UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

# PROCEDURA DI DATA BREACH

# Procedura da adottare in caso di violazione dei dati personali

Art. 4, 33, 34 del Regolamento UE 679/2016

Versione aggiornata al 5 NOVEMBRE 2018

## 1. Premesse

Il presente documento è redatto in adempimento a quanto previsto dal Regolamento UE 679/2016 (di seguito GDPR) in materia di violazione del dato personale.

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.*

Il GDPR definisce violazione del dato personale o DATA BREACH ogni "*violazione di 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* "dal Titolare del trattamento.

## 2. Scopo e ambito di applicazione

Questa procedura è redatta al fine di tutelare le persone, i dati e le informazioni e documentare i flussi per la gestione delle violazioni dei dati personali trattati dall'Università degli Studi di Bari Aldo Moro in qualità di Titolare del trattamento (di seguito Titolare del trattamento).

La procedura definisce le modalità e le responsabilità per:

- Identificare la violazione
- Analizzare le cause della violazione
- Definire le misure da adottare per rimediare alla violazione dei dati personali e attenuarne i possibili effetti negativi
- Registrare le informazioni relative alla violazione, le misure identificate e l'efficacia delle stesse
- Notificare una violazione di dati personali al Garante, nel caso in cui la violazione comporti un rischio per i diritti e la libertà delle persone fisiche
- Comunicare una violazione dei dati personali all'interessato nel caso in cui il rischio fosse elevato.

Questa procedura si applica a qualunque attività svolta dal Titolare del trattamento con particolare riferimento a tutti gli archivi e/o documenti cartacei e a tutti i sistemi informativi attraverso cui sono trattati dati personali, anche con il supporto di fornitori esterni.

## 3. A chi si rivolge questa procedura?

Questa procedura è rivolta a **tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento**, in qualsiasi formato e con qualsiasi mezzo, quali:

• i 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;

• qualsiasi soggetto (persona fisica o persona giuridica) 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.

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.

## 4. Perché definire una procedura di gestione delle violazioni di dati personali (data breach)

L'**Università degli Studi di Bari Aldo Moro**, ad integrazione delle procedure già adottate in materia di protezione dei dati personali ai sensi della legislazione vigente, ha predisposto azioni da attuare nell'eventualità in cui si presentino violazioni concrete, potenziali o sospette di dati personali trattati dall'Ateneo in qualità di Titolare, al fine di:

- evitare rischi per i diritti e le libertà degli interessati
- evitare danni economici all'Ateneo
- notificare la violazione (data breach) al Garante e/o agli interessati, nei tempi e nei modi previsti dalla normativa europea,
- non incorrere nelle sanzioni previste dal GDPR per omessa notifica
- minimizzare l'impatto della violazione e prevenire che si ripeta.

## 5. Procedura di gestione della violazione dei dati personali (data breach)

Nel caso in cui uno dei soggetti di cui al punto 4 del presente documento venga a conoscenza di una concreta, potenziale o sospetta violazione di dati personali, dovrà essere attivato il flusso di adempimenti di seguito descritti e schematizzati.

La gestione della violazione concreta, potenziale o sospetta prevede l'attuazione delle seguenti attività:

1. Rilevazione e segnalazione della violazione dei dati personali
2. Raccolta delle informazioni sulla violazione e comunicazione della violazione
3. Valutazione del rischio
4. Individuazione delle azioni correttive
5. Comunicazione delle valutazioni effettuate e delle azioni da intraprendere

