_cinquanta5
Accademia di Belle Arti
Reggio Calabria

PROCEDURA GESTIONE DATA BREACH

Indice

Rev.	Descrizione	Approvato	Data
00	Emissione procedura	Presidente	___/___/2024

1) Scopo

Lo scopo della **Procedura Data Breach**, nel rispetto del Regolamento Europeo 2016/679, è quello di definire tutte le attività che i soggetti coinvolti nei trattamenti dei dati operati dall'Accademia di Belle Arti di Reggio Calabria, devono seguire qualora siano a conoscenza di una violazione di dati (c.d. Data Breach) anche solo parziale o non del tutto definita in tutti gli elementi.

2) Cos'è un "Data Breach" o "Violazione dei dati personali"

Per violazione dei dati personali si deve intendere un incidente 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. Nello specifico, l'art.4 p.12 del GDPR definisce COS'E' UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH).

La violazione dei dati si può dividere in tre categorie:

- **Violazione della riservatezza**: quando si ha una divulgazione di dati o un accesso agli stessi non autorizzato o accidentale;
- **Violazione dell'integrità**: quando un dato è modificato in modo accidentale o non autorizzato;
- **Violazione della disponibilità**: quando il Titolare del trattamento non accede ai dati in modo accidentale o per dolo.

Una violazione dei dati personali può comprendere uno o tutte e tre le violazioni sopra citate anche combinate tra di loro.

Si parlerà di "Violazione della disponibilità "quando la violazione ha un impatto significativo sui diritti e le libertà delle persone fisiche (diversamente, l'interruzione programmata per manutenzione dei dati non deve essere considerata come violazione, in quanto si tratta di una perdita temporanea).

A titolo esemplificativo di seguito vengono evidenziate alcune delle violazioni dei dati personali:

1. Divulgazioni di dati personali a soggetti non autorizzati;
2. Perdita o furto degli strumenti dove vengono custoditi i dati personali;
3. Perdita o furto dei documenti cartacei contenenti dati personali;
4. Smarrimento o furto degli strumenti informatici aziendali contenenti dati personali (es. chiavette USB, telefoni aziendali ecc.);
5. Pirateria informatica:
   - Phishing trattasi di una truffa effettuata su internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire

informazioni personali, dati finanziari, codici di accesso, fingendosi un ente digitale (es. cavallo di Troia);
- Virus o attacchi al sistema informatico della rete aziendale;
- Ransomware/malware (programma informatico) che limita l'accesso del dispositivo che infetta, richiedendo a volte un riscatto (*ransom* in inglese) da pagare per rimuovere la limitazione. Ad esempio, alcune forme di ransomware bloccano il sistema e intimano all'utente di pagare per sbloccare il sistema, altri invece cifrano i file dell'utente chiedendo di pagare per riportare i file cifrati in chiaro;
- Perdita o furto delle credenziali di accesso;

6. Violazione fisica delle misure di sicurezza aziendali (es. forzatura di porte, finestre, armadi contenenti archivi ecc.);
7. Invio di e-mail contenenti dati personali/particolari ad un errato destinatario;
8. Alterazione o distruzione delle banche.

3) Ambito di applicazione della procedura

La procedura si applica a qualsiasi violazione del dato personale (art.4 p.1 GDPR). Di seguito si chiariscono le diverse tipologie di dati:

- Dati Personali: 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;
- Dati Particolari (ex art. 9 GDPR): dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
- Dati Giudiziari (ex art. 10 GDPR): dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza;
- Dati Biometrici: dati relativi a caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermino l'identificazione univoca come immagini facciali;
- Dati relativi alla salute: sono i dati attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni sullo stato di salute
- Dati Genetici: sono i dati relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, che forniscono informazioni univoche sulla

fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

4) A chi si rivolge la procedura di Data Breach

La procedura è rivolta a tutti i soggetti che, a qualsiasi titolo, trattino dati personali di competenza del Titolare del Trattamento:

- Lavoratori dipendenti (designati e autorizzati), nonché coloro che, a prescindere dal tipo di rapporto contrattuale, abbiano accesso ai dati personali nel corso delle prestazioni richieste dal Titolare del trattamento;
- Qualsiasi soggetto che abbia accesso a dati personali e che agisca in qualità di Responsabile del trattamento (art.28 del GDPT).

5) Gestione e comunicazione del Data Breach

In caso di concreto, sospetto e/o avvenuta violazione dei dati personali (Data Breach), sarà opportuno seguire gli step sotto riportati al fine della notifica alle autorità competenti per come previsto dal GDPR.

Il coordinamento delle attività di gestione della violazione dei dati personali è assicurato dal Referente privacy con il supporto del DPO, dei sistemisti informatici per gli aspetti tecnici e dei Designati della struttura/ufficio interessata alla violazione.

La segnalazione della violazione può avvenire o da personale interno: dipendente, dipendente somministrato, stagista ecc., o da soggetti esterni: DPO, Responsabili Esterni, Enti Pubblici interessati alla violazione, ecc.

