

**IMMEDIATAMENTE
ESECUTIVA**

DELIBERA DEL COMMISSARIO STRAORDINARIO

N° 1615 DEL 27 SET 2023

OGGETTO: Parziale modifica deliberazione n. 1640 del 20/09/2023 Revisione della procedura per la gestione di violazione dei dati personali c.d. Data Breach in esecuzione della delibera n. 1138 del 22/06/2023

STRUTTURA PROPONENTE: U.O.C. COORDINAMENTO STRUTTURE DI STAFF **PROPOSTA N°** 281 **DEL** 26.09.2023

Il Dirigente e/o il responsabile del procedimento attestano – con la sottoscrizione del presente atto ed a seguito dell'istruttoria effettuata – la regolarità della procedura seguita, che l'atto è legittimo nella forma e nella sostanza nonché utile per il servizio pubblico.

<p>L'ESTENSORE DEL PROVVEDIMENTO Dott.ssa Daniela Salvato</p> <p><i>(firma)</i></p> <p>Data: <u>26.09.2023</u></p>	<p>IL RESPONSABILE PROCEDIMENTO Dr.ssa Emanuela Carbonaro</p> <p><i>(firma)</i></p> <p>Data: <u>26.09.2023</u></p>	<p>IL DIRETTORE DELLA STRUTTURA PROPONENTE Dr. Tommaso Mannone</p> <p><i>(firma)</i></p> <p>Data: <u>26.09.2023</u></p>
--	--	---

Il Funzionario addetto al controllo di budget attesta – con la sottoscrizione del presente atto – che lo stesso non comporta scostamenti sfavorevoli rispetto al budget economico e, pertanto, ne attesta la copertura economica dei costi. Attesta, inoltre, il NULLA OSTA in quanto conforme alle norme sulla contabilità.

Conto Economico (n°): _____

Importo (€): nessun euro

Sub-autorizzazione (numero): _____

IL FUNZIONARIO ADDETTO AL CONTROLLO DI BUDGET
Dr. _____

Data: 27/09/23

Direttore f.f. dell'U.O.C. Economico-Finanziario Patrimoniale
Firma
(Dott.ssa Giuliana Alga)

<p>PARERE DEL DIRETTORE AMMINISTRATIVO Dr.ssa Loredana Di Salvo</p> <p><input checked="" type="checkbox"/> Favorevole <input type="checkbox"/> Non Favorevole (con motivazioni allegate al presente atto)</p> <p>Data: <u>27/09/2023</u> Firma: <i>(firma)</i></p>	<p>PARERE DEL DIRETTORE SANITARIO Dr. Aroldo Gabriele Rizzo</p> <p><input checked="" type="checkbox"/> Favorevole <input type="checkbox"/> Non Favorevole (con motivazioni allegate al presente atto)</p> <p>Data: <u>27/09/2023</u> Firma: <i>(firma)</i></p>
--	--

Il presente provvedimento si compone di n. _____ pagine, di cui n. _____ pagine di allegati.

IL COMMISSARIO STRAORDINARIO
Dr. Walter Messina

In data 27 SET 2023 nella sede legale dell'Azienda Ospedaliera "Ospedali Riuniti Villa Sofia – Cervello" di Palermo Viale Strasburgo n. 233, P.I. 05841780827

IL COMMISSARIO STRAORDINARIO
Dr. Walter Messina

nominato con Decreto Assessoriale n. 53/2022 del 29 dicembre 2022 e prorogato con Decreto Assessoriale n.28/2023/Gab del 29 giugno 2023, con l'intervento del Direttore Sanitario Dr. Aroldo Gabriele Rizzo, nominato con Delibera n. 257 del 21 giugno 2019 e con l'intervento del Direttore Amministrativo Dr.ssa Loredana Di Salvo, nominato con Delibera n. 101 del 26 gennaio 2021, assistito dal segretario verbalizzante Giuseppe Bartoletta, adotta la seguente deliberazione:

DELIBERA DEL COMMISSARIO STRAORDINARIO

U.O.C. COORDINAMENTO STRUTTURE DI STAFF U.O.S. PROTEZIONE DATI PERSONALI

- VISTO** il decreto legislativo 10.08.2018 n.101, recante “Disposizioni per l’adeguamento della normativa Nazionale alle disposizioni del regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27.04.2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché la libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), che ha sostanzialmente integrato e modificato il citato Codice in materia di protezione dati personali di cui al D. Lgs. 30.06.2003, n.196;
- ATTESO** che le norme introdotte dal regolamento UE 2016/679 (GDPR) si traducono in adempimenti organizzativi, documentali e tecnici che tutti i Titolari del trattamento dei dati personali devono considerare e tenere presenti per consentire la piena e consapevole applicazione del nuovo quadro normativo in materia di protezione dati personali di cui al D.Lgs. 30.06.2003 n.196;
- DATO ATTO** che con deliberazione n. 300 del 27.02.2020 e con successiva deliberazione n. 2103 del 22/12/2022 questa Azienda ha aggiornato il regolamento per protezione dei dati personali in coerenza al Regolamento Europeo 2016/679, D. Lgs. n. 196/2003 modificato dal D. Lgs. n.101/2018;
- DATO ATTO** altresì che, questa Azienda con deliberazione n.1479 del 10.09.2018 ha designato, ai sensi dell’art. 37 del citato GDPR, il Responsabile della Protezione Dati (DPO) e con successivo provvedimento n.580 del 21.04.2021 ha identificato la Dott.ssa Emanuela Carbonaro - Dirigente Analista in servizio presso l’Azienda;
- DATO ATTO** che con deliberazione n.656 del 03.10.2019 questa Azienda ha costituito il Gruppo di Lavoro a supporto del Data Protection Officer e con deliberazione n. 657 del 03.10.2019 ha costituito l’Ufficio per la protezione dei dati;
- DATO ATTO** che questa Azienda, Titolare del trattamento dei dati personali, nella persona del Rappresentante Legale e Direttore Generale, ha aderito ai dettami del Legislatore Europeo mediante l’adozione dei provvedimenti sopradetti e l’avvio delle azioni di carattere organizzativo-gestionale rispettose dei precetti di cui al Regolamento UE 2016/679;
- DATO ATTO** che con deliberazione n. 1179 del 9.08.2021 l’Azienda ha approvato la procedura per la gestione di violazione dei dati personali c.d. Data Breach (art. 33 e 34 del Regolamento UE 2016/679) e dei relativi modelli applicativi;
- PRESO ATTO** delle ulteriori disposizioni contenute nel Provvedimento del 27 maggio 2021, del Garante della Protezione dei dati, in merito alla notifica di una violazione;
- RITENUTO** pertanto, di dovere adeguare le disposizioni richiamate nel Provvedimento per la gestione di violazione dei dati personali c.d. Data Breach e per l’effetto, in sostituzione della precedente procedura approvata con deliberazione n. 1179/2021, adottare la vigente procedura e i relativi atti allegati, quali parti sostanziali e integranti del presente provvedimento, di seguito riportati:
- a) Procedura Gestione Data Breach Azienda Ospedaliera “Ospedali Riuniti Villa Sofia-Cervello” Palermo artt. 33 e 34 Regolamento UE 2016/679;
 - b) “Violazione di dati personali, modello di comunicazione al titolare del trattamento da parte del personale interno” (allegato n.1);
 - c) “Violazione di dati personali, modello di comunicazione al titolare del trattamento da parte del responsabile esterno del trattamento art. 28 GDPR” (allegato n.2);
 - d) “Registro della violazione dei dati Data Breach” (allegato n.3);



