# UNIVERSITA' DEGLI STUDI DI GENOVA

**AREA LEGALE E GENERALE**

**Ufficio Trasparenza, Anticorruzione e Privacy**

IL RETTORE

| | |
|---|---|
| Vista | la legge 9.5.1989, n. 168 e s.m.; |
| Vista | la legge 30.12.2010, n. 240 e s.m.; |
| Visto | il regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati; |
| Richiamato | lo Statuto dell'Università degli studi di Genova; |
| Richiamato | il D.M. n. 759 dell'1.10.2014, inerente alla nomina del prof. Paolo COMANDUCCI alla carica di rettore dell'Università degli studi di Genova per il sessennio accademico 2014/2020; |
| Richiamato | il D.R. n. 2213 del 24.5.2018, inerente alla nomina, dalla stessa data, della prof.ssa Annalisa BARLA quale responsabile per la protezione dei dati personali (RPD-DPO) per l'Università degli studi di Genova |

DECRETA

**Art. 1 -** A decorrere dalla data del presente decreto è emanata la "Procedura di gestione delle violazioni di dati personali (Data Breach) dell'Università degli Studi di Genova" di cui all'allegato 1 che forma parte integrante del presente provvedimento.

**Art. 2 -** Il presente decreto è pubblicato sul sito web istituzionale di Ateneo e diffuso a tutta la comunità accademica. Il documento informatico originale, sottoscritto con firma digitale, è conservato presso l'area legale e generale - ufficio trasparenza, anticorruzione e privacy.

IL RETTORE

Firmato digitalmente da:
PAOLO COMANDUCCI
Università degli Studi di Genova
Firmato il: 04-11-2019 14:56:57
Seriale certificato: 237371
Valido dal 23-02-2019 al 23-02-2022

Università di Genova

# Procedura di Gestione delle Violazioni di Dati Personali

# (Data Breach)

Allegato 1 al D.R. n. 4888 del 04/11/2019

## Sommario

## 1. DEFINIZIONI

**Dato Personale**
Qualsiasi informazione relativa a una persona fisica identificata o identificabile (**interessato**), come definita nelle norme in materia di trattamento dei dati personali.

**Norme in materia di trattamento dei dati personali**
Tutte le leggi, disposizioni e direttive normative applicabili in relazione al trattamento e/o alla protezione dei Dati Personali, così come modificate di volta in volta, ivi incluso, ma non limitatamente, il Regolamento UE 2016/679 (GDPR), la normativa di adeguamento italiana, circolari, pareri e direttive dell'Autorità di Controllo nazionale, le decisioni interpretative adottate dallo *European Data Protection Board*.

**Autorità di controllo**
L'autorità pubblica indipendente istituita da uno Stato membro, ovvero, per l'Italia, il Garante per la protezione dei dati personali.

**Trattamento**
Qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a Dati Personali o insieme 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 messa a disposizione, il raffronto o l'interconnessione, la limitazione, allineamento o combinazione, la cancellazione o la distruzione.

**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 europea 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; ovvero l'Amministrazione.

**Responsabile della protezione dei dati - RPD (o *Data protection officer* – DPO)**
Soggetto individuato dal Titolare del trattamento dei dati come definito dal Regolamento (UE) 2016/679 agli artt. 37-39 per assolvere alle funzioni consultive, formative, informative e di controllo relativamente all'applicazione del Regolamento medesimo. Coopera altresì con l'Autorità di controllo.

**Presidio *data breach***
Presidio permanente dell'Ateneo, nominato dal Titolare, avente funzioni di supporto al RPD-DPO nella gestione delle violazioni e della valutazione d'impatto per le attività di notifica al Garante per la protezione dei dati personali, agli interessati e alle Autorità competenti.

**Incidente di sicurezza**
Violazione o minaccia imminente di violazione alle politiche di sicurezza di trattamento dei dati personali e di utilizzo lecito degli strumenti tecnologici.

**Violazione di dati personali (*data breach*)**
La violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzati ai dati personali trasmessi, conservati o, comunque, trattati dall'Università degli studi di Genova.

## 2. FINALITÀ E AMBITO DI APPLICAZIONE

La procedura di Gestione delle Violazioni di Dati Personali *(Data Breach)* definisce:

- le modalità per l'identificazione, la registrazione e la reazione a una violazione di dati personali;

- i processi e i criteri per valutare il rischio per i diritti e per le libertà degli interessati e per stabilire se procedere alla notifica al Garante per la protezione dei dati personali e alla comunicazione agli Interessati.

Essa si applica a qualunque attività di trattamento dati svolta dal Titolare, con particolare riferimento a tutti i supporti di conservazione quali archivi, documenti cartacei, dispositivi elettronici, sistemi informatici.