6. Notifica della violazione (se necessaria)
7. Documentazione delle violazioni (Registro dei data breach)

| | Attività | Chi | A chi | Quando | Come |
|---|---|---|---|---|---|
| 1 | **Rilevazione e segnalazione eventuale data breach** | - tutto il personale<br>- collaboratori<br>- fornitori<br>- responsabili | - al Responsabile della struttura di appartenenza<br>- al Responsabile per la Sicurezza informatica e la Transizione al digitale (in caso di dati archiviati in formato digitale)<br>- al Responsabile della Protezione dei Dati | Appena se ne viene a conoscenza | Utilizzando le vie più brevi (telefono, e-mail etc.) |
| 2 | **Raccolta delle informazioni sulla violazione e comunicazione del data breach** | Il soggetto che ha rilevato la violazione dei dati | - al Responsabile della Struttura di appartenenza<br>- al Responsabile per la Sicurezza informatica e la Transizione al digitale (in caso di dati archiviati in formato digitale)<br>- al Responsabile della Protezione dei Dati | Entro 24 ore | Modulo per raccolta informazioni (allegato 1) |
| 3 | **Valutazione del rischio** | - Responsabile della Protezione dei Dati<br>- Responsabile per la Sicurezza informatica e la Transizione al digitale nel caso di dati contenuti in sistemi informatici | | Appena ricevuta la comunicazione | Metodologia di valutazione del rischio connesso alla violazione (allegato 2) |
| 4 | **Individuazione delle azioni correttive** | - Responsabile della Protezione dei Dati<br>- Responsabile per la Sicurezza informatica e la Transizione al digitale nel caso di dati contenuti in sistemi informatici<br>- referenti di struttura per la | | Appena terminata la valutazione di impatto | Analizzando i risultati della valutazione del rischio |

| | | | | | |
|---|---|---|---|---|---|
| | | sicurezza (se presenti) | | | |
| **5** | **Comunicazione delle valutazioni effettuate e delle azioni da intraprendere** | - Responsabile della Protezione dei Dati<br>- Responsabile per la Sicurezza informatica e la Transizione al digitale nel caso di dati contenuti in sistemi informatici<br>- Responsabili di struttura o loro Referenti | Al Titolare | | Relazione ed eventuale compilazione della modulistica predisposta dal Garante |
| **6** | **Notifica della violazione (se necessaria)** | Titolare | Al Garante | Entro 72 ore dalla rilevazione | Modulistica predisposta dal Garante (allegato 3) |
| **7** | **Comunicazione agli interessati (se necessaria)** | Titolare nella persona del Responsabile di struttura o suo Referente | Alle persone fisiche coinvolte | Nei termini indicati nella valutazione del rischio | Verbalmente o via e-mail (allegato 4 – Comunicazione agli interessati). Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, allora si potrà utilizzare una comunicazione pubblica, (in via esemplificativa tramite il sito web) che dovrà essere efficace al pari del contatto diretto con l'interessato. |
| **8** | **Documentazione delle violazioni** | - Responsabile per la Sicurezza informatica e la Transizione al digitale o suo refente qualora la violazione riguardi dati contenuti in sistemi informatici<br>- referenti di struttura per la sicurezza (se presenti)<br>- Responsabile di struttura o suo Referente | | Appena concluse le fasi precedenti | Inserimento dati nel Registro delle violazioni attraverso apposita procedura informatica (allegato 5) |

## 6. Violazione in caso di trattamenti di dati esternalizzati

Nel caso di trattamenti di dati esternalizzati, le strutture competenti devono procedere alla nomina dei responsabili esterni del trattamento di dati, secondo il fac-simile predisposto e pubblicato sulla rete intranet di Ateneo, nel quale sono definiti ruoli e responsabilità per la gestione degli obblighi di notifica e di comunicazione in caso di violazione dei dati personali.

I responsabili esterni del trattamento sono tenuti a comunicare al Titolare del trattamento (utilizzando l'allegato 1 – Modulo per la raccolta delle informazioni sulla violazione dei dati), per il tramite del Responsabile della Protezione dei Dati, l'avvenuta violazione entro e non oltre 24 ore dalla scoperta al fine di consentire al Titolare, legalmente responsabile, la eventuale notifica al Garante e la comunicazione agli interessati entro i termini stabiliti dal Regolamento UE 679/2016.

Chiunque riceva segnalazioni di avvenute violazioni da parte di soggetti esterni, compresi i responsabili esterni del trattamento, è tenuto a darne immediata comunicazione via mail al Responsabili della struttura di afferenza, al Responsabile della Sicurezza informatica e della Transizione al digitale di Ateneo e al Responsabile per la Protezione dei Dati.

Fanno parte integrante della presente procedura i seguenti documenti:

Allegato 1 - Modulo per la raccolta di informazioni sulla violazione dei dati
Allegato 2 - Metodologia di valutazione del rischio connesso alla violazione
Allegato 3 - Modello di notifica al Garante
Allegato 4 – Comunicazione della violazione all'interessato
Allegato 5 - Registro  delle violazioni
Allegato 6 – Esempi di violazioni di dati