DELIBERA DEL COMMISSARIO STRAORDINARIO

RICHIAMATA la delibera n. 1138 del 22/06/2023 relativa alla procedura per elaborazione e la gestione Documentale che consente di codificare le procedure aziendali;

DATO ATTO che il presente provvedimento non comporta alcun onere di spesa per questa Azienda;

RITENUTO di dovere disporre l'immediata esecuzione del presente provvedimento, ai sensi del punto 7 dell'art. 53 della L. reg. n. 30/1993;

ATTESO che con la sottoscrizione del presente provvedimento si dichiara che l'istruttoria è corretta, completa e conforme alle risultanze degli atti d'ufficio;

ATTESO che il Responsabile del procedimento e il Responsabile della struttura proponente attestano inoltre, l'assenza di conflitto di interessi, ai sensi della normativa vigente e del Codice di Comportamento;

ATTESO che il Responsabile della Struttura proponente attesta la liceità e la regolarità delle procedure poste in essere con il presente provvedimento, in quanto legittime ai sensi della normativa vigente con riferimento alla materia trattata, nonché attesta l'utilità e l'opportunità per gli obiettivi aziendali e per l'interesse pubblico;

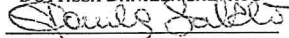
PROPONE


Per i motivi indicati in premessa che qui si intendono integralmente riportati, di:

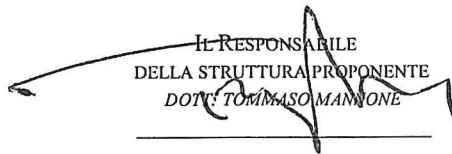
- 1) **adottare** per le motivazioni espresse in premessa, la revisione della procedura aziendale per la gestione delle violazioni di dati personali "Data Breach" - ai sensi e per gli effetti degli artt. 33 e 34 del Regolamento UE 2016/679 - e gli atti allegati di seguito riportati, quali parti sostanziali e integranti del presente provvedimento:
 - a) Procedura Gestione Data Breach Azienda Ospedaliera "Ospedali Riuniti Villa Sofia-Cervello" Palermo artt. 33 e 34 Regolamento UE 2016/679;
 - b) "Violazione di dati personali, modello di comunicazione al titolare del trattamento da parte del personale interno" (allegato n.1);
 - c) "Violazione di dati personali, modello di comunicazione al titolare del trattamento da parte del responsabile esterno del trattamento art. 28 GDPR" (allegato n.2);
 - d) "Registro della violazione dei dati Data Breach" (allegato n.3);
- 2) **dare atto** che il presente provvedimento sostituisce integralmente quello approvato con provvedimento n.1640 del 20/9/2023;
- 3) **incaricare** le Strutture competenti dell'esecuzione del presente provvedimento;
- 4) **dare atto** che la predetta procedura entrerà in vigore dal giorno successivo all'adozione del presente provvedimento;
- 5) **dare atto** ex art 6 bis L. n. 241/1990 e s.m.i. che, per il presente provvedimento, non sussistono motivi di conflitto di interesse, neppure potenziali, per il Responsabile del procedimento, per il Responsabile della Struttura proponente e per chi lo adotta;
- 6) **pubblicare** il presente provvedimento, a cura dell'Ufficio Protezione Dati, sul sito web aziendale alla sezione Protezione Dati, in ottemperanza degli obblighi del D. Lgs. 33/2013 e affinché venga fornita massima pubblicità e diffusione;
- 7) **notificare** il presente provvedimento a tutto il personale, a cura dell'UOC Coordinamento Strutture di Staff mediante comunicazione aziendale;
- 8) **disporre** l'immediata esecuzione del presente provvedimento, ai sensi del punto 7 dell'art. 53 della L. reg. n. 30/1993, al fine di consentire l'adozione delle procedure di che trattasi con tempestività;



DELIBERA DEL COMMISSARIO STRAORDINARIO

L'ESTENSORE
DEL PROVVEDIMENTO
DOTT.SSA DANIELA SALVATO


IL RESPONSABILE
DEL PROCEDIMENTO
DOTT.SSA EMANUELA CARBONARO


IL RESPONSABILE
DELLA STRUTTURA PROPONENTE
DOTT. TOMMASO MANNONE


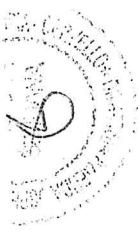
IL COMMISSARIO STRAORDINARIO

- IN VIRTÙ** del Decreto del Presidente della Regione Siciliana n. 198 del 4 aprile 2019 di nomina del Dr. Walter Messina quale Direttore Generale dell'Azienda Ospedaliera "Ospedali Riuniti Villa Sofia Cervello" e della susseguente Delibera n. 1 del 16 aprile 2019 di presa d'atto di detto D.P.R.S., del D.A. n. 53/2022 del 29.12.2022 di nomina a Commissario Straordinario e Decreto Assessoriale n. 28/2023 del 29/06/2023 di proroga a Commissario Straordinario;
- VISTA** la proposta di deliberazione che precede, avente a oggetto "Revisione della procedura per la gestione di violazione dei dati personali c.d. Data Breach (artt. 33 e 34 del Regolamento UE 2016/679) e adozione dei nuovi modelli applicativi";
- ACQUISITI** i pareri espressi dal Direttore Amministrativo e dal Direttore Sanitario;
- RITENUTO** di condividerne il contenuto;

DELIBERA

Per le motivazioni indicate in premessa che qui di seguito si intendono integralmente riportate, di:

- 1) adottare** per le motivazioni espresse in premessa, la revisione della procedura aziendale per la gestione delle violazioni di dati personali "Data Breach" - ai sensi e per gli effetti degli artt. 33 e 34 del Regolamento UE 2016/679 - e gli atti allegati di seguito riportati, quali parti sostanziali e integranti del presente provvedimento:
- e) Procedura Gestione Data Breach Azienda Ospedaliera "Ospedali Riuniti Villa Sofia-Cervello" Palermo artt. 33 e 34 Regolamento UE 2016/679;
 - f) "Violazione di dati personali, modello di comunicazione al titolare del trattamento da parte del personale interno" (allegato n.1);
 - g) "Violazione di dati personali, modello di comunicazione al titolare del trattamento da parte del responsabile esterno del trattamento art. 28 GDPR" (allegato n.2);
 - h) "Registro della violazione dei dati Data Breach" (allegato n.3);
- 2) dare atto** che il presente provvedimento sostituisce integralmente quello approvato con provvedimento n.1640 del 20/9/2023;
- 3) incaricare** le Strutture competenti dell'esecuzione del presente provvedimento;



DELIBERA DEL COMMISSARIO STRAORDINARIO


- 4) **dare atto** che la predetta procedura entrerà in vigore dal giorno successivo all'adozione del presente provvedimento;
- 5) **dare atto** ex art 6 bis L. n. 241/1990 e s.m.i. che, per il presente provvedimento, non sussistono motivi di conflitto di interesse, neppure potenziali, per il Responsabile del procedimento, per il Responsabile della Struttura proponente e per chi lo adotta;
- 6) **pubblicare** il presente provvedimento, a cura dell'Ufficio Protezione Dati, sul sito web aziendale alla sezione Protezione Dati, in ottemperanza degli obblighi del D. Lgs. 33/2013 e affinché venga fornita massima pubblicità e diffusione;
- 7) **notificare** il presente provvedimento a tutto il personale, a cura dell'UOC Coordinamento Strutture di Staff mediante comunicazione aziendale;
- 8) **disporre** l'immediata esecuzione del presente provvedimento, ai sensi del punto 7 dell'art. 53 della L. reg. n. 30/1993, al fine di consentire l'adozione delle procedure di che trattasi con tempestività;

