
	Gestione di una violazione di dati personali (DATA BREACH)	IOdgenT003_ORG
		Pag. 1 a 8

Sommario

1. SCOPO	2
2. CAMPO DI APPLICAZIONE	2
3. RIFERIMENTI NORMATIVI E DOCUMENTALI.....	2
4. DEFINIZIONI, TERMINOLOGIA	3
5. PROCESSO/MODALITA' OPERATIVE.....	4
5.1 Premessa.....	4
5.2 Gestione del <i>data breach</i>	5
5.2.1 Gestione del <i>data breach</i> all'interno della Struttura.....	5
5.2.2 Notifica all'Autorità Garante per la protezione dei dati personali	6
5.2.3 Gestione del <i>data breach</i> esterno alla Struttura.....	7
5.3 Comunicazione agli interessati	7
5.4 Registro delle violazioni	8
5.5 Azioni correttive e di miglioramento	8
6. ELENCO ALLEGATI	8

Rev	Data	Redazione	Verifica	Approvazione	Descrizione
00	07.10.19	Dott.ssa Emanuela Raho Dott.ssa Federica Pierleoni Avv. Alessandra Cesarotti Dott.ssa Paola D'Eugenio Dr. Nicola Nardella Ing. Mauro Luciani Dott.ssa Donatella Giovannini	Dr. E. Berselli RAQ	Dr.ssa Maria Capalbo Direttore Generale	Prima stesura VALIDITA' 2019-2020
01	15.11.2021	Dott.ssa Emanuela Raho Dott.ssa Federica Pierleoni Avv. Alessandra Cesarotti Dott.ssa Paola D'Eugenio Dr.ssa Cristiana Cattò Ing. Mauro Luciani Dott.ssa Donatella Giovannini	Dr. E. Berselli RAQ	Dr.ssa Maria Capalbo Direttore Generale	Revisione dei seguenti paragrafi: paragrafo 3 paragrafo 4 VALIDITA' NOVEMBRE 2023
02	13.03.2024	Dott.ssa Federica Pierleoni RPD	Dr. E. Berselli RAQ	Dr.ssa Nadia Storti Direttore Generale Dott. Matteo Biraschi Direttore Amministrativo	Revisione di tutti i paragrafi per evoluzione del quadro normativo di riferimento e mutato assetto organizzativo aziendale VALIDITA' MARZO 2026

	Gestione di una violazione di dati personali (DATA BREACH)	IOdgenT003_ORG
		Pag. 2 a 8

1. SCOPO

La presente Istruzione ha la finalità di indicare a tutto il personale operante presso l'Azienda Sanitaria Territoriale Pesaro Urbino (di seguito denominata "AST") la modalità di gestione di un *data breach* - ovvero di un evento di violazione dei dati personali - nel rispetto dei principi e delle disposizioni contenute nel Regolamento (UE) 2016/679 sulla protezione dei dati (di seguito denominato "GDPR") e nei successivi provvedimenti attuativi.

Nell'ambito dell'istruzione vengono esplicitate le regole per garantire la realizzabilità tecnica e la sostenibilità organizzativa della gestione del *data breach*, con particolare riferimento ai seguenti aspetti:


- Modalità e profili di segnalazione al Titolare del trattamento per il tramite del Responsabile della protezione dei dati
- Valutazione dell'evento verificatosi
- Modalità e profili di segnalazione all'Autorità Garante
- Eventuale comunicazione agli interessati.

2. CAMPO DI APPLICAZIONE

In presenza di possibile violazione di dati personali – siano essi contenuti in banche informatiche o cartacee – l'Istruzione si applica a tutti i soggetti che, a vario titolo, svolgono attività nell'ambito delle diverse articolazioni organizzative dell'AST.

3. RIFERIMENTI NORMATIVI E DOCUMENTALI

- 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)";
- 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)";
- "Linee Guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679" del Gruppo di lavoro art. 29 del 3 ottobre 2017, emendate e adottate il 6 febbraio 2018;

	Gestione di una violazione di dati personali (DATA BREACH)	IOdgenT003_ORG
		Pag. 3 a 8

- “Provvedimento del Garante per la protezione dei dati personali del 27 maggio 2021 – Procedura telematica per la notifica di violazioni di dati personali (data breach)” del Garante per la protezione dei dati personali;
- “Linee guida EDPB 01/2021 su esempi riguardanti la notifica di violazione dei dati” adottate il 14 dicembre 2021;
- “Linee guida EDPB 09/2022 in materia di notifica delle violazioni di dati personali (data breach)” adottate il 28 marzo 2023.

