Sistema Socio Sanitario

Regione Lombardia

ATS Montagna

Regolamento per la gestione della violazione dei dati personali (*data breach*) di titolarità dell'ATS della Montagna

(Regolamento UE 679/2016)

Indice

Art. 1
Oggetto

1. Il presente Regolamento disciplina le modalità di gestione da parte di ATS della Montagna delle violazioni dei dati personali (c.d. *data breach*) al fine di date attuazione alla previsione degli artt. 33 e 34 del Reg. UE 679/2016.

Art. 2
Definizioni

1. Ai fini del presente Regolamento, per "**violazione dei dati**" si intende «*La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*» (Art. 4 comma 1 n. 12 Reg. UE 679/2016). La violazione dei dati, come chiarito dallo stesso Garante per la Protezione dei Dati Personali nel documento "**Violazioni di dati personali (*data breach),* in base alle previsioni del Regolamento (UE) 2016/679", aggiornato al 5 agosto 2019,** è quindi un evento che «*può compromettere la riservatezza, l'integrità o la disponibilità di dati personali*».

2. La violazione di dati riguarda tanto le ipotesi di trattamenti eseguiti con mezzi informatici quanto i trattamenti eseguiti con strumenti cartacei. A titolo esemplificativo, possibili esempi di violazione di dati sono:

   - l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;

   - il furto o la perdita di dispositivi informatici contenenti dati personali;

   - la deliberata alterazione di dati personali;

   - l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;

   - la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità. Tra queste ipotesi rientra anche la distruzione accidentale di campioni biologici conservati nel Laboratorio;

   - la modifica irreversibile dei dati personali con la conseguenza di rendere indisponibile i dati medesimi all'interessato qualora ne facesse richiesta esercitando i diritti previsti dagli artt. 15 e ss. del Reg. UE 679/2016;

   - la divulgazione non autorizzata dei dati personali (ad es. invio di e-mail contenente dati personali a destinatario errato…).

Si ritiene opportuno, altresì, esplicitare nel seguito alcune definizioni, utili ai fini dell'applicazione del presente Regolamento:

definizione	descrizione
Titolare (Art. 4 comma 1 n. 7	E' la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e

Reg. UE 679/2016)	i mezzi del trattamento dei dati personali; (….)
Interessato (art. 4 comma 1 n. 1 Reg. UE 679/2016)	Persona identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, economica, culturale o sociale.
Destinatario (Art. 4 comma 1 n. 9 Reg. UE 679/2016)	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerati destinatari.
Terzo (Art. 4 comma 1 n. 10 Reg. UE 679/2016)	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.
Trattamento (art. 4 comma 1 n. 2 Reg. UE 679/2016)	Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.
Dato personale (Art. comma 1 n. 1 Reg. UE 679/2016)	Qualunque informazione relativa a persona fisica identificata o identificabile («interessato»).
Dati biometrici (Art. comma 1 n. 14 Reg. UE 679/2016)	I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, biologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
Dati relativi alla salute (Art. comma 1 n. 15 Reg. UE 679/2016)	I dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria che rivelino informazioni relative al suo stato di salute.
Archivio (art. 4 comma 1 n. 6 Reg. UE n. 679/2016)	Qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale sistema sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico
Categorie particolari di dati (art. 9 Reg. UE 679/2016)	Sono i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
Comunicazione (Art. 2-ter comma 4 lett. A del D.Lgs. n. 196/2003 e s.m.i.)	Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione Europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione Europea, dalle

	persone autorizzate, ai sensi dell'art. 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione.
Diffusione (Art. 2-ter comma 2 lett. B del D.Lgs. n. 196/2003 e s.m.i.)	Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Base giuridica del trattamento	Condizione di liceità del trattamento dei dati personali riconducibile ad una delle ipotesi di cui all'art. 6 del Reg. UE 679/2016 e dal D.Lgs. n. 196/2003 e s.m.i.

Per tutte le definizioni non espressamente richiamate nel presente Regolamento si rimanda al Reg. UE 679/2016 ed al D.Lgs. n. 196/2003 e s.m.i. nonché ai provvedimenti dell'Autorità Garante per il trattamento dei dati personali.