IL COMMISSARIO STRAORDINARIO
Dr. Walter Messina

Il Segretario verbalizzante

Giuseppe Barolotta

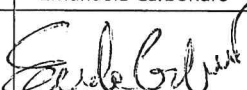



	PROCEDURA GESTIONE DATA BREACH		
	Unità Operative Aziendali	PR-DPO-PG-01 Ed. 01 Rev. 01	Data 26.09.2023

PROCEDURA
GESTIONE DATA BREACH
Azienda Ospedaliera
"Ospedali Riuniti Villa Sofia - Cervello"
Palermo
Artt. 33 e 34 Regolamento UE 2016/679

LISTA DI DISTRIBUZIONE

Tutte le Unità Operative aziendali


Ed.	Rev.	Data	Causale/Motivo della Revisione	Redazione	Verifica	Approvazione	Delibera
01	00	09.08.2021	Prima stesura	Emanuela Carbonaro	Tommaso Mannone		Delibera n. 1179 del 09.08.2021
01	01	26.09.2023	Prima Revisione Aggiornamento intera procedura Data Breach come da Provvedimento del 27 maggio 2021 in merito alla notifica di una violazione	Ufficio Protezione dei Dati	Coordinamento Strutture di Staff	Direttore Generale	Delibera n. ____ del __/__/____
PR-DPO-PG-01 Ed. 01 Rev. 01							In vigore dal
Nome e Cognome				Emanuela Carbonaro	Tommaso Mannone	Direttore Generale	Data di entrata in
Firma							vigore: adozione delibera

	PROCEDURA GESTIONE DATA BREACH		
	Unità Operative Aziendali	PR-DPO-PG-01 Ed. 01 Rev. 01	Data 26.09.2023

<u>1. PREMESSA:</u>	3
<u>2. DEFINIZIONI:</u>	3
<u>3. SCOPO DELLA PROCEDURA:</u>	4
<u>4. IL "DATA BREACH":</u>	4
<u>5. MODALITA' DI GESTIONE DEL DATA BREACH:</u>	5
<u>5.1 SOGGETTI INTERESSATI ALLA PROCEDURA DI DATA BREACH:</u>	6
<u>5.2 ANALISI DELLA VIOLAZIONE:</u>	7
<u>5.2.1. Primo Step – ANALISI SEGNALAZIONE RICEVUTA</u>	7
<u>5.2.2. Secondo Step – RICONOSCIMENTO DELLA VIOLAZIONE E ANALISI CAUSE.</u>	9
<u>5.2.3. Terzo Step - DEFINIZIONE MISURE ATTUATIVE</u>	11
<u>5.2.4. Quarto Step – ANALISI EFFICACIA DELLE MISURE CORRETTIVE APPLICATE</u>	12
<u>5.3 MODALITA' E PROFILI DI SEGNALAZIONE AL GARANTE:</u>	12
<u>5.4 NOTIFICA AGLI INTERESSATI:</u>	13
<u>6. DOCUMENTI DI RIFERIMENTO:</u>	14
<u>7. DOCUMENTI IN ALLEGATO:</u>	14



1. PREMESSA:

	PROCEDURA GESTIONE DATA BREACH		
	Unità Operative Aziendali	PR-DPO-PG-01 Ed. 01 Rev. 01	Data 26.09.2023



Il presente documento è redatto in adempimento a quanto previsto dal Regolamento UE 2016/679 (di seguito GDPR) in materia di violazione del dato personale anche detto “**Data Breach**” che secondo l’art. 4 par. 12 del GDPR si intende “*l’avvenuta 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*”

L’Azienda Ospedaliera “Ospedali Riuniti Villa Sofia – Cervello” in quanto titolare del Trattamento è pertanto obbligata a proteggere i dati personali trattati nell’ambito delle proprie attività e ad agire prontamente in caso di violazione dei dati stessi.

Questa procedura, che individua le attività da porre in essere in caso di violazione dei dati, concrete, potenziali o sospette, modifica e fa decadere quella già adottata giusta deliberazione prot. N° 1179 del 09/08/2021.

2. DEFINIZIONI:

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.

Titolare del trattamento: la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell’Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell’Unione o degli Stati membri (art. 4, punto 7).

Interessato: L’interessato (data subject) al trattamento è la persona fisica a cui si riferiscono i dati personali.


Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l’interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, punto 2).

Data Protection Officer: la persona fisica individuata come Responsabile della protezione dei dati personali ai sensi del GDPR (in particolare artt. 37, 38, 39).

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, punto 6).

Data Breach: l’avvenuta 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 (l’art. 4 par. 12).



	PROCEDURA GESTIONE DATA BREACH		
	Unità Operative Aziendali	PR-DPO-PG-01 Ed. 01 Rev. 01	Data 26.09.2023

3. SCOPO DELLA PROCEDURA:

La procedura Data Breach è redatta al fine di tutelare i dati personali, particolari, giudiziari e per documentare l'eventuale gestione delle violazioni dei dati trattati dall'Azienda Ospedaliera "Ospedali Riuniti Villa Sofia - Cervello" di Palermo in qualità di Titolare del trattamento.

Questo documento fornisce le indicazioni sulle opportune modalità di gestione, nel rispetto della normativa in materia di trattamento dei dati personali, garantendo, in particolare, l'aderenza ai principi e alle disposizioni contenute nel Regolamento UE 2016/679.

4. IL "DATA BREACH":

Una violazione dei dati personali può compromettere le misure, l'integrità o la disponibilità di dati personali, così come chiarito dal Gruppo di Lavoro WP250 nelle Linee Guida in materia di notifica delle violazioni di dati personali.

Il Gdpr chiarisce nell'art. 33 che *"in caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di controllo competente a norma dell'art. 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo"*.

L'articolo 32 del regolamento illustra che nell'attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza proporzionale al rischio, si dovrebbe prendere in considerazione, tra le altre cose, **"la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento"** nonché **"la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico"**.


Pertanto secondo le Linee Guida del WP29 ogni tipo di indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche, concetto sempre valido tranne nel caso di indisponibilità a causa di intervento tecnico di manutenzione programmato che non rappresenta una violazione della sicurezza.

Inoltre, qualsiasi perdita o distruzione permanente dei dati personali che implichi la perdita temporanea di disponibilità dovrebbe essere documentata in conformità all'articolo 33, paragrafo 5. Tuttavia, a seconda delle circostanze in cui si verifica, la violazione potrebbe anche non richiedere la notifica all'autorità di controllo e la comunicazione alle persone fisiche coinvolte.

Al fine di gestire una corretta attività di Data Breach, il titolare del trattamento sarà obbligato a valutare la probabilità e la gravità dell'impatto della violazione dei dati personali sui diritti e sulle libertà delle persone fisiche e nel caso si possa presentare un rischio elevato per i diritti e le libertà dell'interessato, solo in questo caso secondo l'Art. 33 sarà necessario notificare al Garante l'accaduto.

