SCUOLA DELLE ARTI
E DELLA FORMAZIONE
PROFESSIONALE
RODOLFO VANTINI

SCUOLA DELLE ARTI E DELLA FORMAZIONE PROFESSIONALE "RODOLFO VANTINI"

Modello Organizzativo sulla Protezione dei Dati personali ai sensi del Reg. UE 679/2016 (GDPR)

Procedura Data Breach

ELENCO DELLE REVISIONI

REV.	DATA	NATURA DELLE MODIFICHE	APPROVAZIONE
01	25/05/2018	Prima Emissione	Titolare del trattamento
02	Gennaio 2021	Aggiornamento	Titolare del trattamento
03	Novembre 2023	Aggiornamento	Titolare del trattamento

1. PREMESSA

Il Regolamento 679/16 (GDPR) introduce l'obbligo di notifica di una violazione dei dati personali (d'ora in poi "violazione") all'autorità di controllo. A partire dal 25 maggio 2018, tutti i Titolari del Trattamento dovranno notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, **entro 72 ore** e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85). Pertanto, la notifica all'autorità dell'avvenuta violazione **non è obbligatoria**, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'art. 34. Si segnalano, al riguardo, le linee-guida in materia di notifica delle violazioni di dati personali del Gruppo WP29 - 250.

Tutti i Titolari di trattamento dovranno in ogni caso **documentare le violazioni** di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati *(si veda art. 33, paragrafo 5)*.

La mancata segnalazione di una violazione all'Autorità o agli interessati comporta ai sensi dell'articolo 83 una possibile sanzione applicabile al Titolare del trattamento.

I Titolari e i Responsabili del trattamento sono quindi incoraggiati a pianificare in anticipo e mettere in atto procedure specifiche per rilevare e contenere prontamente una violazione

Scuola delle Arti e della Formazione Professionale "Rodolfo Vantini presta attenzione alla protezione dei propri dati personali dagli incidenti al fine di evitare una violazione che potrebbe compromettere la sicurezza.

La compromissione di informazioni, confidenzialità, integrità o disponibilità può comportare danni alle persone, danno alla reputazione della Scuola ed effetti dannosi sulla fornitura di servizi, oltre alla non conformità legislativa.

La presente procedura definisce le operazioni da seguire per garantire un approccio coerente ed efficace per la gestione degli incidenti relativi alla violazione dei dati e alla sicurezza delle informazioni.

1. DEFINIZIONI

Si definisce violazione di dato personale: "una violazione della sicurezza che porta a distruzione, perdita, alterazione, divulgazione non autorizzata o accesso non autorizzato a dati personali trasmessi, archiviati o altrimenti elaborati".

Le principali tipologie di violazioni sono riconducibili a:

- **Violazione della riservatezza** - in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali.
- **Violazione della disponibilità** - in caso di perdita accidentale o non autorizzata di accesso o distruzione di dati personali.
- **Violazione dell'integrità** - in caso di alterazione non autorizzata o accidentale dei dati personali.

A seconda delle circostanze, una violazione può riguardare la riservatezza, la disponibilità e l'integrità dei dati personali allo stesso tempo, nonché qualsiasi combinazione di questi.

Se la mancanza di disponibilità temporanea di dati personali può comportare un rischio per i diritti e le libertà delle persone fisiche, il Titolare dovrà darne notifica. Questo dovrà essere valutato caso per caso.

Ai fini della presente procedura, le violazioni della sicurezza dei dati comprendono sia gli incidenti confermati che sospetti.

Gli incidenti a titolo esemplificativo e non esaustivo includono:

- Perdita o furto di dati o apparecchiature elettroniche su cui tali dati sono archiviati (ad esempio, perdita di laptop, chiavetta USB, dispositivo iPad / tablet o fascicolo di carta);
- Furto o guasto dell'apparecchiatura elettronica;
- Uso non autorizzato, accesso o modifica di dati o sistemi di informazione (software);
- Tentativi (falliti o riusciti) di ottenere accesso non autorizzato alle informazioni o ai sistemi IT;
- Divulgazione non autorizzata di dati sensibili / riservati;
- Defacement del sito web;
- Attacco hacker;
- Situazioni impreviste come un incendio o un'inondazione;
- Errore umano;
- Comportamento infedele di un dipendente.

