Royal Irish Academy: Data Protection Policy

Document Status: Working Document as of 18 May 2018. Document reviewed by Academy Council, 18 May 2018.

Context: This is a general policy document compiled in line with the General Data Protection Regulation (GDPR, EU 2016/679) and it will be subject to regular revision and update to take cognisance of the Data Protection Act 2018 and the forthcoming EU ePrivacy Regulation. For the time being, S.I. no. 336 of 2011 should be referred to: http://www.irishstatutebook.ie/eli/2011/si/336/made/en/print

The Data Protection Acts 1988-2003 will still apply in the case of a data protection complaint or a possible infringement of the law relate to an incident which occurred before the GDPR came into operation on 25 May 2018.

Furthermore, in the case of processing of personal data carried out for a law enforcement purpose (i.e. the prevention, investigation, detection or prosecurtion of a criminal offence or the execution of criminal penalties) then the Law Enforcement Directive, transposed into Irish law under the Data Protection Act 2018, will apply.

This document should be read in conjunction with Data Retention and Protection documents drawn up by the various Academy functions and projects and other guidance documents which are forthcoming. These are all being made available on the Academy website and will accrue with time.

Introduction

The Royal Irish Academy (hereafter, the Academy) collects and uses personal data (information) about its members, staff and other individuals who use our services or contribute to our work[1] in order to:

- administer our core business and activities;
- honour our obligations to our membership, staff and contractors and others;
- call and record meetings of Council, Executive and other Academy committees;
- comply with governance obligations and ensure best practice in all our dealings;

[1] These may include: applicants for grants or awards; applicants for posts; candidates for membership; registered Library readers; subscribers to our mailing lists for event notifications or our newsletter; customers who book events; attendees at events organised by the Academy; invited Academy guests; those whose photographs are taken at Academy functions of any kind; purchasers of publications; journal subscribers; facilitators; trainers; contractors whose services we use; presenters of lectures (list not exhaustive).

- implement procedures, strategies and compliance, incl. meeting health and safety, auditing and other legislative compliance requirements;
- report to the Higher Education Authority, to other agencies, to funders, partners and sponsors;
- manage research projects;
- recruit, train, manage and pay staff and ensure that all legal and statutory obligations in relation to staff are met;
- manage awards and grant schemes;
- select, contract and reimburse suppliers of goods and services;
- enable initiatives, negotiations in relation to partnerships etc.;
- facilitate room rentals and external clients who use our facility.[2]

Data Protection legislation safeguards the privacy rights of individuals in relation to the processing of their personal information. The General Data Protection Regulation (hereafter, the GDPR; EU2016/679), the Irish Data Protection Act 2018 and the forthcoming ePrivacy Regulation confer rights on individuals as well as responsibilities and accountability on those persons processing personal data, i.e. Data Controllers. The interpretation of personal data under the GDPR is extremely broad:

> **'Personal data are all information which is related to an identified or identifiable natural person.**
>
> **Those impacted are identifiable if they can be identified, especially using assignment to an identifier such as a name, an identifying number, location data, an online identifier or one of several special characteristics, which expresses the physical, physiological, genetic, mental, commercial, cultural or social identity of these natural persons. In practice, these also include all data which are or can be assigned to a person in any kind of way. For example, the telephone number, credit card or personnel number of a person, account data, number plate, appearance and customer number or address are all personal data.**
>
> **Since the definition includes "all information," one must assume that the term "personal data" should be as broadly interpreted as possible'.**[3]

The GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.[4]

For the purposes of compliance with the GDPR, the Data Protection Act 2018 and the ePrivacy Regulation, the Royal Irish Academy, 19 Dawson Street, Dublin 2, D02 HH58, is the

[2] List not exhaustive.
[3] https://gdpr-info.eu/issues/personal-data/ Accessed 17 May 2018
[4] GDPR, Article 3.

Controller of most of the personal data held by the Academy. The Academy's Data Protection Officer is: Siobhán Fitzpatrick (email: dataprotection@ria.ie or phone: 00 353 1 6090619).

1. Data Protection Officer's Role[5]:

The Data Protection Officer (hereafter the DPO) ideally will have an accredited Data Protection qualification and in accordance with best practice reports directly to the Executive Secretary. In compliance with GDPR Article 38, the Academy undertakes to involve the DPO properly and in a timely manner in all issues which relate to the protection of personal data; to support the DPO in the performance of the tasks required under GDPR by providing adequate resources to the DPO and access to personal data and processing operations, and to update his/her knowledge.