Art. 3
Gestione della violazione dei dati *(data breach*) all'interno dell'ATS.

1. Gli operatori devono trattare i dati personali nel rispetto dei principi fissati dall'art. **5 del Reg. UE 679/2016**. In particolare, perché un trattamento possa definirsi conforme alla vigente normativa, i dati devono essere:

   - trattati in modo lecito, corretto e trasparente;
   - raccolti per finalità determinate, esplicite e legittime e trattati in modo che non sia incompatibile con le predette finalità (principio della "limitazione delle finalità");
   - adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (principio della "limitazione delle finalità");
   - esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono tratti (principio della c.d. "esattezza");
   - conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. I dati personali possono essere conservati per un periodo più lungo a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'art. 89 par. 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato ("limitazione della conservazione");
   - trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (principi della "integrità e riservatezza").

2. I dipendenti/collaboratori dell'ATS che vengano a conoscenza di violazioni di dati personali o abbiano la percezione che una data situazione possa integrare gli estremi di una "*violazione di dati*" come sopra definita, devono segnalare formalmente la suddetta circostanza al proprio Dirigente Responsabile/Referente che, a sua volta, qualora non sia stato designato Responsabile interno del trattamento, deve darne immediata comunicazione formale al Responsabile interno del trattamento.

3. Il Responsabile interno del trattamento, ricevuta la comunicazione di cui sopra e acquisite le informazioni valutare come necessarie, trasmetterà tempestivamente al Titolare del trattamento una relazione sull'evento oggetto di segnalazione al fine di consentirne la relativa valutazione anche ai fini dell'adozione delle misure di contenimento delle conseguenze.
4. La comunicazione al Titolare deve essere eseguita entro 24 ore dalla prima segnalazione (dell'operatore) al fine di consentire al Titolare medesimo il rispetto della tempistica, prevista dal Regolamento UE 679/2016 per la notifica (72 h).
5. La relazione di cui sopra dovrà contenere il seguente contenuto minimo:

    - una descrizione della violazione dei dati personali oggetto di segnalazione che individui, ove possibile:

    a) la natura della violazione e le cause della stessa;

    - una descrizione delle possibili conseguenze della violazione dei dati personali anche in termini di gravità e le misure tecniche e organizzative che potrebbero essere adottate per rimediare alla violazione dei dati e contenere le conseguenze della stessa;
    - le categorie e il numero (anche approssimativo) delle persone interessate;

    b) le categorie e il volume (anche approssimativo) di dati personali e la descrizione dei dati medesimi;

    c) le misure tecniche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture

Art. 4

La gestione della violazione all'esterno dell'ATS e cioè presso i soggetti che eseguono un trattamento per conto dell'ATS della Montagna (Responsabili del trattamento nominati ai sensi dell'art. 28 Reg. UE 679/2016).

1. Ai sensi dell'art. 33 comma 2 del Regolamento (UE) 67972016, il Responsabile del trattamento ha l'obbligo di segnalare senza giustificato ritardo al Titolare del trattamento la violazione dei dati personali di cui sia venuto a conoscenza. La suddetta comunicazione dovrà essere inviata all'indirizzo PEC dell'ATS della Montagna.
2. A tal fine, il Responsabile del trattamento redige una relazione che abbia il contenuto previsto dal precedente art. 3 e garantisce la piena collaborazione al Titolare nella gestione della violazione rilevata.
3. L'obbligo di cui alla presente disposizione deve essere richiamato:

    - negli atti di gara;
    - nelle istruzioni operative impartite al Responsabile del trattamento e costituenti parte integrante del contratto.

4. La comunicazione, inviata dal Responsabile del trattamento al Titolare, viene assegnata altresì al RUP e al DEC per i successivi adempimenti anche connessi all'istruttoria di cui al successivo art. 5.