4. DEFINIZIONI, TERMINOLOGIA

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile (“interessato”); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all’ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4, n. 1 del GDPR).


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, n. 2 del GDPR).

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia digitalizzato o meno, centralizzato, decentralizzato o ripartito in modo funzionale o geografico (art. 4, n. 6 del GDPR).

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, n. 7 del GDPR).

Titolare del trattamento è l’Azienda Sanitaria Pesaro Urbino nella persona fisica del Direttore Generale, in qualità di legale rappresentante *pro-tempore*.

Responsabile della protezione dei dati (RPD): la persona fisica nominata dal Titolare del trattamento con nota prot. AST-PUMN 7426 dell’08.02.2023, ai sensi degli artt. 37-39 del GDPR.

	Gestione di una violazione di dati personali (DATA BREACH)	IODgenT003_ORG
		Pag. 4 a 8

"Designato" al trattamento dei dati personali: la persona fisica che nell'ambito dell'organizzazione aziendale – in ragione dell'incarico di responsabilità conferito all'interno dell'AST – svolge compiti e funzioni di vigilanza sul rispetto e attuazione delle istruzioni privacy da parte del personale autorizzato al trattamento di dati personali in servizio presso la struttura rispettivamente diretta; ciò secondo le specifiche istruzioni ricevute dal Titolare.

i "Designati" al trattamento dei dati personali sono i Direttori di Struttura Complessa (ovvero i sostituti ex art. 22 del CCNL Area Sanità 2016 – 2018 del 19.12.2019), i Responsabili di Struttura Semplice Dipartimentale ed il Responsabile del Servizio di Prevenzione e Protezione (SPP).

Autorizzato al trattamento dei dati personali: tutte le unità di personale operanti presso le diverse Strutture/Servizi dell'AST che, ai sensi dell'art. 29 del GDPR, effettuano attività di trattamento di dati personali sotto la vigilanza del "Designato" al trattamento e ai quali sono state fornite istruzioni in tal senso.

Responsabile del trattamento dei dati: 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, n. 8 del GDPR). Trattasi, al riguardo, di soggetto esterno all'AST appositamente nominato mediante atto predisposto in conformità all'art. 28 del GDPR.

Interessato: la persona fisica, identificata o identificabile, alla quale i dati si riferiscono.

Violazione dei dati personali (data breach): 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 (art. 4, n. 12 del GDPR).


5. PROCESSO/MODALITA' OPERATIVE

5.1 Premessa

Una violazione dei dati personali (*data breach*) può - se non gestita in modo adeguato e tempestivo - provocare danni fisici, materiali o immateriali alle persone fisiche (interessati), quali, a titolo esemplificativo, perdita di controllo dei dati personali che le riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione di 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 rilevante per la persona fisica interessata.

Le Linee guida in materia di notifica delle violazioni di dati personali ai sensi del Regolamento (UE) 2016/679" del Gruppo di lavoro art. 29 del 3 ottobre 2017, emendate e adottate il 6 febbraio 2018, classificano le violazioni in base ai seguenti principi della sicurezza delle informazioni:

- "violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;

	Gestione di una violazione di dati personali (DATA BREACH)	IOdgenT003_ORG
		Pag. 5 a 8

- “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 dei dati personali.

5.2 Gestione del *data breach*

In caso di accertamento di una violazione che rientri nella fattispecie di *data breach*, occorre osservare le seguenti fasi del processo che verranno esplicitate con maggior dettaglio nei successivi paragrafi:

- Acquisizione notizia della violazione da parte del soggetto interno/esterno all’Azienda
- Comunicazione della notizia di violazione al Responsabile della protezione dei dati (RPD)
- Individuazione e attivazione – a cura del RPD – dei professionisti aziendali tecnicamente competenti per materia nella valutazione della gravità dell’evento e nella relativa gestione
- Eventuale notifica della violazione al Garante per la protezione dei dati personali
- Eventuale comunicazione agli Interessati
- Inserimento dell’evento nel Registro delle violazioni
- Azioni correttive e di miglioramento.

