Violazione di dati personali
(c.d. *Data Breach*)

Revisione	Data	Causale
0	06/04/2021	Redazione

Fasi	Funzioni	Nome e Cognome	Firma	Data
Redazione	Coordinatore personale e attività amministrative a supporto dei percorsi sanitari e Adempimenti Privacy	Dr.ssa Claudia Chesi		26/4/2021
Verifica	Responsabile Protezione dati AOUS	Dr.ssa Nicoletta Minutella		
	Direttore Amministrativo	Dr.ssa Maria Silvia Mancini		29/4/2021
	Direttore Sanitario	Dr. Roberto Gusinu		03/05/2021
Approvazione	Direttore Generale	Prof. Antonio Davide Barretta		03/05/2021
Emissione	Responsabile UOSA Accreditamento e Qualità dei Percorsi Assistenziali	Dr.ssa Anna Grasso		

Luogo di archiviazione e conservazione del documento in originale:
Segreteria UOC Igiene e Epidemiologia

La diffusione del seguente documento è assicurata mediante la pubblicazione sulla intranet aziendale e sul sito web istituzionale dell'AOUS alla sezione "Tutela della riservatezza e dei dati personali"

Essa inoltre sarà distribuita mediante lettera di diffusione a:

- Direzione Generale
- Direzione Amministrativa
- Direttori di UO
- Responsabili di Dipartimento
- Direzione Sanitaria
- Direttori di Dipartimento
- Responsabili di UOP
- Coordinatori

Validità doc fino a:	Prole chiave		
06/04/2024	A.DG.PA.16	Dati personali	*Data Breach*

La UOSA Accreditamento e Qualità ha provveduto per il presente documento, ad effettuare:

- la revisione editoriale;
- la convalida e l'attribuzione della codifica;
- l'emissione e la diffusione con definizione della lista di distribuzione.

INDICE

Allegati:

- Allegato 1: Registro delle violazioni dati personali.

INTRODUZIONE

La presente procedura si applica alla violazione dei dati personali consistente in una violazione di sicurezza (data-breach) che comporta accidentalmente o in modo illecito la distruzione, la perdita la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati **dall'Azienda Ospedaliero – Universitaria Senese (di seguito "AOUS") in qualità di Titolare del trattamento come definito dall'art. 4 punto 7) del RGPD**

La procedura definisce linee di comportamento da seguire, adottate da AOUS, e indica ruoli, responsabilità, tempistiche e modalità di comunicazione di eventuali violazioni di riservatezza, d'integrità e disponibilità dei dati personali all'Autorità di Controllo e, ove necessario, a tutti gli Interessati i cui dati personali sono oggetto di violazione.

Per la omessa notifica di Data Breach all'Autorità di Controllo o per l'omessa comunicazione agli interessati o per entrambi gli adempimenti, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 del RGPD, sono previste, rilevanti sanzioni amministrative , il cui importo può arrivare fino ad euro 10.000.000 o al 2% del fatturato totale annuo dell'esercizio precedente, se superiore, in caso di imprese, nonché misure correttive di cui all'art. 58 del RGPD (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati).

1. SCOPO

La finalità è fornire precisa istruzione operative in presenza di un incidente di sicurezza che determina una violazione dei dati personali per assicurare il rispetto dei principi e delle prescrizioni del Regolamento UE 2016/679, in particolare degli artt. 33 "Notifica di una violazione dei dati personali all'autorità di controllo" e 34 "Comunicazione di una violazione dei dati personali all'interessato".

2. CAMPO DI APPLICAZIONE/DESTINATARI

La presente procedura interna è obbligatoria per tutti i soggetti:

- **Preposti** al trattamento dei dati personali **(**Individuati con la delibera n. 1008/2018): sono delegati ai sensi dell'art. 2 quaterdecies del D.lgs. n.196/2003 e ss.mm.ii. per l'adempimento di specifici compiti e funzioni connessi al trattamento di dati personali che operano sotto l'autorità del Titolare, ovvero, Direttore di Unità Operativa Complessa, Direttore di Unità Operativa Semplice Autonoma, Responsabili di Unità Operativa Semplice, titolari di incarico di Responsabile UOP, e ogni altro Responsabile individuato ai sensi dello stesso articolo con atto aziendale;
- **Incaricati** al trattamento dei dati personali: lavoratori dipendenti, collaboratori e terzi non dipendenti che trattano dati personali per lo svolgimento della propria attività lavorativa presso l'AOUS nel rispetto delle istruzioni operative e del profilo di autorizzazione consentito;
- **Responsabili** del trattamento ex art. 28 del RGPD: soggetti esterni (persona fisica o giuridica l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto dell'AOUS Titolare del trattamento. Gli obblighi del Responsabile del trattamento verso il Titolare relativi alle segnalazioni di violazione dati personali sono specificati nell'atto giuridico stipulato ai sensi dell'art.28 del RGPD.

La mancata conformità alle regole di comportamento previste dalla presente procedura può configurare illecito disciplinare e determinare provvedimenti disciplinari a carico dei dipendenti inadempienti.

3. ABBREVIAZIONI E DEFINIZIONI

Categorie particolari di dati personali (art.9 RGPD)	I dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Codice	D.lgs. 30 giugno 2003, n.196 "Codice in materia di protezione dei dati personali" e s.m.i.
Data Beach	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.
Garante	Autorità Garante per la protezione dei dati personali.
Incaricati del trattamento	Lavoratori dipendenti e terzi non dipendenti che trattano dati personali nel corso della propria attività lavorativa presso l'AOUS nel rispetto delle istruzioni operative e del profilo di autorizzazione consentito.
Interessato	La persona fisica identificata o identificabile (Art. 4, n. 1, RGPD) a cui si riferisce il dato personale oggetto di trattamento.
Pseudonimizzazione	Trattamento dei dati personali tale che i dati personali non possono essere più attribuiti a un interessato specifico senza l'ausilio di informazioni aggiuntive, che sono conservate separatamente e soggette a misure tecniche e organizzative che ne garantiscano la confidenzialità.
Preposti	Soggetti espressamente designati dal Titolare, ai sensi dell'art 2-quaterdecies del Codice, per l'adempimento di specifici compiti e funzioni connessi al trattamento di dati personali che operano sotto l'autorità del Titolare, allo scopo di coordinare e che sovrintendono trattamenti di dati personali effettuati da personale autorizzato nelle attività di rispettiva competenza.
Responsabile del trattamento (Art. 4, n. 8, RGPD)	Persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratta i dati per conto del titolare del trattamento.
Responsabile della Protezione dei Dati (RPD)	La persona fisica (o giuridica) nominata ai sensi dell'art. 37 del RGPD, che svolge i compiti previsti i dall'art. 39 del RGPD o di altre disposizioni ivi contenute.
RGPD	Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, "Regolamento Generale sulla Protezione dei dati".
Titolare	Persona fisica o giuridica, autorità pubblica, servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o a 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, la distruzione.

4. MODALITÀ OPERATIVE

4.1. Comitato di Valutazione del Data Breach

Ai fini della gestione tempestiva di qualsiasi violazione di dati personali, è istituito un Comitato di Valutazione del Data Breach composto dalle seguenti funzioni:

- Responsabile della Protezione dei dati ("RPD");
- Referente aziendale Privacy;
- Direttore/Preposto della struttura presso cui è avvenuta il Data Breach;
- Referente Estar supporto informatico o suo delegato (qualora si tratti di Data Breach informatico);
- Dirigente sanitario individuato dal Direttore Sanitario;
- Direttore Amministrativo.

Nel caso in cui si verifichi un incidente di sicurezza che possa determinare un Data Breach, il Comitato di valutazione è convocato con urgenza dal Titolare con il supporto dell'RPD e del Referente aziendale Privacy che hanno la facoltà di convocare altri soggetti che il Titolare ritenga utile coinvolgere ai fini istruttori.

Il Comitato di Valutazione dovrà riunirsi, anche mediante teleconferenza o videoconferenza, entro 24 ore dalla convocazione, salvo, motivate situazioni eccezionali, per attivare tutte le necessarie azioni, raccogliere le informazioni e

valutare se ricorrono i presupposti per notificare il Data Breach al Garante e, se del caso, per effettuare la comunicazione agli interessati. Le attività di raccolta documentale ed informativa sono coordinate dal Referente Aziendale Privacy.
Le valutazioni effettuate dal Comitato di Valutazione dovranno essere comunicate tempestivamente al Titolare del trattamento per consentire di procedere all'eventuale notifica all'Autorità di Controllo e/o agli interessati nei termini di legge.