The Academy will not instruct the DPO regarding the exercise of tasks laid down under GDPR, nor shall the DPO be dismissed or penalised by the Data Controller for performing these tasks.

Data subjects may contact the DPO with regard to all issues in relation to their personal data and the exercise of their rights under GDPR.

The DPO is bound by confidentiality concerning the performance of the tasks undertaken. The DPO may fulfil other tasks and duties and is bound to ensure that these do not present a conflict of interest.

Duties of the DPO include: Advising and informing the Academy and employees who carry out processing activities of their responsibilities under GDPR; monitoring compliance with GDPR, other privacy regulations and the Academy's policies in relation to the protection of personal data, including assignment of responsibilities, training of staff, and related audits; providing advice in relation to data protection impact assessments; cooperating with the Office of the Data Protection Commissioner (ODPC) and acting as contact for the ODPC, including in the case of need for prior consultation in relation to high-risk processing. The DPO shall in the performance of tasks take due account of the level of risk associated with processing operations as laid down in GDPR, Article 39.2.

[5] GDPR Articles 37-39 apply.

2. Responsibilities of Academy Members and Employees – Data Protection Principles

The Academy has overall responsibility for ensuring compliance with the data protection legislation where it is the controller of personal data. However, all members and employees who collect and/or control the contents and use of personal data are individually responsible for compliance with the data protection legislation. The Academy's DPO will provide support, assistance, advice and training to all officers and staff as required to ensure that the Academy is in a position to comply with the legislation. Codes of conduct, declarations of conflict of interest, confidentiality agreements for assessors and other relevant parties (as required) and other governance protocols are in place: these support the data protection function.

The Academy will administer its responsibilities under the legislation in accordance with the **data protection principles** outlined in the GDPR, Article 5 inter alia, as follows:

GDPR, Article 5 (a): Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

This means that <u>one</u> of the following conditions should be met in order to constitute lawful processing:[6]

- ✓ the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- ✓ processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- ✓ processing is necessary for compliance with a legal obligation to which the controller is subject;
- ✓ processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- ✓ processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- ✓ processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The Academy will obtain and process personal data fairly in accordance with the fulfilment of its functions and its legal obligations. For much of our processing we rely on legitimising bases such as the performance of contractual obligations or, compliance with a legal obligation, or, the exercise of legitimate interests pursued by the Academy.

For some processes, e.g. signing up to mailing lists, other marketing purposes and in order to permit us to use personal data to fulfil orders etc. we shall request consent to the

[6] Based on GDPR, Article 6.

collection and processing of these data. Consent must be informed and customers will be provided with clear information about our processes and made aware of their rights and our obligations. Direct marketing requires explicit consent to enable the processing of data. We shall always provide an opt-in tick box, or an explicit statement for signature when explicit consent is required.

Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:[7]

- the identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the data protection officer, where applicable;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
- the persons or categories of persons to whom the data may be disclosed
- whether replies to questions are obligatory and the consequences of not providing replies to those questions
- the existence of the right to access one's personal data
- the existence of the right to rectify inaccurate data or to request cessation of processing of data which have been or are being processed unfairly
- the existence of the right to have data deleted
- any further information which will enable individuals to make an informed decision before agreeing to the collection of their data
- We shall also include right of appeal information and contact details for the Data Protection Commissioner's Office.

GDPR Article 5 (b): Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archival purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89 (1)[8], not be considered to be incompatible with the initial purposes.

[7] Based on GDPR, Article 13.

[8] 'Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that tecnnical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may

GDPR Art. 5 (c): Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (the concept of 'data minimisation').

The Academy will ensure that personal data are not repurposed, e.g. data collected for attendance at a lecture may not be used for a publications marketing campaign, unless at the outset separate consent for the data to be used for the latter purpose was obtained; similarly, the purchase of a book online should not result in the customer's name being added to a mailing list, unless that option was provided at the outset and consent given.

In many instances, data are held for a single purpose and that will generally mean that we hold your name and contact details. However, in the case of a grant applicant, we would hold sufficient information to enable the assessment of the application, to contact the applicant and to share their application with third-parties, viz. assessors. Data concerning applicants whether successful or unsuccessful, are minimised over time. Eventually, only sufficient data to provide a record of the grant process for audit and archival purposes are retained. We have outlined the processes around data and documents held by the Academy and its departments and projects on the webpages accessible under Data Protection and Retention Policies and Processes.

GDPR Article 5 (d): Personal Data shall be accurate and, where necessary, kept up to date, every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed are erased or rectified without delay.