Rappresentano una Violazione del Dato Personale o Data Breach, anche i fenomeni di seguito indicati:

- furto o smarrimento di strumenti aziendali portatili e fissi contenenti Dati personali;
- furto o smarrimento di documenti cartacei aziendali contenenti Dati personali;
- perdita o modifica irreparabile di archivi contenenti Dati personali in formato cartaceo o digitale;
- diffusione impropria di Dati personali, per mezzo di:
 - invio e-mail contenente Dati personali al destinatario errato;
 - invio di e-mail con un file contenente Dati personali allegati erroneamente;

	PROCEDURA GESTIONE DATA BREACH		
	Unità Operative Aziendali	PR-DPO-PG-01 Ed. 01 Rev. 01	Data 26.09.2023

- esportazione fraudolenta o errata di Dati personali dai sistemi aziendali;
- virus o altri attacchi al sistema informatico o alla rete del Titolare;
- divulgazione di dati confidenziali a persone non autorizzate;
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- segnalazione da parte di un fornitore di beni e servizi di un evento di Data Breach sui propri sistemi che ha interessato o potrebbe potenzialmente interessare Dati personali del Titolare del trattamento.

La mancata notifica di un Data Breach può comportare ulteriori accertamenti da parte del Garante quale la palese assenza di "Accountability" principio cardine del GDPR.

Tutti gli eventi di Data Breach, compresi quelli per cui non sono necessarie le notifiche, devono essere documentati (art. 33 par. 5 del GDPR) su un "Registro delle Violazioni", il cui modello si allega alla presente. L'esigenza di garantire la tutela dei dati impone, anche nel caso in cui il Titolare, per motivi scaturiti da una valutazione puntuale fatta con il supporto del DPO, l'annotazione della violazione nel Registro anche a giustificazione della mancata notifica che deve, comunque, essere motivata. Inoltre sempre secondo l'art. 33 del Regolamento (UE) n. 2016/679, il Titolare del trattamento, in caso sia consapevole di una violazione dei Dati personali trattati ed essa comporti un rischio elevato per i diritti e la libertà delle persone fisiche è tenuto a:

- informare il Garante Privacy entro e non oltre le 72 ore successive all'avvenuta conoscenza della violazione.
- nel caso in cui tale violazione sia suscettibile di comportare un rischio elevato per i diritti e le libertà degli interessati, a informare senza ritardo anche gli stessi Interessati.


5. MODALITA' DI GESTIONE DEL DATA BREACH:

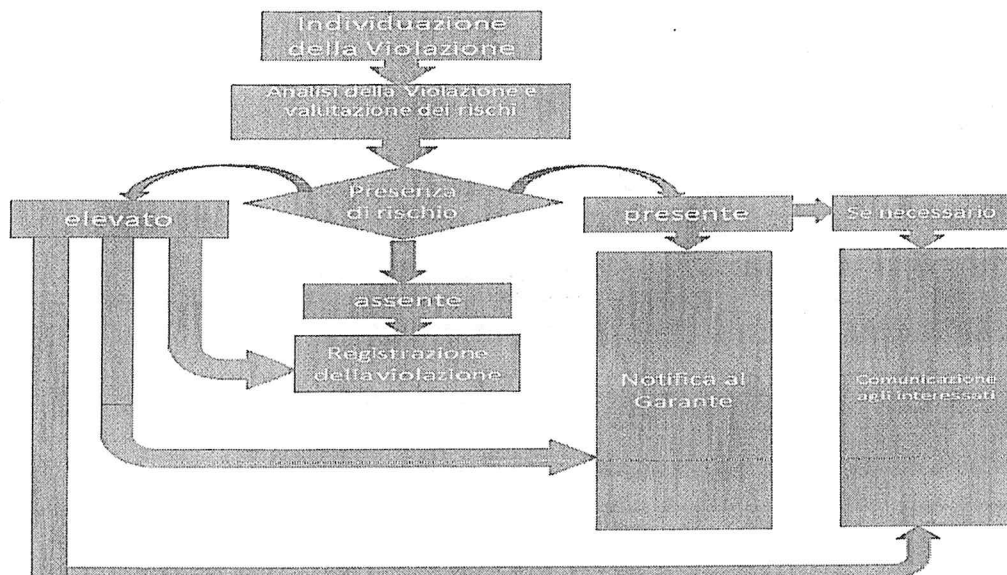
Gli step da seguire per una corretta gestione del data breach sono:

- 1) Identificazione soggetti interessati alla procedura di Data Breach;
- 2) Analisi della violazione;
- 3) Modalità e profili di segnalazione all'Autorità Garante;
- 4) Comunicazione agli interessati dell'avvenuta violazione (sempre in caso di rischio elevato e da valutare anche in tutti gli altri casi).

Le azioni verranno interamente eseguite dal Titolare del Trattamento con il supporto, quando necessario del DPO e del Gruppo di lavoro sulla protezione dei dati.

Di seguito il flusso dei processi:

	PROCEDURA GESTIONE DATA BREACH		
	Unità Operative Aziendali	PR-DPO-PG-01 Ed. 01 Rev. 01	Data 26.09.2023



5.1 SOGGETTI INTERESSATI ALLA PROCEDURA DI DATA BREACH:

La procedura di Data Breach è rivolta a tutti i soggetti che a qualsiasi titolo trattano dati di competenza del Titolare del trattamento, quali:


- i lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto intercorrente - abbiano accesso ai dati personali trattati nel corso del proprio impiego per conto del Titolare del trattamento (collaboratori, tirocinanti, liberi professionisti)
- qualsiasi soggetto (persona fisica o persona giuridica) diverso dai soggetti sopra menzionati che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento ex art. 28 GDPR o di autonomo Titolare (art. 26 Contitolarità del trattamento).

Il responsabile del trattamento oppure il Contitolare sarà tenuto a prendere visione della presente procedura on line sul sito internet degli Ospedali Riuniti.

Qualora uno dei soggetti di cui sopra, venga a conoscenza di un potenziale caso di data breach, è tenuto a dare comunicazione tempestiva al Titolare del Trattamento entro 24h e non oltre, da quando ne è venuto a conoscenza, come di seguito specificato:

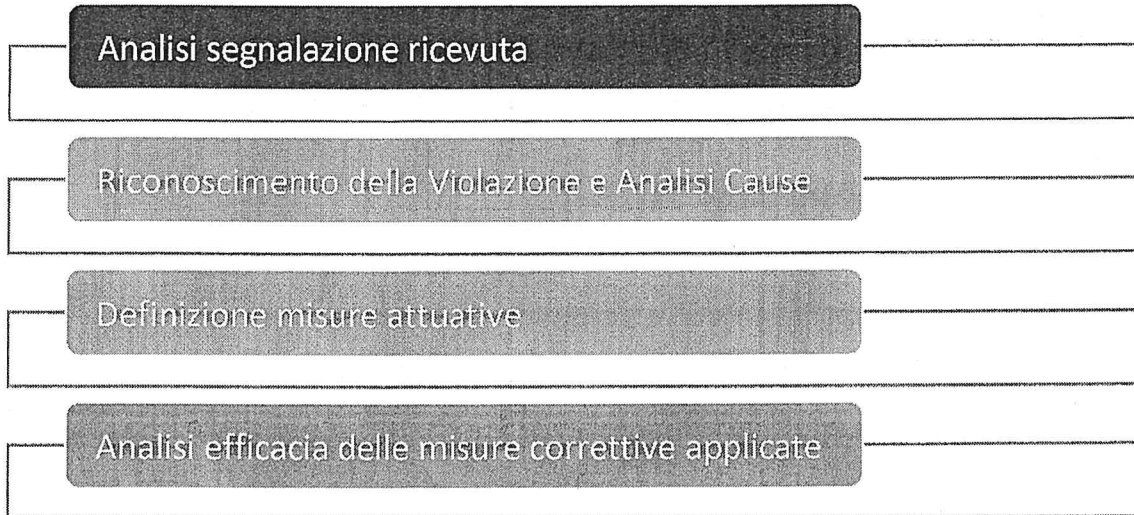
- Nel caso si tratti di una segnalazione da parte di personale interno dell'Azienda Ospedaliera "Ospedali Riuniti Villa Sofia – Cervello", la notifica dovrà avvenire attraverso mail istituzionale con priorità alta all'indirizzo segreteria@ospedaliriunitipalermo.it, con oggetto l'indicazione "potenziale Data Breach" con in allegato il "modulo di comunicazione Data Breach per personale interno" compilato e firmato in ogni sua parte. E' onere di chi segnala l'evento accertarsi dell'arrivo della comunicazione direttamente o attraverso altri canali.
- Se invece si dovesse trattare di una notifica da parte di un Responsabile Esterno, quest'ultimo dovrà inviare mail PEC all'indirizzo protocollo@pec.ospedaliriunitipalermo.it sempre con priorità alta e riportando nell'oggetto "potenziale Data Breach" con in allegato il modulo "modulo di comunicazione Data Breach per Responsabile Esterno" compilato e firmato in ogni sua parte.