Registrazioni

Qualora nel capitolo delle "Modalità operative" sia fatto riferimento a moduli, a documenti o a registri utilizzati durante l'attività dell'Unità Operativa, è opportuno descrivere quali sono e dove vengono conservati.
Ciò al fine di consentire la rapida verifica dell'emissione di quanto previsto dal protocollo e di stabilire i documenti che devono essere archiviati e quelli che possono essere eliminati.

4.2. Attività connesse al Data Breach

Il personale autorizzato al trattamento, qualora venga a conoscenza, nell'espletamento delle attività di competenza o indirettamente nello svolgimento delle stesse, del verificarsi di eventuali violazioni dei dati personali o di incidenti informatici e non, che possano esporre a rischio di violazione dei dati (Data Breach), deve tempestivamente informare il Direttore / Preposto il quale informa il Titolare, senza ingiustificato ritardo, e comunque entro 24 ore da quando ne è venuto a conoscenza, formalizzando la comunicazione (anche con comunicazione per posta elettronica) al Responsabile per la protezione dei dati personali (di seguito RPD).

La comunicazione al Titolare del trattamento della violazione dei dati personali dovrà pervenire in forma scritta.

Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione all'Autorità di Controllo. La notifica dovrà avvenire ove possibile entro 72 ore e comunque senza ingiustificato ritardo, 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.

Anche l'eventuale Responsabile del trattamento designato dall'Azienda ospedaliero-universitaria Senese ai sensi dell'art. 28 del RGPD è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione. Al riguardo, i contratti o altri atti giuridici che disciplinano i trattamenti effettuati dal Responsabile per conto del dovranno prevedere uno specifico obbligo di tempestiva comunicazione del Data Breach all'AOUS quale titolare del trattamento.

Il Responsabile del trattamento e il Preposto al trattamento, qualora non procedano a comunicare al Titolare, con le modalità e la tempistica di cui alla presente procedura, la violazione di dati di cui siano venuti a conoscenza, si assumono ogni responsabilità in ordine alla sanzione o al danno che al Titolare possa derivare da tale omissione o ritardo.

I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD e del modello di notifica allegato al provvedimento del Garante n.157/2019, sono i seguenti:

- perdita del controllo dei dati personali;
- limitazione dei diritti;
- discriminazione;
- furto o usurpazione d'identità;
- frodi;
- perdite finanziarie, danno economico o sociale;
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari);
- conoscenza da parte di terzi non autorizzati;

- qualsiasi altro danno economico o sociale significativo.

Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

La notifica deve avere il contenuto minimo previsto dall'art. 33 RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33, lett. b), c) e d).

I dati personali sono trattati dall'AOUS, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo. In particolare, essi si distinguono nelle seguenti categorie:

- dati personali che permettono l'identificazione diretta come i dati anagrafici (ad esempio: nome e cognome) e l'identificazione indiretta, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP);
- dati rientranti in categorie particolari: si tratta dei "dati personali che rivelino l'origine razziale od etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale di una persona" secondo la definizione di cui all'art.9 RGPD;
- dati relativi a condanne penali e reati: si tratta dei dati c.d. "giudiziari", cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. L'art. 10 del RGPD ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Le fasi di attività connesse alla gestione di eventuali violazioni di riservatezza dei dati (Data Breach) si sostanziano in:

4.2.1 Rilevazione del Data Breach

4.2.2 Valutazione del rischio connesso alla violazione

4.2.3 Gestione del Data Breach

4.2.4 Notifica del Data Breach;

4.2.5 Comunicazione agli Interessati (ove necessario);

4.2.6 Registro delle violazioni e archivio della documentazione;

4.2.7 Pianificazione di Audit Interni.

4.2.1. Rilevazione del Data Breach

Come indicato in precedenza, per Data Breach si intende 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.

Il Garante per la protezione dei dati personali individua le violazioni sotto elencate, a seconda della natura della violazione.

