INDICE

0. MATRICE DELLE REVISIONI

MATRICE DELLE REVISIONI					
REVISIONE	DATA	DESCRIZIONE / SEGNALAZIONE TIPO MODIFICA	EMISSIONE	VERIFICA	APPROVAZIONE
			RGA	RGA	DIR
00	15/10/2023	Prima emissione	X	X	X

1. PREMESSE

Marrelli Health ai sensi del Regolamento Europeo 2016/679 (da qui in avanti GDPR), è tenuta a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività istituzionali e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (incluse eventuali notifiche all'Autorità Garante competente ed eventuali comunicazioni agli interessati).

Di fondamentale importanza è predisporre azioni da attuare nell'eventualità in cui si presentino violazioni concrete, potenziali o sospette di dati personali, ciò al fine di evitare rischi per i diritti e le libertà degli interessati, nonché danni economici alla Società e per poter riscontrare nei tempi e nei modi previsti dalla normativa europea l'Autorità Garante e/o gli interessati.

L'art. 33 del GDPR recita 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*".

2. SCOPO

Lo scopo di questa procedura è di disegnare un flusso per la gestione delle violazioni dei dati personali trattati da Marrelli Health in qualità di Titolare del trattamento. Queste procedure sono ad integrazione delle procedure adottate dal Titolare del trattamento in materia di protezione dei dati personali ai sensi della legislazione vigente.

3. COS'È UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Una violazione di dati personali è ogni infrazione alla sicurezza degli stessi che comporti - 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 dal Titolare del trattamento.

Le violazioni di dati personali possono accadere per un ampio numero di ragioni che possono includere:

- divulgazione di dati confidenziali a persone non autorizzate;
- perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o furto di documenti cartacei;
- infedeltà aziendale (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
- accesso abusivo (ad esempio: data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- casi di pirateria informatica;

- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo “owner”;
- virus o altri attacchi al sistema informatico o alla rete aziendale;
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
- invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

4. A CHI SONO RIVOLTE QUESTE PROCEDURE

Queste procedure sono rivolte a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento (meglio descritti al punto 5 della presente procedura) 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 (di seguito genericamente denominati Destinatari interni);
- qualsiasi soggetto (persona fisica o persona giuridica) diverso dal Destinatario interno 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 (di seguito genericamente denominati Destinatari esterni);

di seguito, genericamente denominati “Destinatari”.

Tutti i Destinatari devono essere debitamente informati dell’esistenza della presente procedura, mediante metodi e mezzi che ne assicurino la comprensione.

Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.

Così che ogni operatore che venga a conoscenza di una violazione di dati personali deve avvisare tempestivamente il Referente privacy aziendale.

L’eventuale Responsabile nominato ai sensi dell’art.28 del Regolamento UE 679 del 2016, in caso di violazione dei dati personali deve avvertire il Titolare del trattamento entro le 36 ore di avvenuta conoscenza dell’incidente.

5. A QUALI TIPI DI DATI SI RIFERISCONO QUESTE PROCEDURE

Queste procedure si riferiscono a:

- dati personali trattati “da “e “per conto” del Titolare del trattamento, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo;
- dati personali conservati o trattati a mezzo di qualsiasi altro sistema aziendale.

Per «dato personale» si intende: 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.

6. GESTIONE COMUNICAZIONE DI DATA BREACHES

Le violazioni di dati personali sono gestite dal Titolare del trattamento o da un suo delegato.

In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la stessa sia affrontata immediatamente e correttamente al fine di minimizzare l'impatto della violazione e prevenire che si ripeta.