The Academy undertakes to correct inaccurate data upon notification and to update data in a timely manner. Data which are no longer relevant to the purpose/s for which they were collected in the first place are deleted securely. Every effort will be made to ensure that public documents clearly indicate whom to contact to update data.

include pseudonymisation, provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing, which does not permit or no longer permits the identification of data subject, those purposes shall be fulfilled in that manner'.

GDPR Article 5 (e): Personal Data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Art. 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

The Academy undertakes to minimise personal data on an ongoing basis and particularly in relation to content stored for lengthy periods for archival, historic or research purposes. Pseudonymisation will be implemented in cases of sensitive personal data or, data judged to be high-risk, or, as technology permits.

GDPR Article 5 (f): Personal Data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Academy shall have appropriate measures in place to safeguard your data. For example, only designated personnel may access specific categories of data; secure file-sharing systems are in place for assessment processes and for spreadsheets or files containing personal data. Data are encrypted as appropriate and access to systems containing large amounts of personal data is limited, e.g. our Information Management System; mailing lists; image files; databases containing records of persons (e.g. the Library's Readers' database) are all accessible to designated personnel only using discrete passwords. Confidential files are secured and a clean desk policy is in operation. PCs, laptops and other devices are secured against unauthorised access and measures are in place to erase hard drives etc prior to disposal. The Academy's Acceptable Usage Policy relating to the use of the Academy's hardware, software systems, mobile devices etc. is accessible internally.

Hardcopy data containing confidential or personal data are secured in locked cabinets and in the case of data requiring higher levels of security these are secured in locked cabinets in locked rooms accessible only to authorised personnel.

Unauthorised access to data, loss of data by theft, physical causes, or accidental damage, or sending personal data in error to an unintended recipient will be dealt with in a timely way and in line with GDPR Articles 33-34.

Data processors contracted by the Academy to assist with systems' development or to store back-up data or to destroy data by secure shredding, must all be GDPR-compliant and have secure procedures in place for handling Academy data. These include reporting breaches immediately and taking appropriate measures to contain or respond to breaches, such as

theft or hacking or damage caused by fire, flood etc. The Academy will ensure that all its processor contracts include appropriate safeguards and procedures in relation to breaches and to report them upon discovery with details of remedial actions taken etc.

The Academy Breach Notification policy will shortly be available.

3. Transferring data outside the European Union

Specific conditions must be met before personal data may be exported to or imported from a country outside the European Union (or EEA countries, viz. Iceland, Liechtenstein and Norway). For transfers of data to the US for example only many companies are regulated under the EU-US Privacy Shield which means that data may be transferred without specific authorisation from the supervisory authority, i.e. the Office of the Data Protection Commissioner. US-based companies covered by the Privacy Shield may be found here: https://www.privacyshield.gov/welcome It should be borne in mind that the Privacy Shield is subject to periodic review.

In the absence of Privacy Shield cover, bodies in third countries must satisfy all the provisions re data transfers laid down in the GDPR, Chapter V, Articles 44-50.

The Academy uses several distribution systems, e.g. MailChimp (newsletter and mailing lists), Jotform (surveys and forms), Eventbrite (lecture, conference booking system). In most of these instances, the systems are US-based but all are regulated under the EU-US Privacy Shield which aims to provide additional safeguards for EU-generated personal data. In the case of MailChimp and Jotform, the Academy is the Data Controller of data held on our behalf and MailChimp and Jotform are Data Processors. Eventbrite is a Data Controller and in that case the Academy processes data collected by Eventbrite.

RIA Transparency Statement re use of Eventbrite
https://www.ria.ie/sites/default/files/eventbrite_0.pdf

RIA Transparency Statement re use of Jotform
https://www.ria.ie/sites/default/files/jotform_transparency_statement.pdf

RIA Transparency Statement re use of MailChimp

https://www.ria.ie/sites/default/files/mailchimp.pdf

4. CCTV

The Academy operates a CCTV system for security purposes only. CCTV data are not used for employee monitoring. A specific CCTV policy is in place: https://www.ria.ie/sites/default/files/royal_irish_academy_dp_policy_cctvv1.1_may_2018.pdf

5. Accountability

The Academy is cognisant of the requirement for accountability in relation to the collection and processing of personal data and the need to respect the confidentiality of the data we hold in relation to individuals. Clear statements relating to processes and workflows operating across departments and in relation to activities such as grant assessments and allocations, financial information, HR files, and other activities in which we engage are available on the website at appropriate locations as are documents outlining the procedures and processes around the work of the Academy's departments and projects. Full details relating to the processing involved in specific activities are supplied at the outset to prospective customers, applicants, donors or others as appropriate.

