Data Breach Management Policy

Policy name: Data Breach Management Policy

Approved by RIAM Governance Committee: 19/02/2024
Approved by RIAM Governing Body: 29/02/2024
Approved by Trinity Academic Council:

1. Context

1.1 The Royal Irish Academy of Music, hereinafter referred to as RIAM or the Academy, has a legitimate business requirement to collect and use personal data (information) for a variety of purposes concerning its staff, students and other individuals who come in contact with it. These purposes include the organisation and administration of courses, examinations, research activities, the recruitment and payment of staff, compliance with statutory obligations, and also to protect the legitimate interests of the organisation.

1.2 The General Data Protection Regulation (GDPR) and Data Protection Act 2018 apply to the processing of personal data. RIAM is committed to complying with its legal obligations in this regard.

1.3 Data Protection legislation safeguards the privacy rights of individuals in relation to the processing of this personal data. The GDPR confers rights on individuals as well as responsibilities on those persons processing personal data.

1.4 Safeguarding personally identifiable information in the possession of the RIAM and preventing its breach is essential to ensure the organisation retains the trust of both staff, students and the public.

1.5 The RIAM as data controller and appropriate data processors so contracted, are subject to the provisions of the Data Protection Acts, 1988 and 2003 and exercise due care and attention in collecting, processing and storing personal data and sensitive personal data provided by data subjects for defined use.

1.6 The RIAM has prepared a Data Protection Policy and monitors the implementation of that policy at regular intervals. The RIAM retains records (both electronic and manual) concerning personal data in line with its Data Protection Policy and seeks to prioritise the safety of personal data and particularly sensitive personal data, so that any risk of unauthorized disclosure, loss or alteration of personal data is avoided.

2. Purpose

2.1 The purpose of this policy is to provide RIAM with a framework for reporting data breaches, in compliance with GDPR and Irish legislation guidelines.

2.2 This Code of Practice applies to the Royal Irish Academy of Music (RIAM) as *Data Controller.* This Code of Practice will be:

2.2.1 available on the RIAM website

2.2.2 circulated to all appropriate *Data Processors* and incorporated as part of the service-level agreement/data processing agreement between the RIAM and the contracted company, and

2.2.3 shall be advised to staff at induction and at periodic staff meeting(s) or training organised by the RIAM.

3. Scope

3.1 This policy applies to all personnel under the remit of the RIAM.

4. Benefits

4.1 This policy is intended to protect and safeguard the rights of staff members, students and other individuals when RIAM is processing their personal data.

5. Principles

5.1 RIAM undertakes to perform its responsibilities under the legislation in accordance with the GDPR.

6. Policy

6.1 This Policy sets out the RIAM's policy and procedures which shall be followed in the event of a breach of the security of the systems used by the RIAM.

6.2 For the purpose of this policy the term "**breach"** includes the loss of control, compromise, unauthorised disclosure or unauthorised access or potential access to personally identifiable information, whether in physical (paper) or electronic form.

A data security breach can happen for a number of reasons including:

- loss or theft of data or equipment on which data is stored (including break-ins to our premises)
- inappropriate access controls allowing unauthorised use
- equipment failure
- on-premise and online system failure
- cyber-attack
- ransomware attack
- human error
- unforeseen circumstances such as flood or fire
- a hacking or phishing attack
- access where information is obtained by deceiving the organisation.

6.3 The RIAM will make all reasonable efforts to protect confidential information and specifically personal data as a "**Data Controller**" when it acts in that capacity.

6.4 The RIAM will make all reasonable efforts to protect such information under the RIAM's control from unauthorised access, use, disclosure, deletion, destruction, damage or removal. Although reasonable efforts are made to protect facilities, equipment, resources and data, there exists the possibility that the security of data maintained by the RIAM may be breached. As a result, this Policy sets out a breach notification procedure or action plan in place should security procedures not prevent a breach**.**

7. Procedures

<u>Notification of Data Breach</u>

7.1 It is the duty of each staff member to report data breaches and cyber-incidents if and when they occur.

7.2 As soon as a member of RIAM staff becomes aware that personal data has been compromised (e.g. through loss of a portable device, misaddressing of labels, sensitive information left where unauthorised viewing could take place – for instance, photocopies not properly disposed of or left on copier), the RIAM member of staff shall:

7.2.1 Immediately notify his/her Line Manager, and

7.2.2 Complete the **Data Security Breach Incident Report** and send copy to the RIAM Data Protection Officer at dataprotection@riam.ie (ref Appendix 1).

