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

Revisione	Data	Causale
0	06/04/2021	Redazione
1	12/06/2023	Revisione delle modalità di gestione del Data Breach

Fasi	Funzioni	Nome e Cognome	Firma	Data
Redazione	Direzione Amministrativa Coordinatrice Ufficio Privacy	Dr.ssa Claudia Chesi	….OMISSISS…..	06/07/2023
	Direzione Amministrativa Ufficio Privacy	Dr.ssa Francesca Todaro	….OMISSISS…..	06/07/2023
Verifica	Responsabile Protezione dati AOUS	Ditta Morolabs s.r.l. - Avv. Michele Centoscudi	….OMISSISS…..	04/07/2023
	Direttore Amministrativo	Dr.ssa Maria Silvia Mancini	….OMISSISS…..	11/07/2023
	Direttore Sanitario	Dr.ssa Maria De Marco	….OMISSISS…..	18/07/2023
Approvazione	Direttore Generale	Prof. Antonio Davide Barretta	….OMISSISS…..	--
Emissione	Responsabile UOSA Accreditamento e Qualità dei Percorsi Assistenziali	Dr.ssa Anna Grasso	….OMISSISS…..	06/07/2023

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 avviso agli utenti e lettera di diffusione a:

- Direzione Generale
- Direzione Sanitaria
- Direttori di UO (tecnico/sanitari ed amministrativi)
- Responsabili infermieristici e amministrativi di Dipartimento
- Lista Utenti
- Direzione Amministrativa
- Direttori di Dipartimento
- Responsabili di UOP
- Coordinatori sanitari, tecnico/sanitari e amministrativi

Validità doc fino a:	Parole chiave		
12/06/2026	A.DG.PA.17	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.

1. Sommario

ALLEGATI

Scheda delle violazioni dati personali	Allegato 1
Registro delle violazioni dati personali	Allegato 2
Scheda di sintesi della modalità operativa	Allegato 3

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.

1. SCOPO E CAMPO DI APPLICAZIONE

La finalità è fornire precise istruzioni operative al personale 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".

La presente procedura interna si applica a tutto il personale dell'AOUS, nonché a tutti i soggetti che a diverso titolo svolgono attività di trattamento di dati personali per la stessa. In particolare, è obbligatoria per i seguenti soggetti:

- i **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;
- gli **Incaricati** al trattamento dei dati personali, ovvero i 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.;
- i **Responsabili del trattamento** ai sensi dell'art. 28 RGPD.

Per le definizioni si rimanda all'articolo successivo.

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

2. DEFINIZIONI

Autorità di controllo	Autorità pubbliche indipendenti incaricate nei singoli Paesi UE di sorvegliare l'applicazione del GDPR al fine di tutelare i diritti e le libertà fondamentali degli interessati. In Italia, Garante per la protezione dei dati personali.
Autorizzati al trattamento	Chiunque, sia esso definito "preposto" o "incaricato", agisce sotto l'autorità del Titolare o del responsabile che abbia accesso e gestisca dati personali per le funzioni che gli competono.
Codice	D.lgs. 30 giugno 2003, n.196 "Codice in materia di protezione dei dati personali" e s.m.i.
Comitato di valutazione del data breach	Comitato composto dal Responsabile della Protezione dei dati (d'ora in poi anche "RPD"), dall'Ufficio privacy aziendale, dal Direttore/Preposto della struttura presso cui è avvenuta il Data Breach, dal Referente ESTAR supporto informatico o suo delegato e dal Responsabile dell'Ufficio Innovazione AOUS (qualora si tratti di Data Breach informatico) e da altri soggetti che per qualifica o per competenza sono informati o possono fornire un contributo per la gestione della violazione.

