**Casa di ricovero Muzan**

# PROCEDURA PER LA GESTIONE DI EVENTI POTENZIALMENTE QUALIFICABILI COME DATA BREACH

| | | | |
|---|---|---|---|
| Titolo | Procedura per la gestione di eventi potenzialmente qualificabili come Data Breach | | |
| Emesso da | Casa di ricovero Muzan | | |
| Approvato da | Casa di ricovero Muzan | | |
| Firma legale rappresentante | | | |
| Revisione | 1.0 | | |
| Data revisione | 03 | marzo | 2020 |

## Scopo

Scopo della Procedura è descrivere le norme di comportamento che devono essere osservate in caso di Violazione dei dati personali.

## Destinatari

La Procedura è vincolante per i dipendenti di Casa di ricovero Muzan senza distinzione di ruolo e/o livello, nonché per ogni eventuale ulteriore collaboratore al quale Casa di ricovero Muzan ritenga in qualsivoglia momento e con le modalità ritenute opportune di applicare la Procedura.

## Conoscenza della procedura e formazione

La Procedura viene portata a conoscenza dei Destinatari con una o più tra le seguenti modalità:

- distribuzione con contestuale presa d'atto, ricevuta e sottoscrizione di impegno al rispetto della stessa;
- pubblicazione nell'area personale del portale CBA;
- lettura e spiegazione nel corso di riunioni periodiche;
- comunicazione circolare, anche avvalendosi dei responsabili di ciascuna area, per dare atto di eventuali aggiornamenti della Procedura;
- affissione/pubblicazione della versione più aggiornata della Procedura negli ambienti comuni ritenuti idonei;
- partecipazione ad incontri di formazione.

## Registro delle Violazioni

Casa di ricovero Muzan mantiene aggiornato il Registro delle Violazioni compilando il modello allegato *sub* A, contenente le seguenti informazioni:

- la data scoperta dell'evento;
- la natura della violazione con indicazione, ove possibile, delle categorie e del numero approssimativo di interessati nonché delle categorie e del numero approssimativo di registrazioni dei dati personali in questione;
- 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 ("Azioni di miglioramento e/o correttive") e anche, se del caso, per attenuarne i possibili effetti negativi.

La tenuta e l'aggiornamento del Registro delle Violazioni è responsabilità del Direttore, che vi provvede con il supporto del Funzionario in servizio, dei Fornitori IT, degli ulteriori soggetti che ritenga opportuno coinvolgere caso per caso e/o del DPO: quest'ultimo ha comunque accesso al Registro delle Violazioni.

## Modalità operative

Chi accerta un evento che può risolversi in una Violazione, non deve compiere autonomamente alcuna azione correttiva, di ripristino o intervento sui sistemi informatici, ma limitarsi ad effettuare tempestivamente la segnalazione ed attendere l'intervento da parte delle funzioni competenti, secondo le istruzioni che seguono.

La persona che verifica il manifestarsi di un evento che può risolversi in una Violazione, deve darne immediata comunicazione al Funzionario in servizio, raggiungendolo di persona, telefonicamente o a mezzo posta elettronica oppure, se impossibilitato, con lo strumento ritenuto più idoneo: il Funzionario in servizio, di concerto con il segnalante, redige verbale di ricevuta segnalazione, compilando il modello allegato *sub* B.

Redatto il verbale di ricevuta segnalazione, il Funzionario in servizio contatta tempestivamente gli ulteriori soggetti che ritenga opportuno coinvolgere (es. i Fornitori IT di interesse), oltre che il DPO, al fine di appurare l'entità e la natura dell'evento, valutare se lo stesso costituisca Violazione, nonché, in tale ultima eventualità, per avvisare il Direttore e provvedere alla compilazione del Registro delle Violazioni, in conformità con le prescrizioni della Procedura.

