Data Protection Policy

Policy name: Data Protection Policy

Approved: 25th November 2016
Revision 1 approved 10th March 2017
Revision 2 approved 25th May 2018
Revision 3 approved by Trinity Academic Council 13th May 2020

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.

2. Purpose

2.1 This policy is a statement of RIAM's commitment to protect the rights and privacy of individuals in accordance with the GDPR, the Data Protection Act 2018 and related legislative frameworks (see the Appendix).

3. Scope

3.1 This policy applies to all personal data which RIAM gathers, processes and stores on behalf of current and former staff and students, interested parties and stakeholders.

3.2 Personal data, both automated and manual, are data relating to a living individual who is or can be identified, either from the data or from the data in conjunction with other information.

3.3 Processing of personal data comprises: collecting, recording, storing, altering, disclosing, destroying and blocking.

4. Benefits

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

4.2 This policy provides RIAM with a framework for securing the personal data it collects in the course of its business activities, dealing with access requests and reporting data breaches, in compliance with GDPR and Irish legislation guidelines.

5. Principles

5.1 RIAM undertakes to perform its responsibilities under the legislation in accordance with the eight stated data protection principles outlined in the GDPR as follows:

(i) ***Obtain and process information fairly*.** RIAM will obtain and process personal data fairly in accordance with the fulfilment of its functions and its legal obligations.

(ii) ***Keep it only for one or more specified, explicit and lawful purposes*.** RIAM will keep data for purposes that are specific, lawful and clearly stated and the data will only be processed in a manner compatible with these purposes.

(iii) ***Use and disclose it only in ways compatible with these purposes***. RIAM will only use and disclose personal data in ways that are necessary for the purpose/s or compatible with the purpose/s for which it collects and keeps the data.

(iv) ***Keep it safe and secure***. RIAM will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. RIAM acknowledges that high standards of security are essential for processing all personal information.

(v) ***Keep it accurate, complete and up-to-date*.** RIAM will have procedures that are adequate to ensure high levels of data accuracy and completeness and to ensure that personal data is kept up to date.

(vi) ***Ensure that it is adequate, relevant and not excessive*.** Personal data held by RIAM will be adequate, relevant and not excessive in relation to the purpose/s for which they are kept.

(vii) ***Retain it for no longer than is necessary for the purpose or purposes*.** RIAM will have a defined policy on retention periods for personal data and appropriate procedures in place to implement such a policy.

(viii) ***Give a copy of his/her personal data to an individual, on request*.** RIAM will have procedures in place to ensure that data subjects can exercise their rights under the data protection legislation.

6. Procedures and Guidelines

6.1 RIAM is committed to ensuring the protection of the privacy of personal data and in order to assist in it's compliance with the data protection legislation will provide best practice guidelines and procedures in relation to all aspects of data protection.

6.2 Personal data collected by RIAM will be stored in secure systems. Highly sensitive data, such as medical information will be kept in separate files in order to ensure the highest levels of confidentiality. The organisation will ensure that only authorised personnel have access to personnel files, student records, examination/assessment results, payment details, etc. The organisation has put appropriate security measures in place to protect against unauthorised access to this personal data.

6.3 RIAM will endeavour to ensure personal data held by the organisation is up to date and accurate.

6.4 *Human Resources (HR)*

6.4.1 RIAM processes certain data relevant to the nature of the employment of its employees to comply with relevant legal obligations, to perform the employment contract and, where

necessary, to protect its legitimate business interests and the rights and entitlements of employees.

6.4.2 Personal data is normally obtained directly from the employee concerned. In certain circumstances, it will, however, be necessary to obtain data from third parties, e.g., references from previous employers. Where relevant to the nature of the work, the organisation may make an application to the Garda Vetting Bureau for Garda clearance of an individual employee.

6.4.3 Personal data collected by the organisation is used for ordinary HR management purposes. Where there is a need to collect data for another purpose, the organisation shall inform the individual of this. In cases where it is appropriate to get the individual's consent to such processing, the organisation will do so.

6.4.4 Employees will be responsible for ensuring that they inform the HR department of any changes in their personal details, e.g. change of address. Managers and supervisors must inform the HR department of any changes in employees' personal details, e.g. promotion, pay increases.

6.5 *Retention of Data*

6.5.1 RIAM is under a legal obligation to keep certain data for a specified period of time.

6.5.2 In addition, RIAM will need to keep personal data for a period of time in order to protect its legitimate interests (ref RIAM Records Retention Policy).

6.6 *Security and Disclosure of Data*

6.6.1 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. Employees must play their part in ensuring the confidentiality of this data.

