UNIMORE

UNIVERSITÀ DEGLI STUDI DI
MODENA E REGGIO EMILIA

Procedura di gestione della violazione dei dati personali

Data Breach Policy

Art. 30 del “Regolamento in materia di protezione dei dati personali”

Versione 1.0 del 22 marzo 2019

Sommario

1 - Introduzione

Per violazione di dati personali deve intendersi ogni infrazione alla sicurezza 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 dall'Università degli studi di Modena e Reggio Emilia.

Lo scopo di questo documento è disegnare un flusso di procedure per la gestione delle anzidette violazioni.

Le procedure sono rivolte a tutti coloro che, in Ateneo, trattano a qualsiasi titolo dati personali, quindi:

- i lavoratori dipendenti ed il personale che, a prescindere dal tipo di rapporto contrattuale in essere, ha accesso ai dati personali trattati nel corso di prestazioni richieste per conto dell'Ateneo;
- qualsiasi soggetto, persona fisica o persona giuridica, che, in ragione del rapporto contrattuale in essere con l'Ateneo, abbia accesso ai dati e agisca in qualità di Responsabile del trattamento (art. 28 GDPR) o di autonomo Titolare.

Il rispetto delle procedure è obbligatorio per tutti i soggetti coinvolti.

2 - Titolare del trattamento dati

Titolare del trattamento dati (o Titolare) è l'Università degli studi di Modena e Reggio Emilia

3 - Responsabile della protezione dei dati

Il Responsabile per la Protezione dei Dati (o DPO) nominato dall'Ateneo, email: dpo@unimore.it, dpo@pec.unimore.it

4 - Recapito per la segnalazione della violazione

Ogni violazione deve essere prontamente segnalata all'indirizzo segnalazioni.privacy@unimore.it

5 - Procedura di gestione

La gestione di una violazione dei dati personali prevede le seguenti fasi:

1. Rilevazione e segnalazione della violazione;
2. Raccolta informazioni e comunicazione della violazione;
3. Contenimento, recovery e risk assessment;
4. Notifica all'Autorità Garante (solo se necessaria);
5. Comunicazione agli interessati coinvolti (solo se necessaria);
6. Documentazione della violazione (Registro dei Data Breach).

Le singole fasi sono meglio descritte nei seguenti paragrafi.

5.1 - Rilevazione e segnalazione della violazione

Chi può segnalare
Tutto il personale, i collaboratori, gli studenti, i fornitori o chiunque venga a conoscenza di una possibile violazione dei dati personali propri o altrui
A chi segnalare
Al Responsabile della Struttura o al Referente Informatico della Struttura
Quando
Appena se ne viene a conoscenza
Come
Utilizzando le vie più brevi (telefono, email, ecc.)

5.2 - Raccolta informazioni e comunicazione della violazione

Chi deve raccogliere e comunicare
Il Responsabile della Struttura o il Referente Informatico della Struttura
A chi inviare la comunicazione
Al DPO e al Gruppo Sicurezza ICT
Quando
Appena ricevuta la segnalazione
Come
Inoltrando il modulo di raccolta informazioni (Allegato A) debitamente compilato tramite l'indirizzo email segnalazioni.privacy@unimore.it

5.3 - Contenimento, recovery e risk assessment

Chi agisce
Il DPO, d'intesa con il Titolare, il Gruppo Sicurezza ICT e i Responsabili delle Strutture coinvolte
Destinatari
I soggetti incaricati di svolgere le attività di contenimento e recovery
Quando
Nei termini indicati nell'attività di risk assessment indicati dal DPO
Come
Valutazione dei rischi legati alla violazione accertata. Valutazione della necessità di comunicazione della violazione al Garante e agli interessati e, in caso affermativo, informazione al Titolare affinché venga inoltrata la notifica al Garante. Individuazione dei soggetti incaricati delle attività di contenimento e recovery. Definizione delle operazioni da svolgere e dei tempi di attuazione Comunicazione delle operazioni da effettuare ai soggetti incaricati Eventuali operazioni di verifica di efficacia delle misure di contenimento e recovery stabilite ed eventuale prosecuzione delle indagini a seguito di indicazioni da parte del Garante o del Titolare

5.4 - Notifica all’Autorità Garante (solo se necessaria)

Chi la effettua
Il Titolare, sentito il DPO
A chi viene inoltrata
Al Garante
Quando
Entro 72 ore dal momento in cui la violazione è rilevata
Come
Mediante la modulistica e i canali di comunicazione predisposti dal Garante

5.5 - Comunicazione agli interessati coinvolti (solo se necessaria)

Chi la effettua
Il Titolare, sentito il DPO
A chi viene inoltrata
Alle persone fisiche i cui dati sono stati violati
Quando
Nel più breve tempo possibile, senza ingiustificato ritardo
Come
Mediante comunicazione diretta o mediante pubblicazione in sito a loro accessibile

5.6 - Documentazione della violazione (Registro dei Data Breach)

Chi compila il documento
Il DPO insieme al responsabile della Struttura coinvolta nella violazione
Quando
Ogni volta che riceve la segnalazione di una violazione
Come
Registrazione della violazione nel Registro dei Data Breach con la descrizione della violazione, delle azioni intraprese e annotazione dei successivi aggiornamenti se necessario proseguire le indagini. Registrazione della risposta del Garante e delle eventuali prescrizioni in essa contenute. Registrazione della chiusura dell'incidente se non necessita di ulteriori indagini oppure indicazione della prosecuzione delle indagini.

Allegato A - Modulo per la raccolta informazioni

In caso di scoperta di un data breach:

1. **Informare immediatamente il Responsabile della struttura di afferenza e/o il Referente Informatico**
2. **Il Responsabile della Struttura o il Referente Informatico devono compilare il modulo seguente e inviarlo via mail a segnalazioni.privacy@unimore.it**

Data della violazione

- ❑ tra il __ / __ / ____ e il __ / __ / ____
- ❑ in un tempo non ancora determinato
- ❑ è possibile che sia ancora in corso

Luogo della violazione[1]

Riferimenti di chi segnala la violazione [2]

Descrizione dell'evento in breve[3]

Banche dati oggetto di data breach e breve descrizione dei dati personali trattati

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: _____

Tipo di dati oggetto della violazione

- ❑ Dati anagrafici
- ❑ Numero di telefono (fisso o mobile)
- ❑ Indirizzo di posta elettronica
- ❑ Dati di accesso e di identificazione (user name, password, altro)
- ❑ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)
- ❑ Altri dati di personali (sesso, data di nascita, età, ...), dati sensibili e giudiziari
- ❑ Altro: _____

Dispositivo oggetto della violazione

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

[1] Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili

[2] Indicare nome, cognome, email, telefono se personale interno, ragione sociale se personale esterno

[3] Riportare una descrizione sintetica del data breach, dei sistemi di elaborazione o memorizzazione dei dati coinvolti, la loro ubicazione, le categorie e il numero approssimativo di persone interessate dalla violazione