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.
Dato Personale Comune	Qualsiasi informazione riguardante una persona fisica(interessato), identificata o identificabile. 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 di caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Dati Personali Particolari	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, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona ai sensi dell'art. 9 RGPD.
Dati Giudiziari	Dati personali idonei a rivelare condanne penali, reati o connesse misure di sicurezza, oltre che i provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.
Incaricati al trattamento	Coloro che operano sotto l'autorità del Titolare e svolgono compiti di secondo livello in merito al trattamento dei dati personali.
Incidente di sicurezza	Un singolo o una serie di non voluti o inaspettati eventi di sicurezza che hanno un'alta probabilità di compromettere le attività dell'Organizzazione e di minacciare la sicurezza delle informazioni ed in particolare la loro riservatezza, integrità e disponibilità.
Interessato	Persona fisica identificata o identificabile (Art. 4, n. 1, RGPD) a cui si riferisce il dato personale oggetto di trattamento.
Linee Guida dell'ex WP29 (oggi "EDPB") sul data breach	Linee guida in materia di notifica di un data breach adottate dall'ex WP29 (oggi "European Data Protection Board" o "EDPB") il 3 Ottobre 2017, come riviste e adottate il 6 Febbraio 2018 ("*Guidelines on Personal data breach notification under Regulation 2016/679*" - WP250rev.01).
Linee-guida 01/2021	Linee-guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali.
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 al trattamento	Coloro che operano sotto l'autorità del Titolare e sono stati individuati da questi a svolgere specifici compiti e funzioni di primo livello connessi al trattamento di dati personali.
Provvedimento del Garante per la protezione dei dati personali	Provvedimento sulla notifica delle violazioni dei dati personali (data breach) adottato dal Garante italiano per la protezione dei dati personali il 30 luglio 2019.
Responsabile del trattamento (Art. 4, n. 8, RGPD)	Persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratta i dati 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.

Responsabile della Protezione dei Dati (RPD o DPO)	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 del Trattamento	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. Si precisa che nella presente procedura, il Titolare del trattamento, d'ora in poi ("Titolare") è rappresentato dal Legale Rappresentante.
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.
Ufficio Privacy Aziendale	Ufficio, afferente alla Direzione Amministrativa, individuato dal Titolare ed incaricato della gestione e del coordinamento di tutti gli aspetti legati alla protezione dei dati personali nel rispetto delle norme applicabili in materia.
Violazione di dati personali o "Data breach"	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.

3. VIOLAZIONE DEI DATI

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.

3.1. Rischi

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.

3.2. Tipologia di Violazione

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

- **PERDITA DI CONFIDENZIALITÀ (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; o 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 INTEGRITÀ (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 DISPONIBILITÀ (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.

3.3. Valutazione del Rischio Connesso alla Violazione

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

GRAVITA'	**Impatto della violazione sui diritti e le libertà delle persone coinvolte**.
Rilevanza degli effetti pregiudizievoli che la violazione è in grado di produrre sui diritti e le libertà delle persone coinvolte.	• Basso: nessun impatto. • Medio: impatto poco significativo, reversibile. • Alto: impatto significativo, irreversibile.
PROBABILITA'	**Possibilità che si verifichino uno o più eventi temuti.**
Grado di possibilità che si verifichino uno o più eventi temuti (es. la perdita di ogni traccia dei dati).	• 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 (gravità e probabilità) 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. GESTIONE VIOLAZIONE DI DATI (DATA BREACH)

L'AOUS individua le fasi di attività connesse alla gestione di eventuali violazioni di riservatezza dei dati (Data Breach) che possono essere suddivise in:

- Rilevazione del Data Breach e Comitato di Valutazione
- Analisi dell'incidente di sicurezza come Data Breach e gestione
- Notifica del Data Breach (ove necessario);
- Comunicazione agli Interessati (ove necessario);
- Registro delle violazioni e archivio della documentazione;
- Pianificazione di Audit Interni.

5. DESCRIZIONE DELL'ATTIVITÀ

5.1. Rilevazione del Data Breach e Comitato di Valutazione

Qualsiasi soggetto autorizzato al trattamento, qualora venga a conoscenza, nell'espletamento delle attività di competenza o indirettamente nello svolgimento delle stesse, del verificarsi un incidente di sicurezza che possa determinare una violazione di dati personali (Data Breach), deve tempestivamente, a mezzo e-mail e telefonicamente o di persona, informare il Direttore / Preposto il quale informa l'Ufficio privacy (e-mail ufficioprivacyaous@ao-siena.toscana.it – tel. 0577/585815) e l'RPD (e-mail privacy@ao-siena.toscana.it), senza ingiustificato ritardo, e comunque NON oltre le 24 ore da quando ne è venuto a conoscenza.

Dopodiché l'Ufficio privacy aziendale con il supporto dell'RPD convoca con urgenza il Comitato di valutazione e informa dell'accaduto anche il Titolare in forma scritta a mezzo e-mail. Il Comitato di Valutazione dovrà riunirsi, anche mediante teleconferenza o videoconferenza, entro 24 ore dalla convocazione, salvo, motivate situazioni eccezionali per attivare l'istruttoria volta all'identificazione e valutazione dell'evento.