7.3 The RIAM Manager, who receives the notification, investigates the issues surrounding the breach. The seriousness of the breach will determine the type of investigation that will take place. It may include an on-site examination of systems and procedures.

7.4 In the event of a serious data security breach the RIAM Manager will escalate the matter to the Data Protection Officer in the first instance. If the incident is deemed to be serious the Breach Management Team will be informed and contact will be made with the Office of the Data Protection Commissioner for advice and clarification.

7.5 Where appropriate the Breach Management Team will put a communication plan in place to contact the owner of the data involved (the Data Subject). Security of the medium used for notifying individuals of a breach of data protection procedures and urgency of situation should be borne in mind. Specific and clear advice should be given to individuals on the steps they can take to protect themselves and what the RIAM is willing to do to assist them.

Protocol for Action in the Event of a Data Breach

7.6 In circumstances where an incident gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data, in manual or electronic form, contact should be immediately made with RIAM ICT Services. The Response Team should follow the steps below to contain the matter and mitigate any further exposure of the personal data held:

7.6.1 Detection of a Cyber-Incident

The Response Team should review the report on the cyber-incident to establish the nature of the breach.

a. The Team should contact the Managed Service provider and Backup Solution vendor to obtain assistance in carrying out the necessary procedures.
b. The Team should only use the telephone to communicate, as attackers may be capable of monitoring e-mail traffic to and from the site.
c. The Team should not contact the suspected perpetrator.

7.6.2 Containment of a Cyber-Incident

Depending on the nature of the threat to the personal data, this could involve a quarantine of some or all PCs, laptops and other endpoints, network equipment etc.

a. The Team should immediately isolate the affected system to prevent further intrusion, release of data, damage, etc.
b. The Team should not delete, move or alter files on the affected systems or conduct a forensic analysis
c. The Team should seek to preserve all pertinent logs, e.g. firewall, router and intrusion detection system.
d. The Team should make copies of damaged or altered files and keep these backups in a secure location.
e. End users should be requested not to access PCs, networks etc.
f. Quarantine manual records storage area/s and other areas as appropriate.

7.6.3 Investigation of a Cyber-Incident

The Response Team should commence an investigation and call on security experts in the National Cyber Security Centre, HEAnet ICT Security Services (ICTSS) and Cybersecurity insurance agents/inspectors for advice as appropriate.

a. An audit of the records held or backup server should be undertaken to ascertain the nature of what personal data might potentially have been exposed
b. The Team should endeavour to identify where the affected system resides within the network topology
c. The Team should identify all systems and agencies that connect to the affected system(s)
d. The Team should examine the programs and processes that operate on the affected system(s) and assess the impact of the disruption and the maximum allowable outage time

Remediation of a Cyber-Incident

7.7 After the cyber-incident has been successfully contained, the Response Team should act to remove all elements of the incident from the environment. This might include removing malware, restoring clean data backups to affected hosts, running tests to ensure systems and services are functioning as expected and closing or resetting passwords for breached user accounts.

Recovery from a Cyber-Incident

7.8 Once the threat has been eradicated, the Response Team should restore systems and recover normal operations as quickly as possible, taking steps to safeguard the same assets from future attacks. The Response Team should document these processes and collect evidence to learn from the attack and increase the security team's expertise. This evidence could also be required for potential litigation and a cybersecurity insurance claim.

Post-incident Activity

7.9 Stakeholders and vendors should meet to discuss specific decisions the Response Team made during the incident to learn from this experience to improve the process and better respond to future security events. As educational institutions have become the targets of cyber criminals, protecting RIAM requires a focussed and determined effort to harden the network infrastructure against malicious actors.

7.10 Where data has been "damaged" (as defined in the Criminal Justice Act 1991, e.g. as a result of hacking), the matter must be reported to An Garda Síochána. Failure to do so will constitute a criminal offence in itself ("withholding information") pursuant to section 19 Criminal Justice Act, 2011. The penalties for withholding information include a fine of up to €5,000 or 12 months' imprisonment on summary conviction.

7.11 Where the data concerned is protected by technological measures such as to make it unintelligible to any person who is not authorised to access it, the RIAM may conclude that there is no risk to the data and therefore no need to inform data subjects or contact the Office of the Data Protection Commissioner. Such a conclusion would only be justified where the technological measures (such as encryption) were of a high standard.

7.12 Depending on the nature of the personal data at risk and particularly where sensitive personal data may be at risk, the assistance of An Garda Síochána should be immediately sought. This is separate

from the statutory obligation to report criminal damage to data arising under section 19 Criminal Justice Act 2011 as discussed at (6.2) above.