Tutti coloro che sono a conoscenza anche di una non certa violazione hanno il dovere di segnalarla al proprio Responsabile/Designato utilizzando le vie più brevi (telefono, e-mail, di persona) appena ne vengano a conoscenza.

Dal momento in cui i soggetti preposti vengono a conoscenza della violazione di sicurezza, anche se non si è ancora in possesso di una descrizione dettagliata, è necessario procedere senza indugio e **non oltre le 48/72** ore alla comunicazione alle Autorità competenti, anche se le informazioni sono incomplete.

Al fine di consentire una gestione efficace e tempestiva delle violazioni dei dati personali, il Titolare del trattamento adotta un processo strutturato per la gestione dei casi di incidenti che prevede:

- Segnalazione dell'incidente;
- Analisi dell'Incidente;
- Registrazione dell'Incidente;
- Risposta ed eventuale notifica del Data Breach.

5.1 Segnalazione dell'incidente

La rilevazione e segnalazione dell'Incidente è un obbligo per tutti i dipendenti e/o collaboratori. Nel caso in cui si verifichi uno degli eventi sopradescritti o in tutti gli altri casi in cui il soggetto che tratta dati sia consapevole di altri eventi potenzialmente rischiosi, è tenuto a informare immediatamente il proprio Responsabile che senza indugio comunicherà la violazione.

Il Responsabile (Designato) dell'area dove si presume si sia verificata la violazione dovrà compilare il "**Mod. Segnalazione Data Breach"** per le opportune verifiche ed inoltrarlo a mezzo e-mail all'ufficio di Presidenza all'indirizzo *presidente@abarc.it*, ed al DPO all'indirizzo *dpo@abarc.it*.

5.2 Analisi dell'incidente

La suddetta analisi è finalizzata alla raccolta e identificazione delle informazioni e stabilirne la gravità attraverso la compilazione del "**Mod. Valutazione del rischio"**. La valutazione del rischio dovrà essere condotta dal DPO e dall'ufficio Privacy. Per la valutazione vengono utilizzati i criteri di seguito elencati, tenendo conto della probabilità di accadimento del danno e della gravità delle conseguenze.

La gravità della violazione dei dati personali è proporzionale all'impatto che la perdita ha sulle persone fisiche. Al momento della valutazione d'impatto di gravità di una violazione è bene tenere conto delle linee guida WP250 del gruppo di lavoro art.29, come sottorappresentato in modo esemplificativo:

- Aspetti generali: Valutare la gravità dell'impatto della violazione sui diritti e sulle libertà delle persone fisiche, della probabilità che tale impatto si verifichi;
- Tipo di violazione: Identificare la tipologia della violazione (distruzione, modifica, perdita, divulgazione);
- Natura dei dati trattati: Categoria dei dati trattati e se coinvolgono un numero notevole di persone;
- Identificazione delle persone fisiche: Sulla base dei dati compromessi, valutare la possibilità di identificazione delle persone fisiche, collegando anche più informazioni;
- Gravità delle conseguenze: Valutare il danno e le conseguenze che la perdita potrebbe potenzialmente provocare alle persone fisiche interessate;
- Dati particolari: analizzare se le perdite dei dati interessano categorie di persone fisiche correlate da informazioni su minori o informazioni che potrebbero rendere le stesse soggetti vulnerabili (dati sanitari);
- Numero di persone fisiche interessate: analizzare il numero delle persone fisiche che la violazione potrebbe interessare.

Sulla base dei suddetti parametri si procede alla valutazione della gravità dell'incidente relativamente ai diritti ed alle libertà degli Interessati, a seconda della natura dei dati personali (ad esempio, c.d. *Dati Sensibili e/o Giudiziari*), delle misure di sicurezza adottate, della tipologia di interessati (ad es., minori o altri soggetti vulnerabili). Il rischio (R) è calcolato mediante la formula sotto riportata:

R = Probabilità della minaccia X Impatto

Il rischio è tanto maggiore quanto più è probabile che accada l'incidente e tanto maggiore è la gravità del danno arrecato (Impatto). Una volta determinati gli indici di rischio, sarà possibile individuare e definire le priorità d'intervento.

In base ai valori attribuiti alle due variabili "Probabilità della Minaccia" e "Impatto", il rischio è numericamente definito secondo una scala crescente con valore **da 1 a 12** secondo la matrice sotto riportata:

	IMPATTO			
PROBABILITÀ DELLA MINACCIA	Basso (1)	Medio (2)	Elevato (3)	Molto Elevato (4)
Basso (1)	1	2	3	4
Medio (2)	2	4	6	8
Alto (3)	3	6	9	12

La ***probabilità*** è misurata mediante la ponderazione delle variabili che influenzano il trattamento del dato come: le risorse tecniche utilizzate, i processi e le procedure, la tipologia di trattamento svolto. ***L'impatto*** della violazione viene misurato in base ai soggetti coinvolti nel trattamento.