Nel caso in cui uno dei Destinatari si accorga di una concreta, potenziale o sospetta violazione dei dati personali, dovrà immediatamente informare dell'incidente il superiore gerarchico il quale si occuperà, con il supporto dei Destinatari stessi, di informare il Titolare del trattamento o un suo delegato inviando una comunicazione mail all'indirizzo rpd@marrellihealth.it

7. GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI

Per gestire una violazione dei dati personali è necessario seguire i seguenti quattro step:

Step 1: Segnalazione evento Data Breach al DPO, identificazione e indagine preliminare

Step 2: Contenimento, recovery e risk assessment

Step 3: Eventuale notifica all'Autorità Garante

Step 4: Eventuale comunicazione agli interessati

Step 5: Documentazione della violazione

Nello specifico:

Step 1: Segnalazione evento Data Breach al Responsabile della protezione dei dati (DPO) Identificazione e indagine preliminare

Quando viene riscontrato un caso di violazione dei dati personali, il personale coinvolto (anche di ditte esterne Responsabili del trattamento) lo fa presente al Responsabile della U.O. Quest'ultimo contatta il DPO e compila assieme al personale della struttura il modulo di Segnalazione violazione allegato alla presente procedura e reperibile anche sul sito aziendale nella sezione Trasparenza/Privacy.

La segnalazione su modulo deve pervenire al DPO tramite email (rpd@marrellihealth.it). Il DPO informerà immediatamente i vertici aziendali e coinvolgerà nella gestione dell'incidente le diverse funzioni aziendali di competenza.

Il DPO, deve condurre una valutazione iniziale riguardante la notizia dell'incidente occorso, ciò al fine di stabilire se si sia effettivamente verificata un'ipotesi di Data Breach (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto, procedendo con il risk assessment (step 2).

Nel caso in cui si tratti di violazione di dati contenuti in un sistema informatico, DPO dovrà coinvolgere in tutta la procedura indicata nel presente documento anche un esperto informatico.

Detta valutazione iniziale sarà effettuata attraverso l'esame di alcune informazioni quali:

I. la data di scoperta della violazione (tempestività);

II. il soggetto che è venuto a conoscenza della violazione;

III. la descrizione dell'incidente (natura della violazione e dei dati coinvolti);

IV. le categorie e il numero approssimativo degli interessati coinvolti nella violazione;

V. la descrizione di eventuali azioni già poste in essere.

Step 2: Contenimento, Recovery e risk assessment

Una volta stabilito che un Data Breach è avvenuto, il DPO lo comunica al Titolare del Trattamento e insieme dovranno stabilire:

- se esistono azioni che possano limitare i danni che la violazione potrebbe causare (i.e. riparazione fisica di strumentazione; utilizzo dei file di back up per recuperare dati persi o danneggiati; isolamento/chiusura di un settore compromesso della rete; cambio dei codici di accesso… ecc.);

- una volta identificate tali azioni, quali siano i soggetti che devono agire per contenere la violazione;

- se sia necessario notificare la violazione all'Autorità Garante per la Protezione dei dati personali (ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche);

- se sia necessario comunicare la violazione agli interessati (ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche).

Al fine di individuare la necessità di notificazione all'Autorità Garante e di comunicazione agli interessati, il Titolare del trattamento valuterà la gravità della violazione facendo una Valutazione del Rischio connesso al Data Breach che dovrà essere esaminata in debita considerazione dei principi e le indicazioni di cui all'art. 33 GDPR.

Se, infatti, gli obblighi di notifica all'Autorità di Controllo scaturiscono dal superamento di una soglia di rischio semplice, l'art. 34 GDPR prevede, invece, che l'obbligo di comunicazione agli interessati sia innescato dal superamento di un rischio elevato.

Step 3: Eventuale notifica all'Autorità Garante competente

A seguito delle determinazioni sul punto raggiunte e solo qualora si debba ritenere che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche interessate, il Responsabile della Protezione dei Dati – con lo specifico contributo delle professionalità coinvolte - supporta il Titolare del trattamento nella predisposizione della notificazione all'Autorità Garante,

utilizzando a tal fine apposito modulo reso disponibile dalla stessa Autorità Garante sul proprio sito web istituzionale (https://www.garanteprivacy.it/data-breach). Detta notificazione deve essere inviata senza ingiustificato ritardo e, ove possibile, entro 72 ore da intendersi decorrenti dal momento in cui il Titolare sia venuto a conoscenza della violazione di dati, ovvero da quanto il Titolare abbia raggiunto un ragionevole grado di certezza sul fatto che l'incidente di sicurezza comporti una violazione di dati personali.