- **PERDITA DI CONFIDENZIALITÁ (diffusione/accesso non autorizzato o accidentale)**

  Si verifica in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali, come ad esempio:

  - quando nella redazione di un atto non si redige la versione con omissione dei dati da non pubblicare e l'atto viene pubblicato nella sua interezza;
  - quando si inoltrano messaggi contenenti dati a soggetti non interessati o autorizzati al trattamento;
  - quando un operatore abbandona la propria postazione di lavoro senza prima prendere le opportune precauzioni (riporre la documentazione, lasciare attive procedure sulla risorsa informatica utilizzata, ecc..) e terze persone possono prendere visione di informazioni;
  - quando un soggetto in malafede comunica dei dati non pubblici a terzi in modo non autorizzato;

- **PERDITA DI INTEGRITÁ (modifica non autorizzata o accidentale)**

  Si verifica in caso di alterazione non autorizzata o accidentale dei dati personali.
  L' "alterazione" è la situazione in cui i dati sono danneggiati, corrotti o non più completi. L'alterazione non autorizzata può essere la conseguenza di un attacco esterno o di una manipolazione inconsapevole da parte di personale non competente. Un'alterazione accidentale si può verificare per errore umano (ad es. nel momento di un aggiornamento delle informazioni) o per un disguido tecnico quando all'interno di una base dati si perdono i collegamenti a determinate informazioni (integrità referenziale).

- **PERDITA DI DISPONIBILITÁ (impossibilità di accesso, perdita, distruzione non autorizzata o accidentale)**

  Si verifica in caso di perdita o distruzione dei dati personali (accidentale o non autorizzata).
  La "perdita di dati" è la situazione in cui i dati, presumibilmente, esistono ancora, ma il titolare ne ha perso il controllo o la possibilità di accedervi, mentre la "distruzione" dei dati personali è la condizione in cui i dati non esistono più o non esistono più in un formato che sia utilizzabile dal titolare.

  La violazione dei dati può avvenire a seguito di un attacco informatico, di un accesso abusivo, di un incidente (es. incendio, allagamento, etc.) o per la perdita di un supporto informatico (smartphone, notebook, chiavetta USB, etc.) o per la sottrazione di documenti con dati personali (furto, etc.).

  A seconda delle circostanze, una violazione può riguardare anche tutti gli aspetti sopra indicati o una combinazione di essi. La casistica è molto ampia.

Il Titolare del trattamento, avuta notizia dell'avvenuto Data Breach, con il supporto del RPD e del Referente aziendale privacy, convoca il Comitato di Valutazione del Data Breach che effettua l'istruttoria per l'identificazione e valutazione dell'evento.

4.2.2. Valutazione del rischio connesso alla violazione

Il livello di rischio è definito sulla base di due parametri, gravità e probabilità:

GRAVITA' Rilevanza degli effetti pregiudizievoli che la violazione è in grado di produrre sui diritti e le libertà delle persone coinvolte.	Impatto della violazione sui diritti e le libertà delle persone coinvolte. • Basso: nessun impatto. • Medio: impatto poco significativo, reversibile. • Alto: impatto significativo, irreversibile.
PROBABILITA' Grado di possibilità che si verifichino uno o più eventi temuti (es. la perdita di ogni traccia dei dati).	Possibilità che si verifichino uno o più eventi temuti. • Basso: l'evento temuto non si manifesta. • Medio: l'evento temuto potrebbe manifestarsi. • Alto: l'evento temuto si è manifestato.

Ai fini della identificazione dei valori da attribuire ai due parametri per la valutazione del rischio, occorre considerare anche i seguenti fattori:

- tipo di violazione;
- natura, sensibilità e volume dei dati personali;
- facilità di associare i dati violati ad una persona fisica;
- gravità delle conseguenze per gli interessati;
- particolarità degli interessati (es. minori);
- particolarità degli autorizzati al trattamento (es. personale sanitario);
- numero degli interessati esposti al rischio.