LIVELLI DI IMPATTO	
Nullo/Basso	I soggetti interessati non vengono colpiti o subirebbero disagi minimi, superabili senza alcun problema (tempo necessario per reinserire le informazioni, fastidio, irritazione, ecc.)
Medio	I soggetti interessati subiscono notevoli disagi risolvibili con qualche difficoltà (costi extra, negazione accesso a servizi aziendali, timori, difficoltà di comprensione, stress, indisposizione fisica, ecc.)
Elevato	I soggetti interessati subiscono notevoli disagi risolvibili con serie difficoltà (appropriazione indebita di fondi, inserimento nella *black list* dei cattivi pagatori da parte delle banche, danni a proprietà, perdita dell'impiego, citazione a comparire, peggioramento dello stato di salute, ecc.)
Molto Elevato	I soggetti interessati subiscono notevoli conseguenze, perfino irreversibili, e impossibili da risolvere (difficoltà finanziarie quali ingenti debiti, impossibilità a lavorare, problemi fisici o psicologici a lungo termine, morte, ecc.)

Una volta stabilito che si sia verificato realmente di un Data Breach, il Referente privacy aziendale congiuntamente al Titolare del trattamento, al Designato e al DPO, dovranno:

1 stabilire se esistono le azioni per limitare i danni della violazione (es. cambio codici di accesso, riparazioni della strumentazione aziendale, ecc.);
2 stabilire se il tipo di violazione presenti un rischio per i diritti e la libertà delle persone fisiche;
3 procedere alla notifica al Garante Privacy della violazione, che deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo *https://servizi.gpdp.it/databreach/s/* nella sezione "Compilazione della Notifica"
4 stabilire se sia necessario comunicare la violazione agli interessati;
5 Il DPO di concerto con il CISO e/o l'Amministratore di sistema e il Referente privacy, in caso di incidente cibernetico, in ottemperanza alla Direttiva NIS valuteranno la segnalazione dell'evento al CSIRT Italia attraverso la notifica dello stesso all'indirizzo *https://csirt.gov.it/segnalazione*

5.3 Registrazione dell'incidente

È necessario riportare la violazione (anche se non si ha la certezza del data Breach) all'interno del Registro delle Violazioni (**Mod. PVC-018**), che dovrà essere messo a disposizione del Garante Privacy qualora ne richieda la revisione. All'interno del Registro dovranno essere annotati:

- Data e ora della violazione,
- Natura della violazione;
- Categoria dei dati personali violati;
- Effetti della violazione e contromisure adottate;
- Se è stata effettuata la notifica al Garante Privacy;
- Se è stata effettuata comunicazione agli interessati;
- Numero degli Interessati.

Numero Violazione	Data Violazione	Ora Violazione	Natura della Violazione	Categoria di Interessati	Categoria di dati personali coinvolti	Numero approssimativo soggetti interessati	Conseguenze della Violazione	Contromisure adottate	Notifica Autorità Garante Privacy (SI/NO)	Comunicazione ai soggetti interessati (SI/NO)

5.4 Risposta ed eventuale notifica del Data Breach

La precedente fase di analisi dell'incidente di Data Breach fornisce gli strumenti necessari a identificare e valutare le conseguenze negative e gli impatti causati dall'incidente rilevato. Nel caso in cui dovesse risultare improbabile che l'incidente presenti rischi per i diritti e le libertà degli interessati, la notifica all'Autorità Garante risulta essere non obbligatoria, ma dovrà essere comunque annotata nel Registro delle Violazioni (Mod. Registro Data Breach).

Qualora, al contrario, dovesse risultare possibile che l'incidente abbia determinato una violazione dei dati che presenti rischi per i diritti e le libertà degli Interessati, con il supporto del DPO, si procede a predisporre la notifica all'Autorità Garante utilizzando il modello messo a disposizione dalla stessa e rinvenibile al seguente link: *https://servizi.gpdp.it/databreach/s/*

6) Comunicazione del Data Breach agli interessati

Dopo la verifica e l'eventuale Notifica al Garante della Privacy di una violazione dei dati personali, il Titolare, unitamente al DPO, valuterà se sia opportuno darne comunicazione anche agli Interessati coinvolti nella violazione. Si dovrà valutare l'opportunità ed i modi con cui comunicare a tutti gli Interessati la perdita dei dati personali Data Breach; Se singolarmente comporta uno sforzo sproporzionato rispetto al rischio, si valuterà l'opportunità di procedere a una comunicazione pubblica o a una misura simile, tramite la quale gli Interessati siano comunque informati con analoga efficacia. La notifica deve contenere:

- nome e dati di contatto del DPO;
- descrizione delle probabili conseguenze della violazione;
- descrizione delle misure adottate o che intende adottare per porre rimedio alla violazione.

Al fine di rendere più semplici le procedure, si procede alla compilazione del Mod. Comunicazione violazione agli interessati.

7) Modifiche e integrazioni

In caso di modifiche e/o integrazioni alla presente procedura o agli atti allegati, al fine di rendere disponibili e facilmente rintracciabili i documenti aggiornati, gli stessi saranno pubblicati sul sito aziendale, in apposita sezione dedicata, e comunicati internamente attraverso circolari e/o vademecum.

IL PRESIDENTE
Firmato digitalmente da
Maria Cerzoso
CN = Cerzoso Maria
C = IT