Oltre il termine delle 72 ore la notifica deve essere corredata delle ragioni del ritardo.

E' comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il Titolare venga a conoscenza a seguito di ulteriori indagini e verifiche sull'evento.

La scelta e le motivazioni che hanno condotto a non notificare l'evento devono risultare documentate a cura del Responsabile della Protezione dei Dati e delle professionalità coinvolte.

Step 4: Eventuale comunicazione agli interessati

Una volta valutata la necessità di effettuare la comunicazione della violazione dei dati a coloro dei cui dati si tratta, sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, Marrelli Health dovrà provvedervi, senza ingiustificato ritardo.

Quanto al contenuto di tale comunicazione, il Titolare del trattamento dovrà:

- comunicare il nome e i dati di contatto del Titolare o un suo Responsabile;
- descrivere le probabili conseguenze della violazione dei dati personali;
- 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, se del caso, per attenuarne i possibili effetti negativi.

Quanto alle modalità di comunicazione, caso per caso, il Titolare del trattamento o un suo delegato dovranno sempre privilegiare la modalità di comunicazione diretta con i soggetti interessati (quali e-mail, SMS o messaggi diretti). Il messaggio dovrà essere comunicato in maniera evidente e trasparente. Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, allora si potrà utilizzare una comunicazione pubblica, che dovrà essere ugualmente efficace nel contatto diretto con l'interessato.

Step 5: Documentazione della violazione

Indipendentemente dalla valutazione circa la necessità di procedere a notificazione e/o comunicazione della violazione di Data Breach, ogni qualvolta si verifichi un incidente comunicato dai Destinatari, Marrelli Health sarà tenuta a documentarlo.

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

Gestione del data breach esterno alla struttura

Ogni Responsabile esterno del trattamento (Fornitore/Ditta) – incaricato dal Titolare ad effettuare attività di trattamento dati in nome e per suo conto sulla base di specifico contratto a tal fine stipulato tra le parti – qualora venga a conoscenza di un potenziale caso di data breach, ne dà avviso senza ingiustificato ritardo alla Marrelli Health, inviando alla stessa una comunicazione a mezzo mail all'indirizzo rpd@marrellihealth.it.

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

Il DPO effettua a sua volta una valutazione dell'evento avvalendosi del supporto e della collaborazione di professionalità interne all'Azienda, necessarie per la corretta analisi di contesto.

A seguito delle determinazioni sul punto raggiunte e solo qualora si debba ritenere che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche interessate, il Responsabile della Protezione dei Dati – con lo specifico contributo delle professionalità coinvolte - supporta il Titolare del trattamento nella predisposizione della notificazione all'Autorità Garante. Detta notificazione deve essere inviata senza ingiustificato ritardo e, ove possibile, entro 72 ore da intendersi decorrenti dal momento in cui il Titolare sia venuto a conoscenza della violazione di dati, ovvero da quanto il Titolare abbia raggiunto un ragionevole grado di certezza sul fatto che l'incidente di sicurezza comporti una violazione di dati personali.

Oltre il termine delle 72 ore la notifica deve essere corredata delle ragioni del ritardo.

E' comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il Titolare venga a conoscenza a seguito di ulteriori indagini e verifiche sull'evento.

La scelta e le motivazioni che hanno condotto a non notificare l'evento devono risultare documentate a cura del Responsabile della Protezione dei Dati e delle professionalità coinvolte.

ALLEGATI

MOD 01 Data Breach - Modulo per la segnalazione di un sospetto caso di data breach

MOD 02 Data Breach - Registro delle violazioni