Il Titolare del Trattamento con il supporto del DPO procederà ad analizzare la segnalazione ricevuta e valutare se si è in presenza di un Data Breach valutando la portata di questo in termini di impatto rispetto ai dati personali ed ai diritti e libertà degli interessati.

	PROCEDURA GESTIONE DATA BREACH		
	Unità Operative Aziendali	PR-DPO-PG-01 Ed. 01 Rev. 01	Data 26.09.2023

5.2 ANALISI DELLA VIOLAZIONE:

Sulla scorta del “Modulo notifica potenziale Data Breach”, il Titolare del Trattamento, inizierà un processo di analisi e definizione evento definito “step by step”, di seguito schematizzato e dettagliato:



L'analisi della violazione può essere portata all'ordine del giorno del Gruppo di lavoro sulla protezione dei dati.

Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto della normativa.

5.2.1. Primo Step – ANALISI SEGNALAZIONE RICEVUTA


Il primo step è l'analisi della segnalazione ricevuta del potenziale Data Breach, al fine di stabilire se davvero si tratta di una Violazione dei dati personali come da punto 4 della presente procedura.

Per procedere con tale analisi, il Garante della Privacy ha istituito con Provvedimento del 27 maggio 2021, un utile strumento di autovalutazione (self assessment) all'indirizzo web <https://servizi.gpdp.it/databreach/s/self-assessment>, che consente di individuare le azioni da intraprendere a seguito di una probabile violazione dei dati personali derivante da un incidente di sicurezza.

Tale strumento è esclusivamente quale ausilio al processo decisionale del Titolare del trattamento.

Di seguito l'estratto delle pagine del Garante in merito all'autovalutazione:

immagine 1

	PROCEDURA GESTIONE DATA BREACH		
	Unità Operative Aziendali	PR-DPO-PG-01 Ed. 01 Rev. 01	Data 26.09.2023

Autovalutazione per individuare le azioni da intraprendere a seguito di una violazione dei dati personali

* Si è verificato un incidente di sicurezza che ha comportato la perdita di riservatezza, integrità o disponibilità di dati?

SI

NO

Pertanto, se la risposta sarà "no", il form di autovalutazione chiuderà il processo, indicando: "Se non si è verificato un incidente di sicurezza - che ha comportato la perdita di riservatezza, integrità o disponibilità di dati - di conseguenza non c'è stata una violazione dei dati personali."

Il Titolare del Trattamento provvederà a chiudere l'evento dandone riscontro al soggetto segnalante e ne darà evidenza sul "Registro delle Violazioni dei Dati", annotando l'accaduto e includendo i motivi per cui il Titolare del trattamento ritiene improbabile che la violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche.

Se la risposta sarà "si", si procederà con la prossima immagine.

Immagine 2

Autovalutazione per individuare le azioni da intraprendere a seguito di una violazione dei dati personali

L'incidente di sicurezza occorso costituisce una violazione dei dati personali.

Una **violazione dei dati personali** è una «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» (cfr. art. 4 punto 12), del Regolamento (UE) 2016/679 e art. 2, comma 1, lett. m), del D.Lgs 51/2018).

Una violazione dei dati personali (*personal data breach* o, più comunemente, *data breach*) è, infatti, un particolare tipo di incidente di sicurezza che, causando perdita di riservatezza, integrità o disponibilità dei **dati personali**, fa sì che il titolare del trattamento non sia più in grado di garantire l'osservanza dei principi relativi al trattamento dei dati personali (cfr. art. 5 del Regolamento (UE) 2016/679 e art. 3 del D.Lgs 51/2018).

Il Garante, sulla base delle informazioni inserite dall'utente, conferma che si tratta ufficialmente di una "Violazione dei Dati personali", proseguendo con la prossima immagine.


Immagine 3

Autovalutazione per individuare le azioni da intraprendere a seguito di una violazione dei dati personali

* Sei titolare o responsabile del trattamento dei dati personali oggetto di violazione?

Responsabile

Titolare

	PROCEDURA GESTIONE DATA BREACH		
	Unità Operative Aziendali	PR-DPO-PG-01 Ed. 01 Rev. 01	Data 26.09.2023

Sarà necessario indicare se chi sta eseguendo l'autovalutazione è Titolare del Trattamento o Responsabile e nel caso in cui si selezioni "Responsabile", il Garante ci invita senza ingiustificato ritardo, a comunicare al Titolare del trattamento la violazione dei dati personali occorsa.

Se invece si selezionerà "Titolare del Trattamento", si potrà procedere con l'autovalutazione come da prossimo paragrafo.

Nel caso in cui l'evento segnalato si dovesse configurare come Data Breach, il Titolare del trattamento dovrà coinvolgere i servizi o i partner segnalatori, così da procedere all'approfondimento e così al secondo step.

5.2.2. Secondo Step – RICONOSCIMENTO DELLA VIOLAZIONE E ANALISI CAUSE.

Per procedere allo svolgimento di un processo di autovalutazione reale e completo, sarà utile procedere non solo con l'analisi delle cause ma valutarne il rischio che potrebbe derivarne, anche in funzione delle misure di sicurezza adottate, della tipologia dei dati trattati e del grado di identificabilità delle eventuali persone fisiche coinvolte, sempre con l'obbligatorio coinvolgimento di tutti i soggetti che hanno procurato o solo segnalato l'evento di violazione di dati personali.

Sarà pertanto utile procedere alla classificazione dell'evento di violazione, secondo le macro aree di seguito specificate e con il necessario coinvolgimento di tutti i soggetti che hanno procurato o solo segnalato l'evento di violazione di dati personali.

- Distruzione dati
- modifica di dati;
- perdita di dati;
- divulgazione non autorizzata;
- accesso non autorizzato;
- Indisponibilità temporanea del dato


Da questa stima ne consegue la definizione delle priorità di azione. Pertanto è necessario assegnare un livello identificativo di rischio:

- NULLO
- BASSO
- MEDIO
- ALTO

Ricordiamo che il rischio, secondo il Considerando 75 e le Linee guida del Gruppo di lavoro Articolo 29 WP248 rev.1, va riferito alla probabilità e alla gravità, che il verificarsi di una Violazione di trattamenti, possa cagionare un danno fisico, materiale o immateriale all'interessato valutato in base a una valutazione oggettiva.