6.6.2 Employees 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.

6.6.3 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, Theresa Doyle, at theresadoyle@riam.ie.

6.7 *Medical Data*

6.7.1 RIAM carries out pre-employment medicals as part of the recruitment process. This data will be retained by the organisation.

6.7.2 RIAM does not retain medical reports on job applicants who do not become employees for longer than is necessary and in line with our data retention policy.

6.7.3 Occasionally, it may be necessary to refer employees to RIAM's doctor for a medical opinion and all employees are required by their contract of employment to attend in this case. RIAM

may receive certain medical information, which will be stored in a secure manner with the utmost regard for the confidentiality of the document.

6.7.4 Safeguards are applied to the processing of medical data of employees. These include:

(i) limitations on access to prevent unauthorised consultation, alteration, disclosure or erasure of personal data;

(ii) strict time limits for erasure of personal data in line with RIAM's retention policy;

(iii) specific targeted training for those involved in handling medical data;

(iv) logging mechanisms to permit verification of whether and by whom personal data has been consulted, altered, disclosed or erased;

(v) a requirement that medical examinations are undertaken only by RIAM's occupational health specialists;

(vi) pseudonymisation;

(vii) encryption.

6.7.5 Employees are entitled to request access to their medical reports. Should an employee wish to do so, they should contact the RIAM Secretary, who will consult with the examining doctor and request the data. The final decision lies with the doctor. Employees are required to submit medical certificates in accordance with the sick pay policy. These will be stored by the organisation, having the utmost regard for their confidentiality.

6.8 *Right of Information*

6.8.1 Under Articles 13 and 14 of the GDPR, each European citizen has a right to be informed as to how his/her personal data is being processed (handled or used) by an organisation. RIAM undertakes, when obtaining personal data from an individual, to advise him/her of *inter alia* the purpose(s) of, and legal basis for, the processing of his/her data; any other recipient(s) of this personal data); how long it intends to retain this data, or the criteria by which it determines how long it retains this data; and the existence of any automatic decision making processes applied to this data.

6.8.2 Where the personal data has not been obtained from the particular individual, RIAM will provide this individual with additional information relating to the types of personal data it holds and how it obtained this data.

6.8.3 This information will be provided to the individual within a reasonable period, and at the latest within a month of the organisation obtaining the data (as per Article 12 of the GDPR).

6.8.4 If the personal data is used to communicate with an individual, the information about the types of data obtained and how it was obtained should be provided to him/her, at the latest, when the first communication takes place.

6.8.5 If it is expected that an individual's personal data will be disclosed to another recipient, the information should be provided to the individual when his/her personal data is first disclosed.

7. Data Access Requests

7.1 Each individual data subject associated with RIAM is entitled to request data held about him/her on computer or in relevant databases or filed in hard copy. RIAM will, in most circumstances, provide this data within one month. In some cases, due to the complexity of the request or the number of requests being handled by it, RIAM may require a further two months to provide this data. There is no charge for processing these data requests.

7.2 The Data Subject (e.g. teacher, student, parent, etc.) should make a request in writing to the Data Controller, Kevin Kelleher, email kevinkelleher@riam.ie, stating the exact data required (ref Subject Access Form (SAR)) and producing sufficient form of identification e.g. driver's licence, passport, etc.

7.3 Data Subjects are only entitled to access data about themselves and will not be provided with data relating to other individuals or third parties. It may be possible to block out data relating to a third party or conceal his or her identity, and if this is possible RIAM may do so.

7.4 Data that is classified as the opinion of another person will be provided unless it was given on the understanding that it will be treated confidentially.

7.5 Employees who express opinions about other employees in the course of their employment should bear in mind that their opinion may be disclosed in an access request, e.g., performance appraisals.

7.6 In some circumstances where relevant exemptions apply, certain personal data may not be provided to an employee. A Data Subject will be informed where personal data is not being disclosed on the basis of such an exemption.

7.7 An individual Data Subject who is dissatisfied with the outcome of an access request has the option of using RIAM 's Grievance and Mediation procedure.

7.8 A Data Subject may also refer a complaint to the Data Protection Commissioner.

7.9 *Right to Erasure ('Right to be Forgotten')*

7.9.1 Article 17 GDPR states that the Data Subject can request to have his/her personal details erased if this data are no longer necessary in relation to the purposes for which they were collected or otherwise processed or the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing.

7.9.2 The Data Controller shall have the obligation to erase personal data without undue delay where one of the above grounds apply.

7.9.3 A request for erasure should be made in writing to the Data Controller, outlining the data in question and the reason why this personal data should be erased.