Art. 5

La valutazione della violazione e la notifica al Garante per la Protezione dei Dati Personali

1. Il Titolare, una volta ricevuta la relazione di cui agli artt. 3 e 4 del presente Regolamento deve eseguire le relative valutazioni del caso, supportato dal Responsabile della Protezione dei Dati, dal Responsabile interno del trattamento e, nei casi in cui la possibile violazione dei dati riguardi trattamenti eseguiti con strumenti informatici, dal Responsabile dei Servizi informativi. Il Titolare sarà altresì supportato dal RUP e dal DEC nel caso in cui la violazione dei dati sia avvenuta all'esterno dell'ATS e cioè presso il responsabile del trattamento, nominato ai sensi dell'art. 28 Reg. UE 679/2016.
2. L'istruttoria di cui sopra sarà finalizzata ad accertare se la violazione rilevata comporti o meno un rischio per i diritti e le libertà delle persone fisiche e quindi se la stessa possa produrre «…*effetti avversi i significativi sugli interessati, causando danni fisici, materiali o immateriali*» (cfr: Garante per la Protezione dei Dati Personali, documento "**Violazioni di dati personali (*data breach),* in base alle previsioni del Regolamento (UE) 2016/679", aggiornato al 5 agosto 2019).**
3. A meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, senza giustificato ritardo e, se possibile **entro 72 ore** dal momento in cui ne è venuto a conoscenza, il Titolare ha l'obbligo di notificare la violazione rilevata al Garante per il Trattamento dei Dati Personali (art. 33 comma 1 Reg. UE 679/2016).
4. La comunicazione in argomento deve contenere almeno le informazioni richieste dal comma 3 del citato art. 33 del Reg. (UE) 679/2016. La stessa sarà redatta utilizzando il modello allegato al provvedimento del Garante per la Protezione dei dati Personali del 30 luglio 2019, reperibile sul sito istituzionale del Garante Privacy (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9128501).
5. La notifica in argomento non deve includere i dati personali oggetto di violazione e, pertanto, non dovranno essere forniti i nomi dei soggetti interessati dalla violazione e/o dati che possano indirettamente identificare gli stessi.
6. La notifica al Garante Privacy, sottoscritta dal titolare, deve essere eseguita tramite posta elettronica certificata all'indirizzo, attualmente indicato nel seguente: **protocollo@pec.gpdp.it**

Art. 6

La documentazione delle violazioni

1. Il Titolare del trattamento, a prescindere dalla notifica al Garante Privacy, documenta tutte le violazioni dei dati personali. A partire dall'adozione del presente Regolamento, le violazioni dei dati saranno annotate in un apposito Registro (Registro delle violazioni dei dati personali), redatto secondo lo schema allegato al presente Regolamento (All.to 1) e conservato a cura del Responsabile della Protezione dei dati (R.P.D.).
2. Il Titolare, ove ragioni organizzative lo rendessero necessario, potrà delegare un soggetto diverso dal R.P.D. per la tenuta e alimentazione del Registro in argomento.
3. Ogni evento registrato dovrà essere contraddistinto da un numero progressivo (ad es. 1/2020).

Art. 7

La comunicazione agli interessati

1. Ai sensi dell'art. 34 del Reg. UE 679/2016, quando la violazione dei dati personali è «*suscettibile di presentare un rischio elevato per i diritti e le libertà fondamentali delle persone fisiche, il Titolare del trattamento comunica la violazione all'interessato senza giustificato ritardo*».

2. La comunicazione all'interessato deve avere almeno i contenuti di cui al comma 3 lett. B) C) e D) del citato art. 33 e quindi, oltre alla descrizione con linguaggio semplice e chiaro della violazione rilevata, deve recare:

   - il nome e i dati di contatto del Responsabile della Protezione dei dati Personali (R.P.D.) dell'ATS;
   - una descrizione delle possibili conseguenze della violazione dei dati personali;
   - la descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e, ove possibile, le misure adottate per mitigare eventuali effetti negativi.

3. Ai sensi dell'art. 34 comma 3 del Reg. UE 679/2016, non è richiesta la comunicazione all'interessato quando:

   - 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;
   - il Titolare del trattamento ha successivamente adottato le misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
   - la 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.