È rivolta a tutti i soggetti che, a qualsiasi titolo, trattano dati personali di competenza del Titolare del trattamento:

- personale dipendente (docente e tecnico-amministrativo, inclusi i collaboratori ed esperti linguistici);
- personale non dipendente, con qualsivoglia tipologia di contratto o incarico; a titolo esemplificativo: i collaboratori, i consulenti, i titolari di incarichi di didattica, di contratti di assegni di ricerca, di dottorato e di ricerca, nonché gli studenti titolari di contratti di collaborazione a tempo parziale (c.d. 150 ore) o per le attività di tutoraggio didattico;
- qualsiasi soggetto (persona fisica o persona giuridica) che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento, agisca in qualità di Responsabile del trattamento ex art. 28 del Regolamento UE 2016/679.

Attraverso l'adozione della presente procedura, l'Università di Genova intende sensibilizzare i propri dipendenti e collaboratori sulle responsabilità in materia di protezione dei dati personali e sull'importanza della tempestiva segnalazione e risoluzione delle loro violazioni al fine di:

- contenere l'impatto sui diritti degli interessati;

- consentire all'Ateneo di concludere la gestione dell'evento nei termini di legge, considerato che il mancato rispetto delle prescrizioni di legge potrebbe esporre l'Ateneo a gravose sanzioni.

## 3. INCIDENTE DI SICUREZZA

Le violazioni di dati personali possono essere classificate all'interno della più ampia categoria degli incidenti di sicurezza. In questo senso, ogni violazione di dato personale è un incidente di sicurezza, mentre non tutti gli incidenti di sicurezza possono determinare un *data breach*.

Al fine quindi di individuare tempestivamente eventuali compromissioni di dati personali derivanti da un incidente di sicurezza, è importante che questo ultimo venga segnalato al DPO per le valutazioni di competenza.

Si ricorda che il concetto di incidente di sicurezza non si limita alle ipotesi di eventi causati da persone esterne all'amministrazione, ma include gli incidenti derivanti da atti o fatti del personale strutturato. Tali episodi includono sia eventi dolosi sia eventi accidentali.

Si riportano, per quanto di utilità, alcuni esempi di incidenti di sicurezza:

- gli utenti sono indotti ad aprire un file allegato alla e-mail che in realtà è un *malware*; l'esecuzione del codice malevolo comporta l'infezione del dispositivo stabilendo eventualmente connessioni dall'esterno alla rete informatica dell'Ente;
- un utente ottiene dati sensibili dell'organizzazione e minaccia l'organizzazione di diffonderli se non viene pagato un riscatto in denaro;
- un utente invia intenzionalmente un numero elevato di richieste di connessione ad un server web, provocando l'arresto anomalo del servizio.

## 4. *DATA BREACH*: TIPOLOGIE E CASISTICA

Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali. Pertanto un *data breach* può essere ricompreso in una o più delle seguenti tipologie di violazione:

**Violazione della Riservatezza** (*Confidentiality Breach*): divulgazione o accesso non autorizzati o accidentali ai dati personali;

**Violazione dell'Integrità** *(Integrity Breach)*: modifica dei dati personali in modo accidentale o senza autorizzazione;

**Violazione della Disponibilità** (*Availability Breach*): perdita, accesso o distruzione accidentali o non autorizzati di dati personali. L'impossibilità di accedere ai dati anche in via temporanea costituisce comunque una violazione.

Al fine di agevolare la corretta individuazione di un *data breach*, si riporta di seguito, a titolo esemplificativo, una casistica di eventi che potrebbero costituire casi di violazione di dati personali:

- perdita o furto di dispositivi informatici (es. *pc, computer* portatili, chiavetta *usb*, *hard disk* esterno, *smartphone, ecc…)* nei quali i dati personali sono memorizzati;
- perdita o furto di documenti cartacei contenenti dati personali;
- accesso o acquisizione di dati personali da parte di terzi non autorizzati;
- perdita o distruzione di dati personali a causa di incidenti, eventi avversi, allagamenti, incendi o altre calamità;
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi);
- impossibilità di accedere ai dati personali per cause accidentali o per attacchi esterni, quali *virus, malware*, o altri attacchi al sistema informatico o alla rete aziendale;
- i documenti contenti dati personali risultano alterati rispetto agli originali senza autorizzazione rilasciata dal relativo proprietario;
- divulgazione di dati personali non autorizzata (anche involontaria) a *mailing list*;
- indisponibilità, anche solo temporanea, delle liste di attesa per visite mediche o trattamenti sanitari.

**5. RILEVAZIONE DEL DATA BREACH**

Chiunque rilevi una concreta, potenziale o sospetta violazione dei dati personali, dovrà informare immediatamente il DPO dell'Università, individuato dal D.R. n. 2229 del 24.05.2018, (https://intranet.unige.it/sites/intranet.unige.it/files/2018.05.24%20Decreto%20responsabili%202 0.pdf) e scrivere, entro 24 ore e comunque senza giustificato ritardo, all'indirizzo e-mail abuse@assistenza.unige.it seguendo le indicazioni che verranno fornite per la compilazione del *form* di cui all'allegato A.