7.13 In addition and where appropriate, contact may be made with other bodies such as financial institutions, etc.

Reporting of incidents to the Office of Data Protection Commissioner

7.14 All incidents in which personal data (and sensitive personal data) has been put at risk shall be reported to the **Office of the Data Protection Commissioner** as soon as the RIAM becomes aware of the incident (or within 72 hours thereafter).

7.14.1 The General Data Protection Regulation (GDPR) introduces a requirement for organisation to report personal data breaches to the relevant supervisory authority, where the breach presents a risk to the affected individuals.

7.14.2 Where a breach is likely to result in a high risk to the affected individuals, the RIAM will also inform those individuals without undue delay.

7.14.3 All national breach notifications must be notified using the 'National Breach Notification Form'

7.14.4 All cross-border personal data breaches must be notified using the 'Cross-Border Breach Notification Form'

7.14.4.1 Cross-border processing means either:

a. Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of an organisation; or

b. Processing of personal data which takes place in the context of the activities of a single establishment of an organisation that substantially affects or is likely to substantially affect data subjects in more than one Member State

7.15 Data Protection Commissioner and Office of the Data Protection Commission (DPC)

Dublin Office and Postal Address

21 Fitzwilliam Square South
Dublin 2
D02 RD28
Phone +353 (17650100) | **LoCall** 1800437 737

Portarlington Office

Canal House
Station Road
Portarlington
Co Laois
R32 AP23

Webforms | **Email** info@dataprotection.ie
Website: www.**data**protection.ie

7.15.1 The DPC should be notified of all serious breaches. The completed notification forms should be emailed to: breaches@dataprotection.ie.

7.15.2 Where any doubt may arise as to the adequacy of technological risk-mitigation measures (including encryption), the RIAM shall report the incident to the Office of the Data Protection Commissioner within 72 hours of becoming aware of the incident, outlining the circumstances surrounding the incident. This initial contact will be by e-mail, telephone or fax and shall not involve the communication of personal data.

7.15.3 The Office of the Data Protection Commissioner will advise the RIAM of whether there is a need for the RIAM to compile a detailed report and/or for the Office of the Data Protection Commissioner to carry out a subsequent investigation, based on the nature of the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data.

7.15.4 Should the Office of the Data Protection Commissioner request the RIAM to provide a detailed written report into the incident, the Office of the Data Protection Commissioner will specify a timeframe for the delivery of the report into the incident and the information required.

7.15.5 Such a report should reflect careful consideration of the following elements:

- the amount and nature of the personal data that has been compromised
- the action being taken to secure and/or recover the personal data that has been compromised
- the action being taken to inform those affected by the incident or reasons for the decision not to do so
- the action being taken to limit damage or distress to those affected by the incident
- a chronology of the events leading up to the loss of control of the personal data
- the measures being taken to prevent repetition of the incident.

7.15.6 Depending on the nature of the incident, the Office of the Data Protection Commissioner may investigate the circumstances surrounding the personal data security breach. Investigations may include on-site examination of systems and procedures and could lead to a recommendation to inform data subjects about a security breach incident where the RIAM has not already done so. If necessary, the Commissioner may use his enforcement powers to compel appropriate action to protect the interests of data subjects.

Internal Recording of Incidents

7.16 Where no notification is made to the Office of the Data Protection Commissioner, the RIAM shall keep a **summary record of the incident** which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data.

7.16.1 Where the RIAM determines that there is no risk to affected individuals following a personal data breach, the RIAM will keep an internal record of the details, the means for deciding there was no risk, who decided there was no risk, and the risk rating that was recorded.

7.16.2 The record shall comprise a brief description of the nature of the incident and an explanation why the Secretary did not consider it necessary to inform the Office of the Data Protection Commissioner. Such records shall be provided to the Office of the Data Protection Commissioner upon request.

Internal Working Party

7.17 The RIAM shall form a working party to assess the potential exposure/loss. This working party will assist the Secretary with the practical matters associated with this Policy and Procedures. Action shall be undertaken in accordance with the DPC's direction/advice. Each member of the working party shall have a backup member to cover holidays, sick leave etc.

NAME	LOCATION	CONTACT NUMBER
Secretary/Finance Officer	House 36 RIAM HQ	+353-1-6325302
ICT Manager	House 36 RIAM HQ	+353-1-6325305
Buildings & Facilities Manager	House 36 RIAM HQ	+353-1-6325393
Head of RIAM Connect	House 36 RIAM HQ	+353-1-6325331
Head of RIAM Junior	House 36 RIAM HQ	+353-1-6325391
Tertiary	House 36 RIAM HQ	+353-1-6325312
Librarian	RIAM Music Library	+353-1-6325318
Other members of Staff	as appropriate	as appropriate

7.18 The working party will, under the direction of the Secretary, give immediate consideration to informing those affected except where law enforcement agencies have requested a delay for investigative purposes. Even in such circumstances consideration should be given to informing affected data subjects as soon as the progress of the investigation allows.