Gli incidenti riguardanti la sicurezza e la loro definitiva risoluzione dovranno sempre essere adeguatamente documentati.

Gran parte delle problematiche relative alla sicurezza vengono scongiurate grazie ad una costante opera di prevenzione. Le attività su cui la Scuola delle Arti e della Formazione Professionale "Rodolfo Vantini (di seguito "Scuola") focalizza la prevenzione sono sostanzialmente due, aspetto sociale ed aspetto tecnologico.

- Prevenzione sociale: La maggior parte degli incidenti di sicurezza derivano da un comportamento errato di chi opera con le strutture informatiche. Tali mancanze sono spesso dovute alla sottovalutazione dei reali pericoli esistenti. Occorre a tale scopo fare opera di sensibilizzazione verso le risorse più coinvolte e diffondere in maniera capillare policy mirate a stabilire regole e comportamenti "sicuri" da seguire.
- Prevenzione tecnologica: Per prevenzione tecnologica si intende la metodologia adottata da Engineering per la manutenzione dell'ambiente tecnologico al fine di mantenere la "sicurezza" ai massimi livelli. Le attività di prevenzione poste in atto sono:

- Server Security;
- Network Security;
- Sistemi Antivirus, Spyware (es. installazione ed aggiornamento antivirus, antispyware e personal firewall);
- Filtri Antispam;
- Patch management, ovvero l'attività periodica di aggiornamento del software in modo da coprire le falle di sicurezza eventualmente scoperte;
- Configuration check;
- Strumenti diagnostici.

3. FINALITA' E CAMPO DI APPLICAZIONE

Questa procedura si applica a tutto il personale della Scuola e a tutto il suo perimetro dati, trattati sia supporto elettronico che cartaceo.

Questo include il personale temporaneo, occasionale o di agenzia e gli appaltatori, i consulenti, i fornitori e i responsabili del trattamento dei dati che lavorano per o per conto della Scuola.

Il perimetro dati Informatici è delineato dal censimento degli applicativi in uso e dal rimando alle politiche di sicurezza delle informazioni e le misure adottate.

L'obiettivo di questa procedura è contenere eventuali violazioni, minimizzare il rischio associato alla violazione e considerare quale azione è necessaria per proteggere i dati personali e prevenire ulteriori violazioni.

4. SEGNALAZIONE INCIDENTI

Chiunque acceda, utilizzi o gestisca le informazioni della Scuola è responsabile di segnalare immediatamente violazioni alla sicurezza dei dati e incidenti informatici al Titolare del trattamento all'indirizzo **privacy@vantini.it**

Se la violazione si verifica o viene scoperta al di fuori del normale orario di lavoro, deve essere segnalata non appena possibile.

Il rapporto includerà i dettagli completi e accurati dell'incidente, quando si è verificata la violazione (date e orari), chi lo segnala, se i dati si riferiscono alle persone, la natura delle informazioni e il numero di persone coinvolte.

Tutto il personale deve essere consapevole che qualsiasi violazione della legge sulla protezione dei dati può comportare l'attivazione delle procedure disciplinari della Scuola.

5. CONTENIMENTO E RECUPERO

Il Titolare del trattamento determinerà innanzitutto se la violazione è ancora in corso. In tal caso, verranno presi immediatamente i provvedimenti appropriati per ridurre al minimo l'effetto della violazione.

Una valutazione iniziale verrà effettuata dal Titolare del trattamento, in collaborazione con le funzioni coinvolte e competenti per stabilire la gravità della violazione e chi assumerà l'iniziativa per indagare sulla violazione (ciò dipenderà dalla natura della violazione).

Il Titolare del trattamento stabilirà se c'è qualcosa che può essere fatto per recuperare eventuali perdite e limitare il danno che la violazione potrebbe causare. Stabilirà inoltre chi dover essere informato come parte del contenimento iniziale e informerà se necessario la polizia postale e le Autorità.

Il RPD/DPO supporta il Titolare in tutte le fasi investigative.

