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 “GDPR”

Versione 1.0 del 22 Marzo 2019
Versione 2.0 del 21 Giugno 2024

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.

In particolare, le tipologie di violazioni declinate dalla norma sono sintetizzabili come:

- Violazione della riservatezza che si verifica in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali;
- Violazione dell'integrità che si verifica in caso di alterazione non autorizzata o accidentale dei dati personali;
- Violazione della disponibilità che si verifica in caso di perdita o distruzione di dati personali accidentale o illecita o di impossibilità di accesso ai dati personali da parte dei soggetti autorizzati.

Una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione di queste. Lo scopo di questo documento è disegnare un flusso di procedure e di comunicazioni per la gestione delle anzidette violazioni, anche alla luce di quanto definito nella Procedura "POL01 GESTIONE DEGLI INCIDENTI DI SICUREZZA".

La presente policy è rivolta 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 – Definizioni

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato").

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.

Interessato: persona fisica identificata o identificabile al quale si riferiscono i dati personali. 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.

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.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, o altro organismo che tratta dati personali per conto del titolare del trattamento.

Data Protection Officer (DPO): il soggetto fisico o giuridico individuato come Responsabile della protezione dei dati personali ai sensi del GDPR.

Autorizzato al trattamento: la persona fisica, espressamente designata, che opera sotto l'autorità del titolare del trattamento o del responsabile del trattamento, con specifiche mansioni e funzioni connesse al trattamento dei dati personali.

3 - Titolare del trattamento

Il Titolare del trattamento dati (o Titolare) è l'Università degli studi di Modena e Reggio Emilia. Si evidenzia che, nell'adempimento di attività istituzionali, l'Università degli Studi di Modena e Reggio Emilia, può essere nominata **Responsabile del trattamento** in virtù di idoneo atto di nomina. La presente Procedura è applicabile anche ai trattamenti realizzati in qualità di Responsabile del trattamento.

4 - Responsabile della protezione dei dati

Il Responsabile per la Protezione dei Dati (o DPO) nominato dall'Ateneo è reperibile agli indirizzi e-mail: dpo@unimore.it, dpo@pec.unimore.it

5 - Recapito per la segnalazione della violazione

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

6 - Procedura di gestione

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

1. Rilevazione e segnalazione della violazione. In particolare, tale fase può svilupparsi secondo due canali alternativi:
    A. Rilevazione e segnalazione da parte di: personale, collaboratori, studenti, fornitori o chiunque venga a conoscenza di una possibile violazione dei dati personali propri o altrui;
    B. Rilevazione e segnalazione da parte del CSIRT.
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.

6.1.A - 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, e-mail, ecc.)

6.1.B - Rilevazione e segnalazione della violazione da parte del CSIRT

L'Università ha adottato la Procedura "POL01 GESTIONE DEGLI INCIDENTI DI SICUREZZA" che prevede un ruolo centrale del Gruppo Computer Security Incident Response Team ("CSIRT") e del Gruppo ICT nella gestione degli incidenti di sicurezza.

Nello svolgimento delle proprie funzioni, il CSIRT può rilevare o può ricevere segnalazioni di incidenti di sicurezza che possono determinare una violazione di dati personali. Per tale motivo, è opportuno prevedere, nella presente procedura, un ulteriore canale di rilevazione e segnalazione (alternativo rispetto a quello descritto al precedente punto 6.1.A).

Nel solo caso descritto al presente punto, il flusso di gestione passerà dalla fase 6.1.B direttamente alla fase 6.3.

Chi può segnalare

Il Responsabile Sicurezza dopo essere stato informato dal CSIRT in merito ad una segnalazione pervenuta tramite i canali previsti dalla Procedura "POL01 GESTIONE DEGLI INCIDENTI DI SICUREZZA".

A chi segnalare

Al DPO.

Quando

Tempestivamente dopo aver ricevuto la conferma che l'incidente di sicurezza presenta profili potenzialmente rilevanti in tema di protezione dei dati personali.

Come

Scrivendo a mezzo mail all'indirizzo dpo@unimore.it. In particolare, il Responsabile Sicurezza avrà cura di:

- utilizzare la seguente dicitura come oggetto della mail "!! POTENZIALE DATA BREACH – COMUNICAZIONE GRUPPO SICUREZZA ICT",
- compilare e allegare (anche in termini approssimativi, in mancanza di una conoscenza specifica degli elementi) il modulo di raccolta informazioni (Allegato A). Inoltre, è fondamentale indicare, anche nel corpo della mail, la data in cui il Responsabile Sicurezza ha avuto conferma del coinvolgimento dei dati personali;
- mettere a disposizione un contatto telefonico affinché possa intervenire un confronto per le vie brevi nel minor tempo possibile.

6.2 - 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 all'indirizzo e-mail segnalazioni.privacy@unimore.it

(*) NOTA OPERATIVA PER il DPO

Nella prassi potrebbe accadere che della potenziale violazione di dati personali sia informato il solo DPO. In tal caso, laddove ritenga che il potenziale Data Breach sia determinato da un incidente di sicurezza, il DPO dovrà informare il Gruppo ICT procedendo come segue.

I. Il DPO dovrà coinvolgere il Gruppo ICT, nella persona del Responsabile Sicurezza, condividendo tutte le informazioni ricevute;
II. In particolare, il DPO avrà cura di utilizzare la seguente dicitura come oggetto della mail "!! POTENZIALE DATA BREACH – INCIDENTE SICUREZZA COMUNICAZIONE DPO".

6.3 - 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.

6.4 - Notifica all'Autorità Garante (solo se necessaria)

Chi la effettua
Il Titolare, sentito il DPO.
A chi viene inoltrata
All'Autorità di controllo, ossia il Garante per la protezione dei dati personali.
Quando
Entro 72 ore dal momento in cui il titolare del trattamento viene a conoscenza della violazione di dati personali. NB: Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, deve essere corredata dei motivi del ritardo.
Come
Mediante la modulistica e i canali di comunicazione predisposti dal Garante, reperibili sul sito istituzionale: www.gpdp.it

6.5 - 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.

6.6 - Documentazione della violazione (Registro dei Data Breach)

Chi compila il documento
Il DPO insieme al responsabile della Struttura coinvolta nella violazione ovvero, se coinvolti, al CSIRT e al Gruppo ICT
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, e-mail, 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