5.2.1 Gestione del *data breach* all’interno della Struttura


Ogni operatore/professionista aziendale autorizzato a trattare dati personali, qualora venga a conoscenza di un potenziale caso di *data breach*, avvisa tempestivamente il “Designato” al trattamento della Struttura aziendale a cui il medesimo afferisce (Direttore/Responsabile di UOC, Responsabile di UOSD e Responsabile del SPP).

Il “Designato” al trattamento - valutato l’evento - se ritiene confermata la segnalazione di potenziale data breach, ne fornisce comunicazione al RPD a mezzo e-mail utilizzando, a tal fine, l’allegato modulo (MOD01_IOdgenT003_ORG).

Il RPD – in base alla tipologia della violazione e tenuto conto dello specifico ambito – attiva le seguenti professionalità aziendali competenti per materia ai fini della corretta e puntuale gestione del data breach, quali a titolo non esaustivo:

- Servizi Informatici
- Ingegneria Clinica
- Direzioni Mediche dei Presidi
- Distretti Sanitari
- Direttori/Responsabili di struttura coinvolti nell’evento.

I professionisti in tal senso individuati dal RPD – sotto il coordinamento di quest’ultimo – devono attivarsi con immediatezza procedendo ad una approfondita analisi tecnica dell’evento ed al compimento di ogni azione necessaria al contenimento del danno.

	Gestione di una violazione di dati personali (DATA BREACH)	IOdgenT003_ORG
		Pag. 6 a 8

Contestualmente, il RPD fornisce comunicazione al Titolare sull'evento oltreché dei nominativi delle professionalità individuate per la relativa gestione.

Durante l'analisi tecnica dovranno essere accertate le circostanze della violazione, le conseguenze ed individuati i più appropriati rimedi.

Nello specifico dovrà essere effettuato in un tempo consigliabile non superiore alle 8/10 ore:

- Il riconoscimento della categoria della violazione (se di riservatezza, di integrità o di disponibilità)
- L'identificazione dei dati violati/distrutti/compromessi e relativi trattamenti;
- L'identificazione dei soggetti interessati;
- Il contenimento del danno come di seguito indicato:
 - Limitazione degli effetti dell'incidente
 - Raccolta delle prove forensi nel caso sia ipotizzato un reato
 - Determinazione delle possibili azioni 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 esterna
 - Ripristino dei dati, dei sistemi, dell'infrastruttura e delle configurazioni
 - Verifica dei sistemi recuperati.

Tutte le operazioni/attività effettuate devono essere documentate e tracciate.

5.2.2 Notifica all'Autorità Garante per la protezione dei dati personali


A seguito delle determinazioni sul punto raggiunte e solo qualora si debba ritenere probabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche interessate, ai sensi dell'art. 33 del GDPR, il RPD – con lo specifico contributo delle professionalità coinvolte - supporta il Titolare del trattamento nella predisposizione della notifica all'Autorità Garante.

Detta notificazione deve essere inviata senza ingiustificato ritardo e, ove possibile, entro 72 ore da intendersi decorrenti dal momento in cui il Titolare sia venuto a conoscenza della violazione di dati, ovvero da quanto il Titolare abbia raggiunto un ragionevole grado di certezza sul fatto che l'incidente di sicurezza comporti una violazione di 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 di ulteriori indagini e verifiche sull'evento.

La notifica all'Autorità Garante deve essere inviata tramite apposita procedura telematica, resa disponibile nel portale dei servizi *on line* dell'Autorità medesima, osservando le dettagliate istruzioni ivi fornite per la corretta compilazione della notifica stessa.

	Gestione di una violazione di dati personali (DATA BREACH)	IOdgenT003_ORG
		Pag. 7 a 8

Diversamente, non vi è obbligo di notifica della violazione quando è “improbabile” che la stessa comporti un rischio per i diritti e le libertà dei soggetti interessati. In tale caso, il giudizio che determina l’improbabilità del rischio deve essere annotato nel Registro delle violazioni di cui al successivo paragrafo 5.4 della presente Istruzione Operativa.

5.2.3 Gestione del *data breach* esterno alla Struttura

Ogni Responsabile del trattamento (Fornitore/Ditta) – incaricato dal Titolare ad effettuare attività di trattamento dati per suo conto sulla base di specifico contratto a tal fine stipulato tra le parti ex art. 28 del GDPR – qualora venga a conoscenza di un potenziale caso di *data breach*, ne dà avviso senza ingiustificato ritardo all’AST, inviando alla stessa una comunicazione a mezzo PEC all’indirizzo ast.pesarourbino901@emarche.it utilizzando, a tal fine, l’allegato modulo (MOD02_IOdgenT003_ORG) che dovrà, pertanto, essere accluso all’atto di nomina stesso.

