Gestione di una violazione di dati personali *(DATA BREACH) della LDB Medical Care*

SOMMARIO

1. - SCOPO

La presente istruzione ha la finalità di indicare a tutto il personale operante presso la LDB Medical Care, la modalità di gestione di un *data breach* - ovvero di un evento di violazione dei dati personali - nel rispetto dei principi e delle disposizioni contenute nel Regolamento (UE) 2016/679 sulla protezione dei dati (di seguito denominato "GDPR").

Nell'ambito dell'istruzione vengono esplicitate le regole per garantire la realizzabilità tecnica e la sostenibilità organizzativa della gestione del *data breach*, con particolare riferimento ai seguenti aspetti:

- Modalità e profili di segnalazione al Titolare del trattamento per il tramite del Responsabile della protezione dei dati
- Valutazione dell'evento verificatosi
- Modalità e profili di segnalazione all'Autorità Garante
- Eventuale comunicazione agli interessati.

2. - CAMPO DI APPLICAZIONE

In presenza di possibili violazioni dei dati personali – siano essi contenuti in banche informatiche o cartacee – l'istruzione si applica a tutti i soggetti che, a vario titolo, svolgono attività nell'ambito delle diverse articolazioni organizzative della LDB Medical Care.

3. - RIFERIMENTI NORMATIVI E DOCUMENTALI

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)";
- Decreto Legislativo 10 agosto 2018, n. 101 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)";
- Linee Guida WP 250 del Gruppo di lavoro Articolo 29 sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679 - adottate il 3 ottobre 2017 ed emendate il 6 febbraio 2018;
- Provvedimento del Garante del 30 luglio 2019 (9126951) sulla notifica delle violazioni dei dati personali (*data breach*);
- Atto del Titolare per la Nomina del Responsabile della Protezione dei dati (DPO)";
- Atto del Titolare per la Nomina degli Autorizzati e dei Referenti";
- Atto del Titolare per la individuazione dei Responsabili del trattamento dei dati".

4. - DEFINIZIONI E TERMINOLOGIA

***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 (art. 4, n. 1 del GDPR).

***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, n. 2 del GDPR).

***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, n. 6 del GDPR).
***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, n. 7 del GDPR).
Titolare del trattamento è la LDB Medical Care nella persona fisica dell'Amministratore Unico, in qualità di legale rappresentante.
***Responsabile della protezione dei dati (RPD - DPO)*:** la persona fisica nominata dal Titolare del trattamento, ai sensi degli artt. 37-39 del GDPR.
***Autorizzato al trattamento dei dati*:** tutte le unità di personale operanti presso le diverse Direzioni/ Uffici/Unità Operative della LDB Medical Care che, ai sensi dell'art. 29 del GDPR, effettuano attività di trattamento di dati personali sotto la diretta autorità e vigilanza del Titolare e dei Responsabili del Trattamento, e al quale sono state fornite istruzioni in tal senso.
Il predetto personale è stato, parimenti, designato con Nomina del Titolare.
***Responsabile del trattamento dei dati*:** la persona fisica o giuridica (esterna alla LDB Medical Care) l'autorità pubblica, il servizio o altro organismo che – ai sensi dell'art. 28 del GDPR – tratta dati personali per conto del Titolare del trattamento sulla base di apposito atto di nomina.
***Interessato*:** la persona fisica, identificata o identificabile, alla quale i dati si riferiscono.
***Violazione dei dati personali (data breach)*:** 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 (art. 4, n. 12 del GDPR).

5. - PROCESSO/MODALITÀ OPERATIVE

5.1 Premessa

Una violazione dei dati personali (*data breach*) può - se non gestita in modo adeguato e tempestivo - provocare danni fisici, materiali o immateriali alle persone fisiche interessate, quali, a titolo esemplificativo, perdita di controllo dei dati personali che le riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione di identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale rilevante per la persona fisica interessata.

5.2 - Gestione del *data breach* all'interno della struttura

Ogni operatore della LDB Medical Care autorizzato a trattare dati personali, qualora venga a conoscenza di un potenziale caso di ***data breach interno***, avvisa tempestivamente il Responsabile del trattamento a cui il medesimo afferisce (Responsabile IT, Medico Competente, Commercialista, Consulente del Lavoro, Specialisti incaricati).

Il Responsabile del trattamento - valutato l'evento - se ritiene confermata la segnalazione di potenziale *data breach interno*, ne fornisce comunicazione al Responsabile della Protezione dei dati (DPO) a mezzo e mail utilizzando, a tal fine, l'allegato modulo (Modello 1 data breach interno).

Il DPO effettua a sua volta una valutazione dell'evento avvalendosi del supporto e della collaborazione delle Direzioni, degli Autorizzati e dei Referenti Privacy, necessario alla 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, utilizzando a tal fine apposito modulo reso disponibile dalla stessa Autorità Garante sul proprio sito *web* istituzionale.[1] Detta notifica 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.

5.3 - 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 esterno***, ne dà avviso senza ingiustificato ritardo della LDB Medical Care, inviando alla stessa una comunicazione a mezzo PEC all'indirizzo ldbmedicalcare@pec.it e utilizzando a tal fine l'allegato modulo (Modello 2 data breach esterno) che dovrà, pertanto, essere accluso all'atto di nomina stesso.

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 delle Direzioni, degli Autorizzati e dei Referenti Privacy, necessario alla 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 DPO – con lo specifico contributo delle professionalità coinvolte - supporta il Titolare del trattamento nella predisposizione della notificazione all'Autorità Garante. Detta notifica 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 DPO e delle professionalità coinvolte.

5.4 - Modalità di comunicazione agli interessati

Nel caso in cui dal *data breach* possa derivare un rischio elevato per i diritti e le libertà delle persone fisiche interessate, queste ultime devono essere informate senza ingiustificato ritardo al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali pregiudizi derivanti dalla violazione. Il DPO supporta il Titolare del trattamento nella predisposizione della comunicazione all'interessato/agli interessati, da inviarsi nei tempi e con le modalità che il Titolare stesso, sempre attraverso la funzione di consulente del DPO, individuerà come più opportuna anche tenendo conto

[1] https://www.garanteprivacy.it/regolamentoue/databreach

di eventuali indicazioni all'uopo fornite dall'Autorità Garante. La comunicazione descriverà con linguaggio semplice e chiaro la natura della violazione dei dati personali, le probabili conseguenze derivanti dalla stessa, oltreché le relative misure individuate per porvi rimedio.

5.5 - Registro delle violazioni

Presso l'Ufficio del DPO è istituito il registro delle violazioni nell'ambito del quale vengono documentati tutti gli eventi di *data breach* occorsi presso la LDB Medical Care dall'entrata in vigore del GDPR e il cui aggiornamento avviene a cura del DPO per conto del Titolare.

A tal fine si allega alla presente istruzione relativo modello del predetto registro (Modello 3 - Registro delle Violazioni).

Roma, 1 febbraio 2022

Il Data Protection Officer
Dr. Alessandro Pirrone