The Academy does not engage in automated decision-making.

In the case of activities requiring consent, proof of consents will be retained for the duration of the specific process/es for which these were sought.

Data security is continuously monitored and updated and processes are in place to secure systems against unlawful access.

Breaches will be logged and notified to the Office of Data Protection Commissioner as appropriate. Breaches of a serious nature will be brought to the attention of those whose data have been compromised and measures will be taken to deal with breaches in a timely fashion and to minimise their impact.

6. Sharing Data with Third Parties

The Academy does not disclose data to third parties where consent is a requirement e.g. mailing lists, except insofar as this is required to effect distribution of lists via contracted data processors' systems; in these instances due diligence is carried out prior to entering a contract and systems are kept under review. The same would apply in circumstances where our systems require IT upgrading or troubleshooting and we may have to provide temporary access to service providers for these purposes. Every care is taken to ensure that protocols are in place to ensure that data are not accessed illegally.

Due care is taken in relation to the collection and processing of sensitive personal data.

Relevant employee data may be disclosed to Revenue, Social Welfare departments or pensions' providers for statutory or employee benefit purposes.

For the administration of some Academy grant schemes, data are disclosed to grant partners e.g. the Royal Society-Royal Irish Academy Grant Scheme. Details of the processes relating to the administration of grants are accessible on the website. For most assessments data must be shared with assessors for a short period in order to enable assessment. This would apply to assessments of grant or award applications, to the shortlisting of candidates for posts or to assessment of candidates for membership of the Academy. Papers submitted for publication are sent to reviewers for peer review.

Many of the Academy's processes are subject to the scrutiny of auditors on an annual basis and all processes involving finance are subject to Revenue and statutory obligations.

Another category of sharing with third parties would occur in the case of photographs of individuals being requested for publications etc. In this case prior consent for the photography and/or uses of the image will have been obtained from the data subject.

Where data may be shared this will be clearly stated in our documentation.

It should be borne in mind that personal data, even sensitive personal data, could have to be disclosed in the case of legal or state security requirements, or where there is a threat to the life or safety of an individual.

7. Subject Access Requests

Anyone whose data are held by the Academy may submit a Subject Access Request to the DPO. Requests may be made in writing or by email. The DPO will need to assure herself that the request is genuine and not being made by a third party on behalf of the subject. Proof of identification may be requested. Requests will be dealt with within the statutory period under GDPR, viz. 30 days from receipt and acknowledgement of the request.

To contact the Data Protection Officer, please email: dataprotection@ria.ie or write Data Protection Officer, Royal Irish Academy, 19, Dawson Street, Dublin D02 HH58.

8. Review

This policy will be reviewed and updated regularly in light of any legislative or other relevant indicators.

Draft 1.1: S. Fitzpatrick
Data Protection Officer, 28 May 2018

Appendix I: Role of the Data Protection Commissioner

The Data Protection Commissioner is the independent supervisory authority of Ireland. The Commission oversees compliance with the terms of the legislation and has wide enforcement powers, including investigation and audit of records and record-keeping practices. The Data Protection Commissioner's Office may also process appeals on behalf of data subjects. A data controller found guilty of an offence can be fined and/or may be ordered to delete data.

Contact details: Office of the Data Protection Commissioner, Canal House, Station Road, Portarlington, Co. Laois, R32 AP23

Appendix II: Glossary of Data Protection terms

Data Protection: terms used and what they mean

'Personal Data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

'Restriction of Processing' means the marking of stored personal data with the aim of limiting their processing in the future;

'Profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

'Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

'Filing System' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

'Recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not;

'Third Party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

'Personal Data Breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

'Genetic Data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

'Biometric Data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

'Data concerning Health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

'Main Establishment' means:

(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;
(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

'Representative' means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

'Enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

'Group of Undertakings' means a controlling undertaking and its controlled undertakings;

'Binding Corporate Rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

'Supervisory Authority' means an independent public authority which is established by a Member State pursuant to Article 51: in Ireland this is the Office of the Data Protection Commissioner, Canal House, Station Road, Portarlington, Co. Laois, R32 AP23;

'Supervisory Authority Concerned' means a supervisory authority which is concerned by the processing of personal data because:

(a) the controller or processor is established on the territory of the Member State of that supervisory authority;
(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
(c) a complaint has been lodged with that supervisory authority;

'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 a controller or processor in the Union where the controller or processor is established in more than one Member State; or

(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

'Relevant and Reasoned Objection' means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

'Information Society Service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council ([1]);

'International Organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.