Per ingiustificato ritardo è da considerarsi – di norma - la notizia pervenuta al Titolare del trattamento oltre le 48 ore dalla presa di conoscenza iniziale da parte dello stesso Responsabile.

Il RPD – destinatario del predetto modulo di segnalazione congiuntamente al Titolare – attiva il medesimo iter di gestione dell’evento illustrato ai precedenti paragrafi 5.2.1 e 5.2.2.

5.3 Comunicazione agli interessati


Nel caso in cui dal *data breach* possa derivare un rischio elevato per i diritti e le libertà delle persone fisiche interessate, queste ultime devono essere informate senza ingiustificato ritardo al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali pregiudizi derivanti dalla violazione.

La comunicazione agli interessati – conformemente al paragrafo 3 dell’art. 34 del GDPR – non è dovuta 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 misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

In sede di valutazione – da parte dei medesimi professionisti di cui al paragrafo 5.2.1 – se effettuare o meno la notifica dell’evento all’Autorità Garante, verrà altresì valutata anche la necessità di procedere con la comunicazione agli interessati. A tale scopo andrà considerata la gravità del rischio per i diritti e le libertà degli interessati stessi.

Se il rischio è grave occorre individuare:

	Gestione di una violazione di dati personali (DATA BREACH)	IOdgenT003_ORG
		Pag. 8 a 8

- la fattibilità di contattarli singolarmente oppure la necessità di procedere con pubblicazioni su diversi mezzi di comunicazione (es. sito web, quotidiani, radio, tv);
- le misure di contenimento che gli stessi interessati possono mettere in atto per minimizzare i rischi;
- le forme di comunicazione più comprensibili per gli interessati (mezzi, lingue, linguaggio).

La comunicazione dovrà descrivere con linguaggio semplice e chiaro la natura della violazione dei dati personali, le probabili conseguenze derivanti dalla stessa, oltreché le relative misure individuate per porvi rimedio, indicando, altresì, il nome e i dati di contatto del RPD o di altro punto di contatto all'uopo individuato presso cui ottenere maggiori informazioni.

Il RPD supporta il Titolare del trattamento nella predisposizione della comunicazione all'interessato/agli interessati da inviarsi secondo la modalità ed i tempi ritenuti più opportuni, anche avvalendosi del supporto/collaborazione dell'Ufficio Relazioni con il Pubblico.

Delle predette fasi deve essere prodotta e conservata apposita documentazione comprovante le scelte effettuate.

5.4 Registro delle violazioni

Presso l'Ufficio del Responsabile della protezione dei dati è istituito il Registro delle violazioni nell'ambito del quale vengono documentati tutti gli eventi di *data breach* occorsi presso l'AST e il cui aggiornamento avviene a cura del Responsabile della Protezione dei dati per conto del Titolare. A tal fine si allega alla presente Istruzione Operativa relativo modello del predetto registro (MOD03_IOdgenT003_ORG).

5.5 Azioni correttive e di miglioramento

Quando si verifica una violazione di dati personali, le professionalità aziendali coinvolte nella gestione del data breach - come individuate al paragrafo 5.2.1 della presente Istruzione Operativa - devono altresì definire e mettere in campo tutte le misure necessarie a prevenire, in termini di riduzione del rischio, il verificarsi o ripetersi di future violazioni, di cui deve essere prodotta idonea documentazione.

Il RPD, entro il termine di 30 giorni, svolge attività di vigilanza in ordine all'attuazione del predetto obbligo.

6. ELENCO ALLEGATI

ALLEGATO N°	DESCRIZIONE ALLEGATO
MOD01_IOdgenT003_ORG	Modulo per la segnalazione di un sospetto caso di <i>data breach</i>
MOD02_IOdgenT003_ORG	Modulo per la segnalazione di un sospetto caso di <i>data breach</i> da parte di Responsabile del trattamento nominato ai sensi dell'art. 28 del GDPR (Fornitore/Ditta)
MOD03_IOdgenT003_ORG	Registro delle violazioni