Law Enforcement Agencies

7.19 Where the RIAM receives such a direction from law enforcement agencies to delay informing affected subjects for investigative purposes, they should make careful notes of the advice they receive (including the date and the time of the conversation and the name and rank of the person to whom they spoke). Where possible, the RIAM should ask for the directions to be given to them in writing.

Informing Affected Subjects

7.20 At the direction of the Secretary, the working party shall:

7.20.1 Contact the individuals concerned (whether by telephone/email etc.) to advise that an unauthorised disclosure/loss/destruction or alteration of the individual's personal data has occurred.

7.20.2 Where possible and as soon as is feasible, the *Data Subjects* (ie individuals whom the data is about) should be advised of:

- the nature of the data that has been potentially exposed/compromised
- the level of sensitivity of this data, and
- an outline of the steps the RIAM intends to take by way of containment or remediation.

7.20.3 Individuals should be advised as to whether the RIAM intends to contact other organisations and/or the Office of the Data Protection Commissioner.

7.20.4 Where individuals express a particular concern with respect to the threat to their personal data, this should be advised back to the Secretary who may, advise the relevant authority e.g. An Garda Síochána, TUSLA etc.

Notifying Relevant Parties

7.21 Where the data breach has caused the data to be "damaged" (e.g.as a result of hacking), the Secretary of the RIAM shall contact An Garda Síochána and make a report pursuant to section 19 Criminal Justice Act 2011.

7.22 The Secretary of the RIAM shall notify the insurance company with which the RIAM is insured and advise them that there has been a personal data security breach.

7.23 Media enquiries about the breach shall be dealt with by authorised personnel only. A centralised "Fact Sheet" should also be created to ensure that one version, not many, becomes the view of the organisation internally and in contacts with the media.

Contracted companies operating as data processors

7.24 Where an organisation contracted and operating as a *data processor* on behalf of the RIAM becomes aware of a risk to personal/sensitive personal data, the organisation will report this directly to the RIAM as a matter of urgent priority. In such circumstances, the Secretary should be contacted directly. This requirement should be clearly set out in the data processing agreement/contract in the appropriate data protection section in the agreement.

7.25 A full review should be undertaken and having regard to information ascertained deriving from the experience of the data protection breach. Staff should be apprised of any changes to this Policy and of upgraded security measures. Staff should receive refresher training where necessary.

8. Responsibility

8.1 RIAM will take all reasonable steps to ensure that appropriate security measures are in place to protect the confidentiality of both electronic and manual data. Security measures will be reviewed from time to time, having regard to the technology available, the cost and the risk of unauthorised access. Staff and students must implement all organisational security policies and procedures, e.g. use of computer passwords, locking filing cabinets, securing offices, etc.

8.2 All employees must play their part in ensuring the confidentiality of this data and must not disclose personal data, except where necessary in the course of their employment, or in accordance with law. They must not remove or destroy personal data except for lawful reasons and with the permission of the organisation.

8.3 RIAM staff are responsible for ensuring that appropriate and adequate protection and controls are in place and applied in each facility and resource under their control and identifying those that are not.

8.4 Any breach of the data protection principles is a serious matter and may lead to disciplinary action up to and including dismissal. If employees are in any doubt regarding their obligations, they should contact the Data Protection Officer at dataprotection@riam.ie.

8.5 The Secretary is responsible for ensuring that staff follow this Policy and adhere to all related procedures.

8.6 Periodic reviews of the measures and practices in place shall be carried out.

9. Legislation and Regulation

9.1 General Data Protection Regulation (GDPR) (EU Regulation 2016/679)
9.2 General Data Protection Act 2018
9.3 Data Protection Commission Breach Notification

10. Related Documents

10.1 RIAM Data Protection Policy
10.2 RIAM ICT Policy
10.3 RIAM Privacy Policy

11. Review

11.1 This policy will be reviewed on a three year cycle, or as required to take into account changes in the law and the experience of the policy in practice.

12. Document Control

Approved by RIAM Governing body: 29/02/2024

Approved by Trinity Academic Council:

Next review: Academic year

This policy will be reviewed on a three-year cycle, or as required to take into account changes in the law and the experience of the policy in practice.