6. INDAGINE E VALUTAZIONE DEL RISCHIO

Il Titolare del trattamento effettuerà un'indagine immediatamente e ovunque possibile entro 24 ore dalla scoperta / segnalazione della violazione.

Il Titolare del trattamento esaminerà la violazione e valuterà i rischi ad essa associati, ad esempio le potenziali conseguenze negative per gli individui, quanto gravi o sostanziali siano e quanto probabilmente si verificheranno.

L'indagine dovrà tenere conto di quanto segue:

- il tipo di dati coinvolti;
- la "sensibilità" ai fini privacy;
- le protezioni che sono in atto (ad es. Log, Crittografie, etc.);
- cosa è successo ai dati, cosa è stato perso o rubato;
- se i dati potrebbero essere utilizzati in modo illegale o inappropriato;
- chi sono gli individui, numero di persone coinvolte e potenziali effetti su tali soggetti interessati;
- se ci sono conseguenze più ampie sulla violazione.

In questa fase sono prese in esame anche le informazioni contenute nel Registro dei Trattamenti e nel Rapporto Pia inerente rischi e misure.

7. TIPOLOGIA DI VIOLAZIONI CHE DEVONO ESSERE NOTIFICATE

Secondo le linee guida fornite dal Garante per la Protezione dei dati personali (ultimo aggiornamento 29 ottobre 2019), vanno notificate unicamente le violazioni di dati personali che possono avere effetti avversi significativi sugli individui, causando danni fisici, materiali o immateriali.

Ciò può includere, ad esempio, la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti dal segreto professionale, una perdita finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale.

8. NOTIFICA

Il Titolare del trattamento, con il supporto del RPD o DPO, determineranno, terminata la fase investigativa, chi deve essere informato della violazione.

Ogni incidente sarà valutato caso per caso; tuttavia, sarà necessario considerare quanto segue:

- Se procedere con la notifica Autorità Garante;
- Se esistono requisiti di notifica legale / contrattuale;

L'articolo 33, paragrafo 1 stabilisce che:

“in caso di violazione dei dati personali, il titolare del trattamento procede senza indebiti ritardi e, ove possibile, entro 72 ore dopo averne preso atto, notifica la violazione dei dati personali all'autorità di controllo competente ai sensi dell'articolo 55, a meno che il è improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche. Se la notifica all'autorità di controllo non viene effettuata entro 72 ore, è accompagnata dai motivi del ritardo”.

I Responsabili del Trattamento che sono venuti a conoscenza della violazione sono tenuti ad informare il Titolare senza ingiustificato ritardo e a collaborare con esso.

Questo è importante per aiutare il Titolare del trattamento a soddisfare l'obbligo di notifica all'autorità di vigilanza entro 72 ore.

Il Titolare del trattamento, con il supporto del RPD, deve prendere in considerazione inoltre la eventuale notifica a terzi come la polizia, gli assicuratori, le società bancarie o delle carte di credito e i sindacati. Ciò sarebbe appropriato laddove l'attività illegale è nota o si ritiene che si sia verificata, o laddove sussista il rischio che in futuro possano verificarsi attività illegali.

Il Titolare del trattamento, con il supporto del RPD, valuterà in collaborazione con l’alta direzione e il team di comunicazione, se debba essere emesso in merito un comunicato stampa.

La notifica deve contenere le informazioni previste dall’art. 33 paragrafo 3 del GDPR, come indicate nell’allegato al Provvedimento del Garante del 30 luglio 2019 sulla notifica delle violazioni dei dati personali:

- la natura della violazione dei dati personali, compresi, ove possibile, le categorie e il numero approssimativo di interessati e le categorie e il numero approssimativo di record di dati personali interessati;
- il nome e i dettagli di contatto del responsabile della protezione dei dati o di altri punti di contatto in cui possono essere ottenute maggiori informazioni;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate o proposte per essere adottate dal responsabile del trattamento per affrontare la violazione dei dati personali, comprese, se del caso, misure per mitigarne gli eventuali effetti negativi.