Per una valutazione del rischio completa così come dettato dalle Linee Guida wp250, sarà necessario tenere conto dei seguenti fattori:

- Tipo di violazione
- Natura, carattere sensibile e volume dei dati personali

	PROCEDURA GESTIONE DATA BREACH		
	Unità Operative Aziendali	PR-DPO-PG-01 Ed. 01 Rev. 01	Data 26.09.2023

- Facilità di identificazione delle persone fisiche
- Gravità delle conseguenze per le persone fisiche
- Numero di persone fisiche interessate

con particolare attenzione nel caso si rilevi una violazione in merito a:

- l'origine razziale o etnica;
- le opinioni politiche;
- le convinzioni religiose o filosofiche;
- l'appartenenza sindacale;
- i dati genetici, dati relativi alla salute o dati relativi alla vita sessuale;
- le condanne penali e reati o relative misure di sicurezza;
- i di dati di persone fisiche vulnerabili, in particolare minori.

Stimato il rischio, sarà possibile analizzare le cause dell'avvenuto Data Breach e porre gli opportuni rimedi.

Con le informazioni appena rilevate, potremmo pertanto procedere con l'autovalutazione come da prossima immagine.

Immagine 4

Autovalutazione per individuare le azioni da intraprendere a seguito di una violazione dei dati personali

<p>* È probabile che la violazione presenti un rischio per i diritti e le libertà degli interessati?</p> <p><input type="radio"/> SI</p> <p><input type="radio"/> NO</p>
--


Si andrà a capire se esiste il rischio per i diritti e le libertà degli interessati coinvolti e se la risposta sarà "no", il Garante farà chiuderà il processo, indicando: *"Se ritieni che sia improbabile che la violazione occorsa presenti un rischio per i diritti e le libertà delle persone fisiche i cui dati sono stati violati, non è necessario effettuare la notifica al Garante e la comunicazione agli interessati"*, invitando comunque il Titolare a documentare la Violazione. *«Il Titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di verificare il rispetto del presente articolo»* (cfr. art. 33Apertura sito esterno in una nuova scheda per l'articolo 33 del Regolamento (UE) 2016/679, par. 5, del Regolamento (UE) 2016/679 e art. 26 del D.Lgs 51/2018).

Il Titolare del Trattamento provvederà a chiudere l'evento dandone riscontro al soggetto segnalante e ne darà evidenza sul "Registro delle Violazioni dei Dati", annotando l'accaduto e includendo i motivi per cui il Titolare del trattamento ritiene improbabile che la violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche.

Se la risposta sarà "si", si procederà con l'analisi cause del paragrafo 5.2.2. della presente procedura, e con l'autovalutazione si passa alla prossima immagine.

Immagine 5



	PROCEDURA		
	GESTIONE DATA BREACH		
Unità Operative Aziendali	PR-DPO-PG-01 Ed. 01 Rev. 01	Data 26.09.2023	Pagine 11 di 14

Autovalutazione per individuare le azioni da intraprendere a seguito di una violazione dei dati personali

* La violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche?

SI

NO

Se la risposta sarà "no", il Garante farà chiudere il processo, indicando: *"Se ritieni che la violazione occorsa non comporti un rischio elevato per gli interessati, non è obbligatorio effettuare la comunicazione agli interessati."*

Il Titolare del Trattamento provvederà a chiudere l'evento dandone riscontro al soggetto segnalante e ne darà evidenza sul "Registro delle Violazioni dei Dati", annotando l'accaduto e includendo i motivi per cui il Titolare del trattamento ritiene improbabile che la violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche.

Se la risposta sarà "si", vorrà dire che la nostra valutazione del rischio derivante da una violazione dei dati personali ed effettuata eseguendo quanto precisato nel punto 5.2.2. della presente procedura (cfr. considerando 75 e 76 del Regolamento), ha dato come esito, rischio elevato, pertanto si procederà con il processo di autovalutazione, all'immagine successiva

Immagine 6

Autovalutazione per individuare le azioni da intraprendere a seguito di una violazione dei dati personali

DEVI NOTIFICARE LA VIOLAZIONE AL GARANTE

«In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo» (cfr. art. 33 par. 1, del Regolamento (UE) 2016/679 e art. 26 del D.Lgs 51/2018).


Il Garante infine, confermerà l'obbligo da parte del Titolare del Trattamento di notificare la violazione in analisi e chiarendo le modalità di notifica, che dovranno avvenire in via telematica all'indirizzo web <https://servizi.gpdp.it/databreach/s/>

Al fine di garantire la correttezza formale, l'uniformità di trattamento nonché consentire la possibilità di effettuare le necessarie operazioni di gestione e monitoraggio delle notifiche delle violazioni dei dati personali, la procedura telematica costituisce l'unica ed ordinaria modalità mediante la quale l'Autorità accoglierà le stesse.

Il Titolare del Trattamento inoltre, dovrà coinvolgere i Servizi o i partner segnalatori, così da procedere all'approfondimento necessario.

5.2.3. Terzo Step - DEFINIZIONE MISURE ATTUATIVE



	PROCEDURA		
	GESTIONE DATA BREACH		
Unità Operative Aziendali	PR-DPO-PG-01 Ed. 01 Rev. 01	Data 26.09.2023	Pagine 12 di 14

L'ultimo step vede come protagonista l'individuazione delle misure attuative al fine di rimediare alla violazione così da mitigare i possibili effetti negativi.

E' obbligo del titolare mettere in atto tutte le misure tecniche e/o organizzative adeguate a mitigare il rischio di impatto sugli interessati (o meglio sui loro diritti e sulle libertà). Tali misure essenzialmente presidi di sicurezza delle informazioni, vanno stabiliti sia in modo preventivo secondo il principio di Privacy by design sia a seguito di un avvenuto Data Breach, sempre secondo l'art. art. 32 paragrafo 1, tali misure correttive saranno applicate "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche".

5.2.4. Quarto Step – ANALISI EFFICACIA DELLE MISURE CORRETTIVE APPLICATE

Nello step finale abbiamo invece l'analisi conclusiva, nella quale a seguito della raccolta oggettiva delle evidenze, l'analisi delle informazioni sul Data Breach, e le opportune misure correttive attuate, ed eventuali riscontri ricevuti dal Garante della Protezione dei Dati a seguito della notifica, si procede alla verifica dell'efficacia e dell'efficienza delle azioni intraprese durante la gestione dell'evento

Il quarto step è anche utile per eventualmente identificare possibili aree di miglioramento.


5.3 MODALITA' E PROFILI DI SEGNALAZIONE AL GARANTE:

Identificato un Data Breach con le modalità dettagliate nel presente Documento, il Titolare del Trattamento dovrà procedere con la comunicazione dell'accaduto al Garante della Protezione dei Dati tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo <https://servizi.gpdp.it/databreach/s/> come da Provvedimento del 27 maggio 2021, le informazioni da fornire saranno quelle presenti nel fac-simile prodotto dal Garante, che per comodità si allega alla presente procedura.

La notifica dovrà avvenire, ricordiamo, senza ingiustificato ritardo entro 72 ore dal momento in cui il Titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verifica di un incidente di sicurezza che riguardi dati personali, a meno che non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Si dovranno fornire al Garante dettagliate informazioni in merito all'oggetto della violazione, ma l'art. 33 paragrafo n. 4 del DGPR recita "Qualora nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo". Pertanto, sarà fondamentale raccogliere il maggior numero di informazioni e, anche in caso queste non siano per il momento ritenute esaustive, effettuare la notificazione.