4.2.3. Gestione del Data Breach

Il Comitato di Valutazione del Data Breach raccoglie le informazioni necessarie alla descrizione dell'evento, all'analisi delle misure tecniche e organizzative analogiche e/o digitali adottate e di quelle di possibile adozione per porre rimedio alla violazione e/o per attenuarne i possibili effetti negativi. Le valutazioni del Comitato di Valutazione del Data Breach sono comunicate tempestivamente al Titolare del trattamento. All'esito di tale attività che deve compiersi tempestivamente, e comunque in modo da poter effettuare la notifica entro il termine di 72 ore dall'avvenuta conoscenza della violazione, come prescritto dalla normativa, il Comitato di Valutazione del Data Breach formula una proposta operativa corredata dalla documentazione di supporto prodotta dai Direttori / Preposti da sottoporre al Titolare.

Qualora il Titolare del trattamento dovesse ritenere che non ricorrono i presupposti per notificare il Data Breach all'Autorità di Controllo, è necessario che le motivazioni sottostanti a tale decisione siano documentate all'interno del Registro Interno delle Violazioni.

A tale proposito, occorrerà descrivere i motivi per cui il Titolare del trattamento ha ritenuto che la violazione non costituisse fattore di rischio per i diritti e le libertà degli individui.

Ai fini della gestione del Data Breach occorre considerare se:

- i dati siano stati in precedenza resi anonimi oppure pseudonimizzati;
- i dati siano stati oggetto di cifratura e se fosse garantita, al momento della violazione, la riservatezza della chiave di decifratura;
- i dati violati non siano riconducibili all'identità di persone fisiche;
- i dati siano già stati oggetto di pubblicazione;
- l'evento non costituisca un Data Breach.

4.2.4. Notifica del Data Breach

Ai sensi dell'art. 33 del RGPD, il Titolare ha sempre l'obbligo di notificare il Data Breach all'Autorità di Controllo, salvo i casi in cui sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Alla notificazione, effettuata dal Titolare del trattamento utilizzando il modello approvato dall'Autorità di controllo, dovranno essere allegati tutti gli elementi informativi e le valutazioni in merito effettuate.

Qualora il Titolare del trattamento e il RPD abbiano opinioni discordanti circa la sussistenza o meno del rischio per i diritti e le libertà degli interessati, la decisione in merito alla notifica della violazione dei dati personali all'Autorità di Controllo ricade unicamente sul Titolare del trattamento e deve essere debitamente motivata.

Laddove, invece, sia rilevato un rischio per i diritti e le libertà degli interessati, il Titolare del trattamento deve notificare la violazione all'Autorità di Controllo senza ingiustificato ritardo e, ove possibile, **entro 72 ore dal momento in cui ne sia venuto a conoscenza.** Il Titolare deve considerarsi venuto a conoscenza di una violazione quando sia in possesso di un ragionevole grado di certezza in merito alle modalità con cui la stessa si è verificata, ottenuto anche a seguito di un'indagine

approfondita (da parte del Comitato di valutazione). Il Titolare deve dunque ritenersi, prima della conclusione degli accertamenti, ancora privo di un grado di conoscenza sufficiente, e tale da determinare l'obbligo di notifica, per cui il termine da cui iniziano a decorrere le 72 ore deve individuarsi nel momento in cui il Titolare sia venuto in possesso di una ragionevole certezza su quanto accaduto. La fase di accertamento non può essere abusata per prorogare illegittimamente il termine di notifica.

Qualora la notifica al Garante per la Protezione dei dati personali non sia effettuata entro 72 ore, essa dovrà essere corredata dei motivi del ritardo.

Se non fosse possibile fornire tutte le informazioni contestualmente, queste ultime potranno essere inviate in fasi successive senza ulteriore ingiustificato ritardo, avendo cura di dare evidenza delle motivazioni per cui tali informazioni non sono disponibili.

In questo caso sarà cura del Titolare del trattamento raccogliere le informazioni mancanti e procedere, senza ritardo, alle integrazioni eventualmente necessarie avvalendosi della collaborazione delle funzioni interessate che, a tal fine, dovranno prestare pronta, piena e fattiva disponibilità.

La mancata collaborazione delle risorse coinvolte assume rilevanza a fini disciplinari.

Ai sensi dell'art. 33 del Regolamento, la notifica all'Autorità di Controllo deve contenere almeno i seguenti contenuti:

- descrizione della natura della violazione dei dati personali, compresi – ove possibile – le categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione 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.