La notifica deve essere inviata al Garante tramite procedura online all’indirizzo https://servizi.gpdp.it/databreach/s/scelta-auth

Le informazioni relative alla notifica di una violazione sono contenute nel documento **“Fac simile del modello di notifica” (Allegato 2).**

9. COMUNICAZIONE DI UNA VIOLAZIONE ALL'INTERESSATO

In alcuni casi, oltre a notificare all'autorità di vigilanza, il Titolare del trattamento è inoltre tenuto a comunicare una violazione agli individui interessati.

L'articolo 34, paragrafo 1, afferma:

"Quando la violazione dei dati personali può comportare un rischio elevato per i diritti e le libertà delle persone fisiche, il responsabile del trattamento comunica la violazione dei dati personali all'interessato senza indebiti ritardi."

Secondo questa disposizione, il Titolare del trattamento dovrebbe fornire agli interessati almeno le seguenti informazioni:

a) una descrizione della natura della violazione;
b) il nome e i dettagli di contatto del responsabile della protezione dei dati o di altri punti di contatto;
c) una descrizione delle probabili conseguenze della violazione; e
d) una descrizione delle misure adottate o proposte da adottare dal responsabile del trattamento per affrontare la violazione, comprese, se del caso, misure per mitigarne gli eventuali effetti negativi.

Esempi di metodi di comunicazione trasparenti includono di utilizzare la messaggistica diretta (ad es. E-mail, SMS, messaggio diretto), banner di siti Web di primo piano o notifiche, comunicazioni postali e/o comunicati stampa. Il WP29 raccomanda al Titolare di scegliere un mezzo che massimizzi la possibilità di comunicare correttamente le informazioni a tutti gli individui coinvolti nella violazione.

L'articolo 34, paragrafo 3, stabilisce tre condizioni che, se soddisfatte, non richiedono la notifica ai singoli in caso di violazione. Questi sono:

- Il Titolare del trattamento ha applicato misure tecniche e organizzative adeguate per proteggere i dati personali prima della violazione, in particolare quelle misure che rendono i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi.
- Immediatamente dopo una violazione, il Titolare del trattamento ha adottato misure per garantire che non sia più probabile che si concretizzi l'alto rischio posto ai diritti e alle libertà delle persone.
- Contattare le persone comporterebbe uno sforzo sproporzionato. In caso di sforzi sproporzionati, potrebbero anche essere previste disposizioni tecniche per rendere le informazioni sulla violazione disponibili su richiesta, che potrebbero rivelarsi utili per le persone che potrebbero essere interessate da una violazione.

10. VALUTAZIONE E RISPOSTA

Una volta che l'incidente iniziale è stato contenuto il Titolare del trattamento, con il supporto del RPD, effettuerà una revisione completa delle cause della violazione; l'efficacia della risposta e se eventuali modifiche a sistemi, politiche e procedure dovrebbero essere intraprese.

I controlli esistenti saranno rivisti per determinare la loro adeguatezza e se debbano essere intraprese azioni correttive per minimizzare il rischio che si verifichino incidenti simili.

L'analisi prenderà in considerazione:

a) Dove e come vengono conservati i dati personali, dove e come sono archiviati;
b) Dove risiedono i maggiori rischi e individuerà eventuali ulteriori punti deboli all'interno delle misure esistenti;
c) se i metodi di trasmissione sono sicuri; condivisione minima quantità di dati necessari;
d) Identificazione dei punti deboli all'interno delle misure di sicurezza esistenti;
e) Consapevolezza del personale;
f) Implementazione di un piano di violazione dei dati e identificazione di un gruppo di individui responsabili di reagire alle segnalazioni di violazioni della sicurezza.

11. DOCUMENTARE LA VIOLAZIONE

Il Titolare del trattamento, a prescindere dalla notifica al Garante, documenta tutte le violazioni dei dati personali, mediante la predisposizione di un apposito registro (Allegato 3 “Registro delle violazioni”), da considerarsi allegato alla presente procedura.

Tale documentazione consente all’Autorità di effettuare eventuali verifiche sul rispetto della normativa.

12. ALLEGATI

Allegato 1: “SCHEMA DATA BREACH”

Allegato 2: “FAC SIMILE DEL MODELLO DI NOTIFICA”

Allegato 3: “REGISTRO DELLE VIOLAZIONI”