La nuova procedura come da Provvedimento del 27 maggio 2021 dovrà essere utilizzata anche per la trasmissione di informazioni integrative riferite a notifiche trasmesse con le previgenti modalità. Solo per questa fattispecie di notifica integrativa, l'utente non troverà precompilate le diverse sezioni del modulo e non potrà compilare la sez. C e la sez. F, punti 2 e 3.

	PROCEDURA GESTIONE DATA BREACH		
	Unità Operative Aziendali	PR-DPO-PG-01 Ed. 01 Rev. 01	Data 26.09.2023

Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo. Ciò significa che il Regolamento prende atto del fatto che il Titolare del trattamento non sempre dispone di tutte le informazioni necessarie su una violazione entro 72 ore dal momento in cui ne è venuto a conoscenza, dato che non sempre sono disponibili entro tale termine dettagli completi ed esaustivi su un incidente. Pertanto, il regolamento consente una notifica per fasi. Ciò è consentito a condizione che il Titolare del trattamento indichi, ricordiamo, i motivi del ritardo in conformità all'articolo 33 paragrafo 1.

È opportuno infine aggiungere che se, dopo la notifica iniziale, una successiva indagine dimostra che l'incidente di sicurezza è stato correttamente contenuto e che pertanto non è avvenuta alcuna violazione, il Titolare del trattamento può informare di ciò l'autorità di controllo. Tali informazioni possono quindi essere aggiunte alle informazioni già fornite all'autorità di controllo e l'incidente può essere quindi registrato non come un Data Breach.

E' importante sapere che non si incorre in alcuna sanzione se si segnala un incidente che alla fine si rivela non essere davvero una violazione.

E' opportuno infine aggiungere che in caso di disaccordo nell'effettuare la comunicazione al Garante, tra il DPO ed il Titolare del trattamento, prevale la volontà del Titolare del Trattamento. Consiste in una buona prassi documentare le varie fasi decisionali.

5.4 NOTIFICA AGLI INTERESSATI:


Come già più volte indicato, secondo gli articoli 33 e 34 del Gdpr nel caso in cui l'evento di data breach possa generare un rischio elevato per i diritti e le libertà delle persone, queste devono essere informate senza ingiustificato ritardo dall'avvenuta conoscenza e valutazione della violazione, al fine di consentire loro di prendere eventuali provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

Il Titolare del Trattamento pertanto procede alla comunicazione all'interessato/agli interessati da inviarsi tempestivamente e attraverso il canale che si ritiene più opportuno ed anche disponibile. La comunicazione agli interessati dovrà comunque avere precise caratteristiche per garantirne la facile comprensione come anche dettato dall'art. 34. par. 2, dovrà pertanto avere un linguaggio semplice e chiaro, essere concisa e della stessa lingua parlata dall'interessato. Inoltre al fine di avere una comunicazione precisa e dettagliata, la stessa dovrà contenere alcune informazioni basilari, come indicato all' art. 33:

- a) descrivere la 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;
- b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- c) descrivere le probabili conseguenze della violazione dei dati personali;
- d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Ricordiamo infine che secondo l'art. 34 par. 3 non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

8

	PROCEDURA		
	GESTIONE DATA BREACH		
Unità Operative Aziendali	PR-DPO-PG-01 Ed. 01 Rev. 01	Data 26.09.2023	Pagine 14 di 14

- e) 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;
- f) 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;
- g) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Se il Titolare del Trattamento non dovesse avere la possibilità di comunicare una violazione all'interessato perché non dispone di dati sufficienti per contattarlo, il titolare del trattamento provvederà ad informarlo non appena sia ragionevolmente possibile farlo (ad esempio quando l'interessato esercita il proprio diritto ai sensi dell'articolo 15 di accedere ai dati personali e fornisce al titolare del trattamento le informazioni supplementari necessarie per essere contattato).

6. DOCUMENTI DI RIFERIMENTO:

Il presente paragrafo contiene la lista dei documenti di riferimento alla procedura analizzata.

- Regolamento (UE) 2016/679 (GDPR);
- Linee Guida Wp250;
- Fac-simile notifica Data Breach al Garante (in allegato).

7. DOCUMENTI IN ALLEGATO:

- Allegato 1: Modulo comunicazione data breach personale interno (in allegato).
- Allegato 2: Modulo comunicazione data breach responsabile esterno (in allegato)
- Allegato 3: Registro delle Violazioni dei Dati (in allegato).

2

**ALLEGATO 1****MODELLO DI COMUNICAZIONE AL TITOLARE DEL TRATTAMENTO
DA PARTE DEL PERSONALE INTERNO**

Allegato 1 – Procedura Gestione Data Breach -Ed. 01 Rev. 01

AL-DPO-PG-01
Ed. 01 Rev. 00Data
26.09.2023Pagine
1 di 3**VIOLAZIONE DI DATI PERSONALI**

Secondo quanto previsto dalla procedura di Data Breach, il personale interno è tenuto ad informare il Titolare del trattamento, senza ingiustificato ritardo ed in ogni caso **entro le 24 ore** da quando si è venuti a conoscenza della violazione dei dati, comunicazione dall'accadimento compilando il modulo sotto riportato.

Personale interno

Unità Operativa/Area di riferimento _____

Persona fisica addetta alla comunicazione _____

Nome _____

Cognome _____

Funzione rivestita _____

Indirizzo PEC e/o EMAIL per eventuali comunicazioni _____

Recapito telefonico per eventuali comunicazioni _____

Eventuali Contatti (altre informazioni) _____

Denominazione della/e banca/banche dati o dell'archivio cartaceo oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati

Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca dati?

- Il _____
- Tra il _____ e il _____
- In un tempo non ancora determinato
- È possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati?



ALLEGATO 1

**MODELLO DI COMUNICAZIONE AL TITOLARE DEL TRATTAMENTO
DA PARTE DEL PERSONALE INTERNO**

Allegato 1 – Procedura Gestione Data Breach -Ed. 01 Rev. 01

AL-DPO-PG-01
Ed. 01 Rev. 00

Data
26.09.2023

Pagine
2 di 3

Modalità di esposizione al rischio

Tipo di violazione

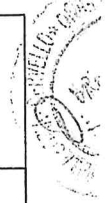
- Lettura (presumibilmente i dati non sono stati copiati)
- Copia (i dati sono ancora presenti sui sistemi del titolare)
- Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
- Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
- Altro

Dispositivo oggetto della violazione

- Computer
- Rete
- Dispositivo mobile
- File o parte di un file
- Strumento di backup
- Documento cartaceo
- Altro

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione

Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

**ALLEGATO 1****MODELLO DI COMUNICAZIONE AL TITOLARE DEL TRATTAMENTO
DA PARTE DEL PERSONALE INTERNO**

Allegato 1 – Procedura Gestione Data Breach -Ed. 01 Rev. 01

AL-DPO-PG-01
Ed. 01 Rev. 00Data
26.09.2023Pagine
3 di 3

- N. persone _____
- Circa persone _____
- Un numero (ancora) sconosciuto di persone

Che tipo di dati sono oggetto di violazione?