La notifica viene in ogni caso effettuata utilizzando il vigente modello di notifica pubblicato nel sito web dell'Autorità Garante.

4.2.5. Comunicazione agli interessati

Nel caso in cui la violazione dei dati personali presenti un rischio elevato per i diritti e le libertà

delle persone fisiche, il Titolare del trattamento provvede alla comunicazione di detta violazione a tutti gli interessati coinvolti, senza ingiustificato ritardo, dandone comunicazione per conoscenza al RPD.

La comunicazione agli interessati deve descrivere, con un linguaggio semplice e chiaro, la natura della violazione dei dati personali e deve contenere almeno le seguenti informazioni:

- la descrizione delle probabili conseguenze della violazione dei dati personali;
- la descrizione 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;
- nome e dati di contatto del RPD.

Ai sensi dell'art. 34, comma 3, non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

- il Titolare del trattamento ritiene che la violazione di dati personali non presenti un rischio elevato per i diritti e le libertà delle persone fisiche;
- il Titolare del trattamento ha messo in atto 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 ad. es. 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;

- detta comunicazione richiederebbe sforzi sproporzionati; in tal caso, è necessario procedere a una comunicazione pubblica, ovvero a una misura simile alternativa, tramite la quale gli Interessati sono informati con analoga efficacia.

Nel caso in cui sia l'Autorità di Controllo a ordinare con provvedimento la comunicazione del Data Breach agli interessati, il Titolare del trattamento pone in essere tutte le attività necessarie per ottemperare al provvedimento.

4.2.6. Registro delle violazioni e archivio della documentazione

Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate all'Autorità di Controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio e registrare.

A tal fine, con il supporto del Responsabile della protezione dei dati (RPD), il Titolare registra nel Registro delle Violazioni (Allegato 1) qualsiasi tipologia di violazione e conserva con la massima cura e diligenza la documentazione a supporto, che può essere richiesta dall'Autorità di Controllo al fine di verificare il rispetto delle disposizioni del RGPD.

4.2.7. Pianificazione di audit

Il Titolare del trattamento prevede, all'interno del proprio piano di audit, con cadenza almeno annuale, una verifica delle segnalazioni di violazione dei Data Breach.

4.3. Matrice delle responsabilità

La tabella descrive le fasi di attività previste nella procedura e i soggetti che in ognuna delle diverse fasi intervengono come Responsabile di quella attività (R), come soggetto che collabora (C), come soggetto che deve essere informato al momento dell'esecuzione dell'attività (I):

Funzione / Attività	Titolare	Responsabile del trattamento (se ha subito il Data Breach)	Referente aziendale della privacy	Referente Estar supporto informatico (se presente)	Direttore di Struttura/ Preposto	RPD
• Rilevazione D.B.	**I**	**R**	**C**	**R**	**R**	**C**
• Valutazione D.B.	**I**	**R**	**C**	**R**	**R**	**C**
• Gestione D.B.	**I**	**C**	**R**	**C**	**C**	**C**
• Notifica D.B.	**R**	**I**	**C**	**C**	**I**	**R**
• Comunicazione agli interessati	**R**	**I**	**C**	**I**	**I**	**R**
• Applicazione delle misure correttiva	**R**	**R**	**I**	**C**	**C**	**I**
• Archivio documentazione: fascicolo di ogni violazione e registro Data Breach	**I**	**I**	**R**	**I**	**I**	**C**

4.4. Sanzioni

Chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento UE 2016/679 ha il diritto di ottenere il risarcimento del danno dal Titolare o dal Responsabile del trattamento, a meno che il Titolare o il Responsabile del trattamento dimostrino che l'evento dannoso non è loro in alcun modo imputabile.

Il Regolamento UE 2016/679 stabilisce che la violazione degli obblighi del Titolare e del Responsabile del trattamento è soggetta a sanzioni amministrative pecuniarie.

Per la omessa notifica di Data Breach all'Autorità di Controllo o per l'omessa comunicazione agli interessati o per entrambi gli adempimenti, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 del RGPD, sono previste, infatti, rilevanti sanzioni amministrative, il cui importo può arrivare fino ad euro 10.000.000 o al 2% del fatturato totale annuo dell'esercizio precedente, se superiore, in caso di imprese, nonché misure correttive di cui all'art. 58 del RGPD (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati).