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 (il Titolare trasmette immediatamente la segnalazione all'Ufficio privacy e all' RPD ai contatti sopra indicati). Al riguardo, i contratti o altri atti giuridici che disciplinano i trattamenti effettuati dal Responsabile per conto dell'AOUS dovranno prevedere uno specifico obbligo di tempestiva comunicazione del Data Breach all'AOUS quale titolare del trattamento.

Laddove la Violazione di dati personali sia posta in essere da un Responsabile ex art. 28 GDPR, il Titolare può richiedere ogni documentazione inerente la gestione della violazione stessa ed effettuare degli audit di verifica.

Il Responsabile del trattamento e il Preposto al trattamento, qualora non procedano a comunicare il Data Breach, 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.

5.2. Analisi e gestione dell'Incidente di Sicurezza come 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. Ciò consente di 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 dall'Ufficio privacy aziendale con il supporto dell'RPD ed, eventualmente, del Referente ESTAR e del Responsabile dell'Ufficio Innovazione AOUS, si occuperà di:

- prendere in carico l'incidente di sicurezza secondo le prassi aziendali per la gestione di incidenti nei diversi ambiti, tenendo adeguatamente traccia delle segnalazioni e delle modalità di gestione;
- acquisire gli elementi necessari per confermare o escludere che l'incidente di sicurezza costituisca una violazione di dati personali, tenuto conto che la stessa può riguardare, congiuntamente o disgiuntamente, la riservatezza, la disponibilità, l'integrità dei dati o la resilienza dei sistemi su cui sono conservati i dati;
- quando ha un ragionevole grado di certezza che l'incidente di sicurezza abbia coinvolto dati personali, qualificare l'incidente come "Violazione di dati personali";

All'esito di tale attività che deve compiersi tempestivamente, e comunque in modo da poter effettuare la notifica all'Autorità di Controllo 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.

Dunque, le situazioni che si possono presentare si racchiudono nelle seguenti ipotesi:

a) Un evento che si qualifica come "incidente di sicurezza" ovvero un evento che ha un'alta probabilità di compromettere le attività dell'Organizzazione ma non coinvolge dati personali. Lo stesso deve essere registrato secondo prassi aziendali anche in collaborazione con il Responsabile esterno;
b) La violazione dei dati personali non costituisce fattore di rischio per i diritti e le libertà delle persone fisiche, per cui ci si limita ad annotare l'evento nel Registro interno delle violazioni non essendo necessario effettuare alcuna notifica all'Autorità di Controllo;
c) La violazione presenta un fattore di rischio per i diritti e le libertà delle persone fisiche, per cui si deve procedere con la notifica all'Autorità di Controllo e con l'annotazione nel Registro;
d) La violazione presenta un rischio elevato per i diritti e le libertà degli interessati, per cui si deve procedere con la notifica anche con la comunicazione agli interessati coinvolti e con l'annotazione nel Registro.

Nel caso sub b), qualora si dovesse ritenere che non ricorrano 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 si è 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 non consentendo di risalire agevolmente all'interessato;
- 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 ovvero hanno scarse informazioni tali da poter essere ricondotte all'interessato;
- i dati siano già stati oggetto di pubblicazione ovvero già disponibili al pubblico in quanto facilmente acquisibili e/o consultabili attraverso fonti pubbliche;
- l'evento non costituisca un Data Breach.

Le valutazioni effettuate dal Comitato di Valutazione, rispetto ai casi sub b), c) e d), sono comunicate dall'RPD tempestivamente al Titolare per la validazione della proposta, il quale disporrà i successivi adempimenti ovvero l'eventuale notifica all'Autorità di Controllo e/o la comunicazione agli interessati nei termini di legge. In particolare, nel caso sub d), spetterà all'RPD trasmettere la comunicazione agli interessati coinvolti.

5.3. 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.

La notifica, effettuata dal Titolare del trattamento utilizzando il modello approvato dall'Autorità di controllo, dovrà contenere tutti gli elementi informativi e le valutazioni in merito effettuate.

Laddove, quindi, dalle valutazioni del Comitato di Valutazione del Data Breach, sia rilevato un rischio per i diritti e le libertà degli interessati, a seguito della relativa comunicazione dall'RPD al Titolare, spetta a quest'ultimo, con il supporto dell'Ufficio Privacy e del RPD, 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 dell'Ufficio Privacy aziendale con il supporto del RPD raccogliere le informazioni mancanti, in collaborazione con le funzioni interessate che, a tal fine, dovranno prestare pronta, piena e fattiva disponibilità, nonché a trasmetterle al Titolare per procedere alla trasmissione delle integrazioni all'Autorità.

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.