Compilato il registro, Casa di ricovero Muzan dovrà:

- ✓ procedere alla notificazione all'Autorità di Controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuta 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; la notificazione deve essere effettuata compilando il modello allegato *sub* C;

- ✓ comunicare la violazione all'interessato senza ingiustificato ritardo, sempre che la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Eseguite le operazioni di cui al paragrafo precedente, il Direttore verifica - con il supporto, eventualmente necessario, del Funzionario in servizio, dei Fornitori IT di interesse e/o del DPO - l'applicazione delle misure di miglioramento e/o correttive, nonché il ripristino della situazione di normalità.

Le decisioni in ordine alla notificazione all'Autorità di Controllo ed alla comunicazione agli interessati sono assunte dal Direttore, sentito il Funzionario in servizio.

[su carta intestata della società/struttura]

**Allegato B**

## MODELLO VERBALE DI RICEVUTA SEGNALAZIONE DI UN EVENTO POTENZIALMENTE QUALIFICABILE COME VIOLAZIONE DEI DATI PERSONALI

| | |
|---|---|
| NUMERO | |
| DATA E ORA DI RILEVAZIONE DELL'EVENTO | |
| DATA E ORA DELL'EVENTO | |
| AREA / REPARTO IN CUI SI E' VERIFICATO | |
| DESCRIZIONE DETTAGLIATA<br>(compresi sistemi interessati) | |

Data

_____

Firma del segnalante

_____

Funzionario in servizio

_____

[su carta intestata della struttura]

**REGISTRO DELLE VIOLAZIONI DEI DATI PERSONALI *EX* ART. 33, PAR. V, GDPR**

| **INFORMAZIONI SULL'EVENTO** | | |
|---|---|---|
| NUMERO | | |
| DATA E ORA DI RILEVAZIONE DEL DATA BREACH | | |
| MODALITA' DI RILEVAZIONE DEL DATA BREACH | | |
| DATA E ORA DELL'EVENTO | | |
| EVENTUALI MOTIVI DI RITARDO NELLA RILEVAZIONE | | |
| AREA / REPARTO IN CUI SI È VERIFICATO | | |
| TIPO DI VIOLAZIONE | VIOLAZIONE DELLA RISERVATEZZA (in caso di divulgazione dei dati personali o accesso agli stessi autorizzati o accidentali) | |
| | VIOLAZIONE DELL'INTEGRITA' (in caso di modifica non autorizzata o accidentale dei dati personali) | |
| | VIOLAZIONE DELLA DISPONIBILITA' (in caso di perdita accesso o distruzione accidentali o non autorizzati di dati personali) | |
| CAUSE DELLA | AZIONE INTENZIONALE INTERNA | |

[su carta intestata della struttura]

| | | |
|---|---|---|
| VIOLAZIONE | AZIONE ACCIDENTALE INTERNA | |
| | AZIONE INTENZIONALE ESTERNA | |
| | AZIONE ACCIDENTALE ESTERNA | |
| | SCONOSCIUTA | |
| | ALTRO (SPECIFICARE) | |
| CATEGORIE DI DATI OGGETTO DI VIOLAZIONE | | |
| NUMERO DEGLI INTERESSATI E VOLUME DI DATI COINVOLTI NELLA VIOLAZIONE | | |
| TIPOLOGIE DI INTERESSATI COINVOLTI NELLA VIOLAZIONE | | |

[su carta intestata della struttura]

| | | |
|---|---|---|
| DESCRIZIONE DETTAGLIATA<br>(compresi sistemi interessati) | | |
| POSSIBILI CONSEGUENZE DELLA VIOLAZIONE DEI DATI | | |
| POTENZIALI EFFETTI NEGATIVI PER GLI INTERESSATI | | |
| MISURE PREVENTIVE INDIVIDUATE PER EVITARE IL RIPETERSI DELL'EVENTO | • Misure Tecniche | |
| | • Misure organizzative | |
| | • Misure procedurali | |
| | • Misure formative | |
| MISURE CORRETTIVE ADOTTATE | • Misure Tecniche | |
| | • Misure organizzative | |
| | • Misure procedurali | |

| | | |
|---|---|---|
| | • Misure formative / informative | |
| NOTIFICAZIONE ALL'AUTORITÀ DI CONTROLLO | Sì perché / no perché | |
| COMUNICAZIONE AGLI INTERESSATI | Sì perché / no perché | |