occorre valutare se è possibile il recupero degli stessi in tempi compatibili con i diritti degli interessati. Se in tale modo i rischi per gli interessati sono trascurabili, la procedura può terminare, dopo aver documentato il processo e le scelte operate: le misure messe in atto sono state adeguate alla minaccia. Se la valutazione invece sii conclude con evidenza di un caso si data breach si deve procedere con la notifica all'Autorità Garante.

4.6 NOTIFICA ALL'AUTORITA' GARANTE

La notifica, effettuata dal Titolare, sulla falsariga del modello reso disponibile dal Garante della privacy (Allegato 1 Modello di notifica all'Autorità Garante) dovrà contenere i seguenti elementi:

1. la descrizione della violazione dei dati personali compresi, ove possibile le categorie e il numero approssimativo di interessati in questione nonché le categorie ed il numero approssimativo di registrazioni dei dati personali in questione;
2. l'indicazione del nome ed i relativi dati di contatto del DPO;
3. la descrizione delle probabili conseguenze della violazione;
4. l'indicazione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e che, se del caso, per attenuare i possibili effetti negativi;

Nello specifico, la notifica al Garante sarà effettuata dal Titolare tramite PEC e per conoscenza al DPO, con indicazione del DPO come punto di contatto con il Garante.

4.7 ALTRE SEGNALAZIONI DOVUTE

Il Responsabile Privacy/Coordinatore del Gruppo Aziendale Privacy e il DPO, con il supporto dei componenti del Gruppo Aziendale Privacy, sulla base delle rispettive competenze, dovrà verificare la necessità di informare altri organi, consultandosi con gli Uffici aziendale competenti quali:

- CERT-PA (in caso di incidenti informatici ai sensi della Circolare Agid n. 2/2017 del 18.04.2017);
- Organi di Polizia (in caso di violazioni di dati conseguenza di comportamenti illeciti o fraudolenti);
- CNAIPC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche).
- Gestore di Identità Digitale e ad Agid nel caso in cui si individui un uso anomalo di un'identità SPID (Sistema Pubblico di Identità Digitale).

All'esito delle valutazioni sarà cura del titolare o suo delegato procedere con le segnalazioni dovute.

4.8 COMUNICAZIONE AGLI INTERESSATI

In caso di elevato rischio per la libertà e i diritti degli individui, si provvederà ad informare gli interessati sul fatto avvenuto, sui dati violati e sulle procedure necessarie a ridurre il rischio.
La comunicazione agli interessati, secondo quanto previsto dal paragrafo n. 3 dell'art. 34 del GDPR, non è richiesta quando:
- il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- la comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece ad una comunicazione pubblica o a una misurazione simile, tramite la quale gli interessati sono informati con analoga efficacia.

La comunicazione deve contenere, ai sensi dell'art.34 paragrafo 2 del GDPR, le seguenti informazioni:

- la natura della violazione;
- il nome e i dati di contatto del DPO o di altro punto di contatto;
- la descrizione delle probabili conseguenze nonché delle 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.

Pertanto a valle della decisione di notificare l'Autorità Garante, il Responsabile Privacy/Coordinatore del Gruppo Aziendale Privacy e il DPO devono valutare se sia il caso di notificare anche gli interessati. A tale scopo va valutata la gravità del rischio per gli interessati e i loro diritti.
Se il rischio è grave occorre individuare, la fattibilità di contattarli singolarmente oppure la necessità di procedere con pubblicazioni su diversi mezzi di comunicazione (sito web, quotidiani, radio, tv), le misure di contenimento che gli stessi interessati possano mettere in atto per minimizzare i rischi e le forme di comunicazione più comprensibili per gli interessati (mezzi, lingue, linguaggio) come indicato nelle Linee guida elaborate dal Gruppo Art. 29 in materia di trasparenza (WP 260), definite in base alle previsioni del Regolamento (UE) 2016/679.

La forma di comunicazione prescelta dal Titolare verrà predisposta e curata dal DPO con la collaborazione del Responsabile Privacy/Coordinatore del Gruppo Aziendale Privacy.

4.9 INSERIMENTO DELL'EVENTO NEL REGISTRO DELLE VIOLAZIONI

L'art. 33 paragrafo n. 5 del GPR, prescrive al Titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'Autorità di controllo di verificare il rispetto della norma.
Pertanto, il Responsabile Privacy/Coordinatore del Gruppo Aziendale Privacy per conto del titolare, è responsabile della tenuta del registro delle violazioni (R02/IOA98), che devono essere documentate, tracciabili e in grado di fornire evidenza nelle sedi competenti.

4.10 MIGLIORAMENTO

Dalla gestione di un data breach scaturiscono una serie di azioni di seguito riportate utili al miglioramento del processo:

- ✓ Analisi della relazione dettagliata sull'incidente
- ✓ Reiterazione del processo di gestione del rischio informativo
- ✓ Eventuale revisione di questo documento (se necessaria) e di eventuali altri documenti collegati (es. Analisi del rischio, Misure di sicurezza)
- ✓ Individuazione di controlli che diminuiscano la probabilità dell'incidente o i relativi impatti sul sistema colpito e su sistemi analoghi
- ✓ Revisione del Sistema di Gestione della Privacy
- ✓ Revisione delle relazioni con Clienti e Fornitori
- ✓ Riesame annuale e eventuale revisione annuale della procedura di gestione del data breach

5.0 ALLEGATI E MODULI UTILIZZABILI

- ✓ R01/IOA98 Comunicazione data breach al responsabile privacy/coordinatore del GAP
- ✓ R02/IOA98 Registro di violazione dei dati
- ✓ R03/IOA98 Comunicazione data breach da parte del Responsabile esterno (ad uso esclusivo dell'Ufficio Privacy)
- ✓ Allegato 1 Modello di comunicazione all'Autorità Garante in caso di violazione di dati personali