**6. VALUTAZIONE PRELIMINARE**

La segnalazione è oggetto di una valutazione preliminare da parte del DPO, il quale verifica che i fatti riportati nella segnalazione costituiscano effettivamente un *data breach* e, in caso positivo, dà l'avvio alla fase di gestione del *data breach*.

In caso di assenza/impedimento del DPO, la valutazione preliminare è effettuata dal Titolare del trattamento.

**7. GESTIONE DEL DATA BREACH**

Il DPO, ritenuta la sussistenza del *data breach*, fornisce tempestive istruzioni per il contenimento della violazione (es. utilizzo dei file di *back up* per recuperare dati persi o danneggiati; isolamento/chiusura di un settore compromesso della rete; cambio dei codici di accesso).

Acquisisce, inoltre, ulteriori informazioni sulla violazione, con particolare riferimento ai contenuti minimi richiesti dalla normativa per una eventuale notifica al Garante della protezione dei dati personali.

Nell'ambito della gestione deve essere valutato il rischio connesso al *data breach*, tenuto conto dell'impatto della violazione sulle libertà e diritti degli interessati. La valutazione permetterà di stabilire il livello di impatto, classificato in: Basso; Medio; Elevato. Per tutte le attività di gestione tecnica, ivi compresa la valutazione del *data breach*, e la verifica del rispetto delle istruzioni impartite, il DPO si avvale del Presidio permanente nominato dal Titolare.

In caso di assenza/impedimento del DPO, la gestione del *data breach* è effettuata dal Titolare del trattamento.

**8. NOTIFICA AL GARANTE**

Qualora la valutazione dell'impatto sia di livello medio o di grado superiore, il Titolare del trattamento, senza indebiti ritardi e, ove possibile, entro 72 ore dalla segnalazione, notifica la violazione al Garante per la protezione dei dati personali

Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, la stessa deve essere corredata dei motivi del ritardo.

Il mancato rispetto dell'obbligo di notifica espone l'Ateneo all'applicazione di misure correttive e sanzionatorie del Garante per la protezione dei dati personali, ovvero: avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi di dati, e sanzioni amministrative il cui importo può arrivare a € 10.000.000 o al 2% del fatturato annuo dell'esercizio.

La mancata notifica può rappresentare per la stessa Autorità di controllo un indice di carenze organizzative, per le quali potrebbe procedere all'irrogazione di ulteriori sanzioni.

**9. COMUNICAZIONE AGLI INTERESSATI**

Qualora dalla valutazione emerga un livello di impatto elevato, l'Ateneo deve procedere, senza ingiustificato ritardo, alla comunicazione della violazione agli interessati affinché gli stessi possano adottare proprie misure cautelative.

La comunicazione deve indicare:

a) la natura della violazione dei dati personali

b) il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni

c) le probabili conseguenze della violazione dei dati personali

d) le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

La comunicazione deve essere data direttamente e personalmente agli interessati coinvolti dalla violazione, a meno che ciò comporti sforzi sproporzionati. In tal caso, si procede ad una comunicazione pubblica (es. avviso su sito web) o a una misura simile, tramite la quale gli interessati sono informati con la medesima efficacia.

La comunicazione deve essere distinguibile dalle altre diverse comunicazioni che vengono fatte dal Titolare agli interessati; in altri termini, la comunicazione deve essere chiara, inequivocabile e richiamare l'attenzione dell'interessato.

La comunicazione non è richiesta se:

a) 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;

b) il titolare del trattamento ha, a seguito della violazione, adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati.

## 10. REGISTRO DELLE VIOLAZIONI

Indipendentemente dalla necessità di procedere alla notifica e alla comunicazione, ogni qualvolta si verifichi un *data breach* l'Ateneo deve documentarlo in un'apposita sezione del Registro dei trattamenti, a cura del DPO coadiuvato dal Presidio *data breach.*

Campi obbligatori

# ALLEGATO A - FORM DI SEGNALAZIONE DI UN INCIDENTE DI SICUREZZA E DI UNA POTENZIALE VIOLAZIONE DI DATI PERSONALI (DATA BREACH)

## Dati identificativi del segnalante

Nome e cognome: _____

Recapito telefonico: _____

E-mail: _____

Struttura di appartenenza: _____

## Informazioni sull'incidente di sicurezza e sul tipo di violazione di dati personali

Data, ora e luogo della violazione (anche approssimativi se non sono noti) _____

Data ed ora in cui si è venuti a conoscenza della violazione: _____

**Classificazione dell'incidente (può essere selezionata più di una voce):**

- ☐ Furto/Smarrimento di device o supporto di memorizzazione (ad esempio: computer, smartphone, tablet, chiavetta USB, documenti cartacei, etc), indicare:
  - quale device: _____
    - si conosce il luogo in cui è avvenuto?
      - NO
      - SI, indicare il luogo: _____