7.10 *Right to Object*

7.10.1 Data Subjects have the right to object to data processing that is causing them distress and/or correct personal data which is inaccurate. Where such objection is justified, RIAM will cease processing the data unless it has a legitimate interest that prevents this. The organisation will make every effort to alleviate the distress caused to the individual.

7.10.2 An objection should be made in writing to the Data Controller, outlining the data in question and the harm being caused to the individual concerned.

7.11 *Closed Circuit Monitoring*

7.11.1 RIAM has closed circuit television cameras located around its premises at Westland Row. This is necessary in order to protect against theft or pilferage, for the security of staff and students and RIAM property.

7.11.2 Access to the recorded material will be strictly limited to authorised personnel. Please refer to the RIAM Closed Circuit Television policy for further details.

7.12 *Transmission of Data outside the State*

7.12.1 As RIAM operates internationally, it may be necessary in the course of business to transfer some individuals' personal data to other agencies in countries outside the European Economic Area, which do not have comparable data protection laws to Ireland. The transfer of such data is necessary for the management and administration of contracts of employment, registration of students and to facilitate the overall administration of personnel and students.

7.12.2 When this is necessary, RIAM will take steps to ensure that the data has the same level of protection as it does inside the State. The organisation will only transmit to companies that agree to guarantee this level of protection.

8. Responsibility

8.1 RIAM has overall responsibility for ensuring compliance with data protection legislation where it is the controller of personal data.

8.2 However all employees and students of RIAM who collect and/or control the contents and use of personal data are individually responsible for compliance with the data protection legislation.

8.3 RIAM will provide support, assistance, advice and training to all departments, offices and staff to ensure it is in a position to comply with the legislation.

8.4 *Contact Details*

Data Controller: Kevin Kelleher at email: kevinkelleher@riam.ie

Data Protection Officer: Theresa Doyle at email: theresadoyle@riam.ie

9. Legislation and Regulation

9.1 General Data Protection Regulation (GDPR).

9.2 Data Protection Act 2018.

10. Related Documents

10.1 Records Management and Retention Policy.

10.2 Closed Circuit Television 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 Board of Studies 25th November 2016.
Revision 1 approved by Board of Studies 10th March 2017.
Approved by ICT Steering Committee 25th May 2018.
Revision 2 approved 2nd November 2018.
Revision 3 approved by Trinity Academic Council 13th May 2020.
Next review: Academic year 2020/2021.

Appendix - General Data Protection Regulation

1. The General Data Protection Regulation (GDPR) came into force on the 25th May 2018. An accompanying Directive establishes data protection standards in the area of criminal offences and penalties. This is known as the Law Enforcement Directive.

2. The GDPR and the Law Enforcement Directive provide for significant reforms to current data protection rules. This legislation emphasises transparency, security and accountability by data controllers and processors, while at the same time standardising and strengthening the right of European citizens to data privacy. It also increases the range of possible sanctions for infringements of these rules.

3. Although the GDPR is directly applicable as a law in all Member States, it allows for certain issues to be given further effect in national law. In Ireland, the national law, which, amongst other things, gives further effect to the GDPR, is the Data Protection Act 2018.

4. Data Protection is the safeguarding of the privacy rights of individuals in relation to the processing of personal data, in both paper and electronic format. The terms of the **Data Protection Act 2018** lay down strict rules about the way in which personal data are collected, accessed, used and disclosed. The terms of the legislation also permit individuals to access their personal data on request, and confer on individuals the right to have their personal data amended if found to be incorrect.

5. The Data Protection Commission (DPC) derives its regulatory authority to protect individuals' data protection rights from a number of legislative frameworks which comprise:

   (i) the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679);

   (ii) the Data Protection Act 2018;

   (iii) the "Law Enforcement Directive" (Directive (EU) 2016/680) which has been transposed into Irish law by way of the Data Protection Act 2018;

   (iv) the Data Protection Acts 1988 and 2003;

   (v) the 2011 "e-Privacy Regulations" (S.I. No. 336 of 2011 – the European Communities (Electronic Communications Networks And Services) (Privacy And Electronic Communications) Regulations 2011).

   For further details please refer to the Data Protection Commission (DPC) at URL: https://www.dataprotection.ie/docs/GDPR/1623.htm

6. The DPC has launched a GDPR-specific website www.GDPRandYou.ie with guidance to help individuals and organisations become more aware of their enhanced rights and responsibilities under the General Data Protection Regulation.

7. Advice on GDPR matters is also available from the Citizens Information Board.