5.4. 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 per il tramite dell'RPD provvede alla comunicazione di detta violazione a tutti gli interessati coinvolti, senza ingiustificato ritardo.

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 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, previste dall'art. 33, lett. b), c) e d):

- 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 (si pensi a siti istituzionali dell'AOUS, giornali, televisioni, radio o altro).

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.

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.

Nello specifico, viene:

- effettuata una valutazione della probabilità e gravità del rischio per i diritti e le libertà degli interessati derivanti dalla violazione di dati personali;
- definito un piano di gestione della violazione, comprensivo di: azioni volte a mitigare gli impatti negativi della violazione, valutazione sulla notifica della violazione all'Autorità di Controllo ed eventuale comunicazione della violazione agli interessati;
- proposta l'adozione di misure volte a mitigare gli impatti negativi della violazione ed evitare che l'evento si ripeta in futuro, documentando e riportando costantemente l'esito delle azioni svolte.

A tal fine, con il supporto del Responsabile della protezione dei dati (RPD), il Titolare registra nel Registro delle Violazioni (Allegato 2) 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.

6.1. 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.

7. 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)	Ufficio Privacy	Referente ESTAR (se presente)	Responsabile dell'Ufficio Innovazione AOUS	Chiunque ne venga a conoscenza e il Direttore di Struttura/Preposto	RPD
Rilevazione D.B.	**I**	**R**	**C**	**R**	**R**	**R**	**C**
Analisi e Valutazione D.B.	**I**	**R**	**C**	**R**	**R**	**R**	**C**
Gestione D.B.	**I**	**C**	**R**	**C**	**C**	**C**	**C**
Notifica D.B.	**R**	**I**	**C**	**C**	**C**	**I**	**C**
Comunicazione agli interessati	**R**	**I**	**C**	**I**	**I**	**I**	**R**
Applicazione della misura correttiva	**R**	**R**	**I**	**C**	**C**	**C**	**I**
Archivio documentazione: fascicolo di ogni violazione e registro D.B.	**I**	**I**	**R**	**I**	**I**	**I**	**C**

8. 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.

9. NORMA FINALE

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

La presente procedura è pubblicata nella sezione "Privacy / 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.**

Allegato 1

Scheda delle violazioni personali

Data della violazione	
Tipo	Violazione impattante sugli elementi: ☐ Riservatezza ☐ Integrità ☐ Disponibilità / Continuità operativa ☐ Resilienza
Natura della violazione	Ad es. illecita (ad es. furto) – accidentale (ad es. smarrimento)
Descrizione della violazione	
Dati personali violati	
Interessati colpiti	
Numero registrazioni dati colpite	
Dati del Titolare	**Azienda Ospedaliero-Universitaria Senese** Strada delle Scotte n. 14, 53100 - Siena Tel. 0577585111 Pec: ao-siena@postacert.toscana.it
Effetti e conseguenze della violazione	
Gli interessati sono stati informati?	
Azioni volte al contenimento della violazione dei dati e alla minimizzazione dell'impatto sugli interessati	
Data completamento azioni	
Altre informazioni	
Valutazione su notifica della violazione all'Autorità Garante	
Lesson learned	

Si attesta che è stata iscritta la violazione in data ___ / ___/ _____

Si attesta che è stata integrata in data ___ / ___/ _____

Allegato 2

Registro delle violazioni personali

Allegato 2 Registro delle violazioni dati personali

Numero Violazione Dati Personali	Data della violazione	Descrizione violazione

Allegato 3

Sintesi della modalità operativa

Chi deve segnalare? 	Chiunque ne venga a conoscenza
A chi devo segnalare? 	Al Direttore/Preposto, il quale informa via e-mail l'Ufficio Privacy aziendale. Quest'ultimo convoca immediatamente il Comitato di Valutazione composto dall'RPD, dall'Ufficio privacy aziendale, dal Direttore/Preposto della struttura presso cui è avvenuta il Data Breach, dal Referente ESTAR supporto informatico o suo delegato e dal Responsabile dell'Ufficio Innovazione AOUS (qualora si tratti di Data Breach informatico) e da altri soggetti che per qualifica o per competenza sono informati o possono fornire un contributo per la gestione della violazione.
Come segnalare? 	Preferibilmente mediante comunicazione scritta trasmessa via e-mail o, comunque, laddove non è possibile procedere immediatamente anche telefonicamente o di persona.
Quando segnalare? 	Tempestivamente, e comunque non oltre le 24 ore dalla presa di conoscenza dell'evento che potrebbe aver dato luogo ad una possibile violazione di dati personali