È pertanto di fondamentale importanza rispettare la presente procedura organizzativa interna per la gestione di eventuali violazioni concrete, potenziali o sospette di dati personali, per adempiere agli obblighi imposti dalla normativa applicabile ed evitare rischi per i diritti e le libertà degli interessati, nonché danni economici per l'AOUS quale titolare del trattamento.

Nel caso in cui alla segnalazione del Data Breach consegua l'apertura di un procedimento da parte dell'Autorità Garante e che si concluda con una sanzione amministrativa, l'atto deliberativo con il quale si dispone il pagamento della sanzione all'Autorità Garante sarà inviato alla competente Procura Regionale della Corte dei Conti.

4.5. Norma finale

Per tutto quanto non espressamente previsto nella presente procedura, si rinvia alla vigente normativa.

La presente procedura è pubblicata nella sezione "Tutela della riservatezza e dei dati personali" del sito web istituzionale dell'Azienda.

La presente procedura sarà soggetta a modifiche e integrazioni che si renderanno necessarie in adeguamento a disposizioni normative intervenute successivamente all'approvazione della **procedura stessa o a pronunciamenti, linee guida e provvedimenti del Garante.**

5. RIFERIMENTI

- 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, RGPD, in particolare art.4, art.33, art.34, Considerando 85,86,87,88;
- D.Lgs. 30 giugno 2003, n.196 e s.m.i. "Codice in materia di 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. Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Provvedimento del Garante sulla notifica delle violazioni dei dati personali (Data Breach) 30 luglio 2019 n. 157;
- Linee guida 01/2021 sugli esempi riguardanti la notifica di violazione dei dati adottate da EDPB il 14 gennaio 2021 in consultazione pubblica;

Data ultimo aggiornamento ____/_____/_____

Cod.	**Data di accadimento della violazione dati personali**	**Natura della violazione** (1)	**Tipo di violazione** (2)	**Dispositivi interessati** (3)	**Dati personali interessati** (4)	**Effetti e conseguenze della violazione** (5)	**Misure tecniche e organizzative applicate** (6)	**Misure tecniche/ organizzative adottate per prevenire violazioni future**	**Livello di gravità della violazione**	**Motivazione di improbabilità di rischio per i diritti e le libertà degli interessati**

Modalità di compilazione

(1) Accidentale o illecita

(2)
- Lettura (presumibilmente i dati non sono stati copiati)
- Copia (i dati sono ancora presenti sui sistemi del Titolare
- Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- Cancellazione (i dati non sono più sui sistemi del Titolare e non sono in possesso dell'autore della violazione)
- Furto (i dati non sono più sui sistemi del Titolare e li ha l'autore della violazione)
- Altro_____

(3)
- Postazioni di lavoro
- Dispositivo di acquisizione o dispositivo-lettore
- Smart card o analogo supporto portatile
- File o parte di un file
- Strumento di back up
- Rete
- Altro_____-

(4)
- Dati anagrafici
- Numero di telefono
- Indirizzo di posta elettronica
- Dati di accesso e identificazione (username, password, altro)
- Dati personali (sesso, data di nascita, età, altro)
- Categorie particolari di dati personali art. 9 RGPD: dati ……..
- Dati relativi a condanne penali o reati art. 10 RGPD
- Dati sconosciuti
- Altro_____

(5)
- Discriminazioni
- Furto o usurpazione di identità
- Perdite finanziarie
- Pregiudizio alla reputazione
- Perdita di riservatezza dei dati personali protetti da segreto professionale
- Decifratura non autorizzata della pseudonimizzazione

(6)
- Pseudonimizzazione e cifratura dati personali
- Assicurazione su base permanente della riservatezza, dell'integrità, della disponibilità e della resilienza dei sistemi e dei servizi di trattamento
- Ripristino tempestivo della disponibilità e dell'accesso ai dati personali in caso di incidente fisico o tecnico
- Verifica e valutazione sistematica dell'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento
- Limitazione della quantità di dati acquisiti (principio di minimizzazione)
- Chiavi robuste di autenticazione
- Idonei controlli sugli accessi