Appendix 1 Data Security Breach Incident Report Form

Complete the **Data Security Breach Incident Report Form** and send a copy to the RIAM Data Protection Officer at dataprotection@riam.ie. If you require assistance completing this form please contact IT Support at 086-8069515.

RIAM Data Security Breach – Incident Report	
Breach ID	
When did the breach take place?	
When was the breach discovered?	
Who reported the breach?	
Were there any witnesses?	**Yes** ☐ **No** ☐
If Yes, state Names of Witness(es)	**Witness 1**
	Witness 2
	Witness 3
Please provide details of the data breach e.g. circumstances and nature and content of personal data concerned	
Were any ICT systems involved? If so, please list systems concerned.	
Is any additional material available e.g. error messages, screen shots, log files, CCTV?	
Any additional comments?	
Signed	
Date	Time

Appendix 2 Procedure for Assessing the Severity of a Personal Data Breach

Methodology

Definition: Data Breach is a breach of security (or any actions) leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

In order to assess the severity of a Data Breach one should apply the following formula to each Data Breach.

Formula: *SE = DPC x EI + CB*

where

SE = Severity

DPC = Data Processing Context

EI = Ease of Identification

CB = Circumstances of Breach

Data Processing Context (DPC)

DPC = 1 for non-sensitive categories of personal data (names, email)

DPC = 2 for non-sensitive categories of personal data but could be used to profile the data subject (data that can be analyzed to predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests for example luxury products, can determine financial status or purchase of medical products might indicate health issues)

DPC = 3 for special categories of personal data (biometric, health, religion, genetic)

Ease of Identification (EI)

EI reflects how easily the identity of the individuals can be determined.

EI = 1 if the personal data was encrypted using modern strong encryption (AES)

EI = 2 if the data was not encrypted (plain text)

Circumstances of Breach (CB)

CB considers the circumstances of the breach, loss of security, malicious intent etc.

Description	Points	Example
Personal data is leaked to some known unauthorized receivers	1	(1) Emails containing personal data are sent to some known receivers who should not receive the emails. (2) Incorrect permission setting enables some unauthorised users to access personal data of others.
Personal data is leaked to some unknown receivers.	2	(1) Personal data is incorrectly uploaded to public web pages. (2) Incorrect configuration enables an arbitrary unauthorized user to access all personal data on the website.
Personal data is changed and incorrectly or unlawfully used, affecting data subjects; however, the changed data can be restored.	1	Some account passwords stored in the system are changed. As a result, the affected accounts cannot be logged into normally within a specific period. However, the changed data can be restored.
Personal data is changed and incorrectly or unlawfully used, affecting data subjects. The changed data cannot be restored.	2	Some account passwords stored in the system are changed, and the changed data cannot be restored. As a result, the affected accounts cannot be logged into anymore.
Personal data cannot be accessed, but the data can be restored.	1	Due to the mistakes of the maintenance personnel, the accounts of online service users are lost. However, the accounts can be re-created through other databases.
Personal data cannot be accessed or restored.	2	The database of a forum is damaged, and all stored forum user activities are lost. The lost data has no backup and cannot be re-provided by the users.
Personal data breaches are caused by malicious behaviour that adversely affects individuals.	2	(1) Employees share the customer's personal data on external websites. (2) Employees sell the customer's personal data to third parties. (3) Hackers break into the corporate IT system and steal personal data.

Calculating the severity (SE)

In the event of a data breach the DPO will evaluate the breach using the above formula.

After calculating the severity (SE) the following table will be consulted to determine the impact of the breach on the affected data subjects, the consequences and notification obligations.

SE Score	Impact	Possible consequences	Notification Obligation
SE less than or equal to 3	Not likely to result in a risk	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations etc.).	The data breach should only be recorded in the register
SE = 4	Likely to result in a risk	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments etc.).	The data breach should be reported to the Supervisory Authority.
SE is greater than or equal to 5	Highly likely to result in risk	Individuals may encounter significant, or even irreversible consequences, which may prove difficult or impossible to overcome (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death etc.).	The data breach should be reported to the Supervisory Authority, as well as to the affected data subjects

Appendix 3 Internal Breach Management Team Incident Form

For Breach Management Team Use	
Details logged by	
Severity of the Data Breach **(0 being minor, 5 being critical)**	**0 ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐**
Data Subjects to be notified	**Yes ☐ No ☐**
Details	
Data Protection Commissioner to be notified	**Yes ☐ No ☐**
Details (Date/time, note of advice received)	
An Garda Síochána to be notified	**Yes ☐ No ☐**
Details	
Actions Completed to Enhance Security	