- ☐ Accesso abusivo a sistema informatico (ad esempio: Server, Data Base, Applicazione), specificare:
  - denominazione del sistema: _____
  - struttura che si occupa della gestione del sistema: _____
  - collocazione fisica del sistema:
    - se interno all'Ateneo (locale, edificio, indirizzo): _____
    - se esterno all'Ateneo (nome del fornitore e indirizzo): _____

Campi obbligatori

- ☐ Perdita/smarrimento/furto di credenziali di accesso a device o ad applicazione (ad esempio: computer, smartphone, tablet, etc.) contenenti dati personali, indicare:
  - o nome account: _____
  - o consente accesso a: _____

- ☐ Altro: _____

**Tipo di violazione di dati personali**:

- ☐ Furto (i dati non sono più sui supporti/negli archivi, ma sono presumibilmente in possesso dell'autore della violazione)
- ☐ Cancellazione (i dati non sono più sui supporti/negli archivi)
- ☐ Copia (i dati sono ancora presenti ma presumibilmente sono stati copiati dall'autore della violazione)
- ☐ Indisponibilità (i dati sono persi o distrutti o non sono più accessibili o non stati accessibili per un periodo limitato)
- ☐ Modifica (i dati sono presenti sui supporti/negli archivi, ma sono stati modificati)
- ☐ Lettura (presumibilmente è stato effettuato un accesso ai dati ma i dati non sono stati copiati)
- ☐ Altro:

  _____

**Tipologia supporto/archivio oggetto della violazione:**

- ☐ Computer
- ☐ Server
- ☐ Storage (es. usb, hard disk esterno)
- ☐ Rete
- ☐ Dispositivo mobile
- ☐ File o parte di un file
- ☐ Strumento di *backup*
- ☐ Archivio cartaceo o singolo fascicolo
- ☐ Altro: _____

Campi obbligatori

**Proprietà del supporto/archivio oggetto della violazione:**

- ☐ Di proprietà di Unige
- ☐ Personale
- ☐ Di terze persone fisiche o giuridiche

**Numero di dati (approssimativo) personali coinvolti (selezionare solo una voce)**:

- ☐ è noto il numero preciso di dati personali, indicare il numero: _____
- ☐ è nota una stima del numero di dati personali, indicare un valore stimato: _____
- ☐ non è noto il numero di dati personali

**Numero degli interessati (persone fisiche) dalla violazione dei dati personali trattati**:

- ☐ Indicare il numero, se noto: _____
- ☐ Indicare una stima del numero di persone fisiche coinvolte: _____
- ☐ Il numero non è noto

**Soggetti a cui si riferiscono i dati personali oggetto della violazione**:

- ☐ Personale docente e ricercatore
- ☐ Personale tecnico-amministrativo
- ☐ Collaboratori/Consulenti
- ☐ Studenti
- ☐ Pazienti
- ☐ Minori
- ☐ Disabili
- ☐ Altri: _____

**Categorie di dati personali oggetto della violazione:**

- ☐ Dati anagrafici/codice fiscale
- ☐ Dati di accesso e di identificazione (es. username, password, altro)
- ☐ Dati relativi a minori
- ☐ Dati relativi ad altre categorie protette
- ☐ Dati biometrici (dati personali che si ricavano da caratteristiche fisiche o comportamentali uniche e identificative di ciascuna persona fisica. Es.: impronte digitali; specifica

Campi obbligatori

conformazione fisica della mano o del volto, dell'iride o della retina; firma grafometrica; timbro e tonalità della voce)

- ☐ Dati genetici (dati personali riguardanti le caratteristiche genetiche di una persona fisica che siano ereditarie o acquisite, che forniscono informazioni uniche sulla fisionomia o sulla salute dell'individuo considerato, ottenuti in particolare dall'analisi di un campione biologico della persona in questione)
- ☐ Dati relativi alla salute
- ☐ Dati giudiziari (dati personali relativi a condanne penali e reati)
- ☐ Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, l'orientamento sessuale, le opinioni politiche, l'adesione a partiti, sindacati
- ☐ Dati economico-finanziari (es. numero carta di credito, conto corrente bancario, cedolino, altro….)

**Ha provveduto ad azioni per limitare i danni e se sì, quali?**

- ☐ Ho effettuato il cambio password
- ☐ Ho controllato tutti i miei dispositivi con un software antivirus e antimalware
- ☐ Altro:

_____

_____

**Eventuali ulteriori informazioni utili relative all'incidente:**

_____

_____

_____