# Royal Irish Academy: Data Protection: Personal Data Breach Policy and Procedures for addressing data breaches.

## Academy collection of Personal Data

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 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;
- 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.

## Data Controllers and Data Processors

The Academy is the Data Controller of most of the data which we process in the course of managing the above activities. In a few instances, we outsource data processing to third parties, e.g. data storage; shredding; web hosting; distribution of newsletters and other direct marketing activities — these third parties are data processors but the Academy remains the Data Controller with primary responsibility for the data. At other times, the Academy is a data processor, e.g. when we use services such as Eventbrite for conference or event registration, Eventbrite is the data controller and the Academy harvests specific data temporarily for the purposes of managing the event in-house. See https://www.ria.ie/sites/default/files/eventbrite_0.pdf

The General Data Protection Regulation (GDPR, EU 2016/679) imposes obligations on Data Controllers and Data Processors to have adequate, up-to-date technical and other measures in place to assure the security of processing at a level appropriate to the severity of risks to individuals' rights and freedoms. In particular, Articles 33 and 34 address the issue of data breaches and the measures Data Controllers and Processors are mandated to take in the event of a breach.

**What is a data breach?**

A 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. Breaches may be accidental or deliberate. Here are some examples:

- Sending an email or letter containing personal data to the incorrect recipient;
- Altering a person's data without permission;
- Unauthorised third party access to a person's data (the third party can be someone within or external to the organisation);
- A deliberate or accidental action by the Data Controller or Processor, or inaction, in certain cases;
- Loss or theft of computing equipment, hardware or software;
- Loss of availability of data, e.g. during a power outage.

So, breach covers a broad sweep of incidents *from*

- sending an email to the wrong John Smith,

  *to*

- a hacking incident,
- a power outage causing corruption of files or their inaccessibility,
- accessing and/or passing on data without appropriate authorisation
- losing a mobile phone containing emails and attachments with personal data,
- CCTV tapes being accessed without appropriate authorisation or being sent to recycling without being properly cleared,
- Insecure disposal of personal data e.g. discarding data which should be securely shredded, in paper disposal bins (list not exhaustive).

**It is important to understand that a security incident or any of the above incidents must not be ignored.**

**GDPR imposes a duty on organisations to:**

1. Have robust systems in place to detect and investigate breaches and strong internal reporting procedures in place so that decisions may be made and actions taken without delay;
2. Know how to identify data breaches;
3. Know how to respond to breaches;
4. **Report certain types of breach to the Office of the Data Protection Commissioner (ODPC) within 72 hours of becoming aware of the data breach**;
5. Assess the risk to individuals' rights and freedoms and if the risk is considered high, those individuals must be informed of the breach. Some personal data breaches could result in physical or material damage to persons for example, by loss of control over their personal

data, or identity theft, fraud, financial or reputational loss, loss of confidentiality of data protected by professional secrecy, or emotional distress. Other breaches might cause inconvenience, for example corruption of some data due to a power outage might disrupt workflows but can probably be addressed by using backup data — therefore, low impact.

6. A record of all breaches, minor or major, must be kept, regardless of whether the Data Protection Commissioner's Office needs to be notified. For accountability purposes, this record must be available for audit by the Commissioner's Office.

**These are guidelines for what to do if you are responsible for a breach or discover a personal data breach:**

1. As soon as you become aware of a breach, inform the Data Protection Officer and your line manager and if the breach relates to electronic data loss, theft or hacking, inform the IT department. Countdown starts at the point of awareness. The organisation must begin to address identifying the cause of the breach and actions to be taken from this point.

   So if you mislay an Academy laptop or it is stolen whilst in your custody, you must immediately inform the Head of IT. If you realise that someone has accessed your computer inform the Head of IT. If you release a list of contacts to a third party inadvertently or suspect that a file has been taken, inform the Data Protection Officer who will advise on appropriate steps to take.

2. Once a breach is detected, the DPO will start to track the situation, and record the facts and actions taken, in consultation with the Head of IT.

   It is necessary to record whether the breach was caused:

   - by human error, e.g. sending confidential data to the wrong recipient,
   - or deliberately, e.g. unauthorised access to data — if you become aware that a file was read by a third party without authorisation,
   - or a data loss was caused by a power failure,
   - or data was hacked or corrupted.

   The DPO must also describe the likely consequences of the breach and the measures taken to deal with it, with mitigating measures proposed or taken, if appropriate.

   The DPO must make a judgement call on whether the risk to an individual or individuals' data is high and if this is the case, the incident must be reported without delay to the ODPC. It will also be necessary to inform the individual/s concerned and let them know what corrective actions have been put in place or whether they need to protect themselves from the effects of the breach. This would apply for example in relation to financial data, credit card details, PPS numbers, or reversal of pseudonymised data which could lead to identity theft.

   Even if a decision is made that it is unnecessary to report a breach, this decision must be justified and documented.

3. Bear in mind that not all security incidents involve personal data breaches, for example, the theft of an encrypted tape which doesn't contain personal data will not be relevant but it could have to be reported to the Gardaí.

4. **Data processors are responsible for reporting a breach to the Academy without undue delay**. It is then incumbent upon the Academy to report the breach to the ODPC, to

ascertain whether the data loss includes Academy data, and in particular personal data, and to liaise closely with the data processor to ensure that all of the necessary steps are taken.

**All data processors whom we use must have a breach reporting clause built in to their contract.**

**The information which must be supplied to the supervisory authority, the ODPC:**

1. Description of the nature of the personal data breach, with details of the categories and number of individuals affected and of the categories and number of personal data records involved.
2. The name and contact details of the DPO or other point of contact in the absence of the DPO.
3. Description of the likely consequences of the breach.
4. Description of the measures taken or proposed to be taken, to deal with the breach, including mitigating measures.
5. If a breach is detected but it is not possible to identify the causes or extent of it, notify the ODPC explaining the situation and that you will report as soon as more information is uncovered.
6. It could be necessary to notify the Gardaí or insurance company or bank in some cases of breach.
7. It could also be necessary to notify the public via the website or by other means, in the event of a major breach. In this instance, the Business Continuity Plan would probably be invoked.

**If we need to contact individuals in the event of a high-risk breach:**

1. Describe in clear language the nature of the breach and the likely consequences of the breach (for example, loss of customer data or grant applicant data due to a ransomware attack);
2. Provide the DPO's details and/or other contact details for further information;
3. Describe the measures taken, or proposed to be taken, to deal with the breach and the measures taken to mitigate any possible adverse effects, e.g. contacting banks etc.

Finally, we should analyse and learn from data breaches and endeavour to put preventive measures in place to ensure greater security of personal data. It's best to face up to breaches and own how we address them. And remember, the ODPC may levy stiff fines on institutions which fail to notify breaches.

S. Fitzpatrick
Data Protection Officer, 17 June 2018