- Dati anagrafici/codice fiscale
- Dati di accesso e di identificazione (user name, password, customer ID, altro)
- Dati relativi a minori Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
- Dati personali idonei a rivelare lo stato di salute e la vita sessuale
- Dati giudiziari
- Copia per immagine su supporto informatico di documenti analogici
- Ancora sconosciuto
- Altro

Possibile livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati

- Basso/trascurabile
- Medio
- Alto Molto alto

Potenziati effetti negativi per gli interessati

- Perdita del controllo dei dati personali Limitazione dei diritti Discriminazione Furto o usurpazione d'identità Frodi Perdite finanziarie Decifrazione non autorizzata della pseudonimizzazione Pregiudizio alla reputazione Perdita di riservatezza dei dati personali protetti da segreto professionale Conoscenza da parte di terzi non autorizzati
- Qualsiasi altro danno economico o sociale significativo (specificare)





ALLEGATO 2

**MODELLO DI COMUNICAZIONE AL TITOLARE DEL TRATTAMENTO
DA PARTE DEL RESPONSABILE DEL TRATTAMENTO A NORMA DELL'ART. 33 P. 2
DEL R.E. 2016/679**

Allegato 2 – Procedura Gestione Data Breach -Ed. 01 Rev. 01

AL-DPO-PG-02
Ed. 01 Rev. 00

Data
26.09.2023

Pagine
1 di 4

VIOLAZIONE DI DATI PERSONALI

Ai sensi dell'art. 33 p. 2 del R.E. 2016/679, il Responsabile del trattamento informa il Titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

Di seguito le informazioni necessarie alla comunicazione che dovrà avvenire entro 24 ore dall'accadimento compilando il modulo sotto riportato.

Responsabile del trattamento

Denominazione o ragione sociale _____

Provincia Comune _____

Cap _____ Indirizzo _____

Persona fisica addetta alla comunicazione

Nome _____

Cognome _____

Funzione rivestita _____

Indirizzo PEC e/o EMAIL per eventuali comunicazioni _____

Recapito telefonico per eventuali comunicazioni _____

Eventuali Contatti (altre informazioni) _____

Denominazione della/e banca/banche dati oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati

Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca dati?

Il _____

Tra il _____ e il _____

**ALLEGATO 2****MODELLO DI COMUNICAZIONE AL TITOLARE DEL TRATTAMENTO
DA PARTE DEL RESPONSABILE DEL TRATTAMENTO A NORMA DELL'ART. 33 P. 2
DEL R.E. 2016/679**

Allegato 2 – Procedura Gestione Data Breach -Ed. 01 Rev. 01

AL-DPO-PG-02
Ed. 01 Rev. 00Data
26.09.2023Pagine
2 di 4

- In un tempo non ancora determinato
- È possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)


Modalità di esposizione al rischio*Tipo di violazione*

- 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 li ha neppure l'autore della violazione)
- Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
- Altro

Dispositivo oggetto della violazione

- Computer
- Rete
- Dispositivo mobile
- File o parte di un file
- Strumento di backup
- Documento cartaceo
- Altro

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione



**ALLEGATO 2****MODELLO DI COMUNICAZIONE AL TITOLARE DEL TRATTAMENTO
DA PARTE DEL RESPONSABILE DEL TRATTAMENTO A NORMA DELL'ART. 33 P. 2
DEL R.E. 2016/679**

Allegato 2 – Procedura Gestione Data Breach -Ed. 01 Rev. 01

AL-DPO-PG-02
Ed. 01 Rev. 00Data
26.09.2023Pagine
3 di 4

Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

- N. persone _____
- Circa persone _____
- Un numero (ancora) sconosciuto di persone

Che tipo di dati sono oggetto di violazione?

- Dati anagrafici/codice fiscale
- Dati di accesso e di identificazione (user name, password, customer ID, altro)
- Dati relativi a minori
Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
Dati personali idonei a rivelare lo stato di salute e la vita sessuale
- Dati giudiziari
- Copia per immagine su supporto informatico di documenti analogici
- Ancora sconosciuto
- Altro

Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati (secondo le valutazioni del titolare)?

- Basso/trascurabile
- Medio
- Alto Molto alto

Potenziali effetti negativi per gli interessati

- Perdita del controllo dei dati personali Limitazione dei diritti Discriminazione Furto o usurpazione d'identità Frodi Perdite finanziarie Decifrazione non autorizzata della pseudonimizzazione Pregiudizio alla reputazione Perdita di riservatezza dei dati personali protetti da segreto professionale Conoscenza da parte di terzi non autorizzati
- Qualsiasi altro danno economico o sociale significativo (specificare)



ALLEGATO 2

**MODELLO DI COMUNICAZIONE AL TITOLARE DEL TRATTAMENTO
DA PARTE DEL RESPONSABILE DEL TRATTAMENTO A NORMA DELL'ART. 33 P. 2
DEL R.E. 2016/679**



Allegato 2 – Procedura Gestione Data Breach -Ed. 01 Rev. 01

AL-DPO-PG-02
Ed. 01 Rev. 00

Data
26.09.2023

Pagine
4 di 4

Misure tecniche e organizzative adottate per porre rimedio alla violazione e ridurre gli effetti negativi per gli interessati

Quali misure tecnologiche e organizzative verranno assunte per prevenire simili violazioni future?

La violazione coinvolge interessati di altri Paesi dello Spazio Economico Europeo

- SI Indicare quali _____
- NO

La violazione coinvolge interessati non appartenenti a Paesi dello Spazio Economico Europeo

- SI Indicare quali _____
- NO

La violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative?

- SI Indicare quali _____
- NO

È stata effettuata una segnalazione all'autorità giudiziaria o di polizia?

- SI
- NO



DELIBERA DEL COMMISSARIO STRAORDINARIO

PUBBLICAZIONE

Il sottoscritto dichiara che la presente deliberazione – ai sensi e per gli effetti dell’art. 53, comma 2, della L.R. n. 30/93 e dell’art. 32 della Legge n. 69/09 e s.m.i.– in copia conforme all’originale è stata pubblicata in formato digitale all’Albo on-line dell’Azienda Ospedaliera “*Ospedali Riuniti Villa Sofia – Cervello*”, istituito sul sito www.ospedaliriunitipalermo.it, a decorrere dal giorno 01 OTT 2023 e che nei 15 giorni successivi:

- non sono pervenute opposizioni
 sono pervenute opposizioni da _____

L’ADDETTO
ALLA PUBBLICAZIONE

IL FUNZIONARIO
INCARICATO

Notificata al Collegio Sindacale il _____ prot. n. _____

**DELIBERA NON SOGGETTA
AL CONTROLLO**

- Delibera non soggetta al controllo, ai sensi dell’art. 4, comma 8, della L. n. 412/1991 e divenuta:

ESECUTIVA

decorso il termine (10 giorni
dalla data di pubblicazione)
ai sensi dell’art. 53, comma 6,
L.R. n. 30/93

- Delibera non soggetta al controllo, ai sensi dell’art. 4, comma 8, della L. n. 412/1991 e divenuta:

IMMEDIATAMENTE ESECUTIVA

ai sensi dell’art. 53, comma 7,
L.R. n. 30/93

IL FUNZIONARIO
INCARICATO

**ESTREMI
RISCONTRO TUTORIO**

- Delibera trasmessa, ai sensi della L.R. n. 5/09, all’Assessorato Regionale Salute in data _____
 prot. n. _____

SI ATTESTA

che l’Assessorato Regionale Salute,
esaminata la presente Deliberazione:

- ha pronunciato l’approvazione con atto prot. n. _____ del _____ come da allegato.
 ha pronunciato l’annullamento con atto prot. n. _____ del _____ come da allegato.
 Delibera divenuta esecutiva per decorrenza del termine previsto dall’art. 16 della L.R. n. 5/09 dal _____

IL FUNZIONARIO
INCARICATO

