2023 Annual Report

Data Protection Office

The purpose of this Annual Report is to provide an overview of the activities of the Data Protection Office in 2023 on the following topics:

- Summary of performance of 2023
- Key Achievements
- Challenges and risks
- Audit Outcomes
- Priorities for 2024.

GDPR integrates accountability as a principle which requires that organisations put in place appropriate technical and organisational measures and be able to demonstrate what they did and its effectiveness when requested. Maynooth University ("MU") must demonstrate its compliance with this principle and an Annual Report is a useful means of demonstrating accountability.

Accountability obligation | Data Protection Commission

Who we are: Staff & Department Structure

There are 3 full-time staff members in the Data Protection Office.

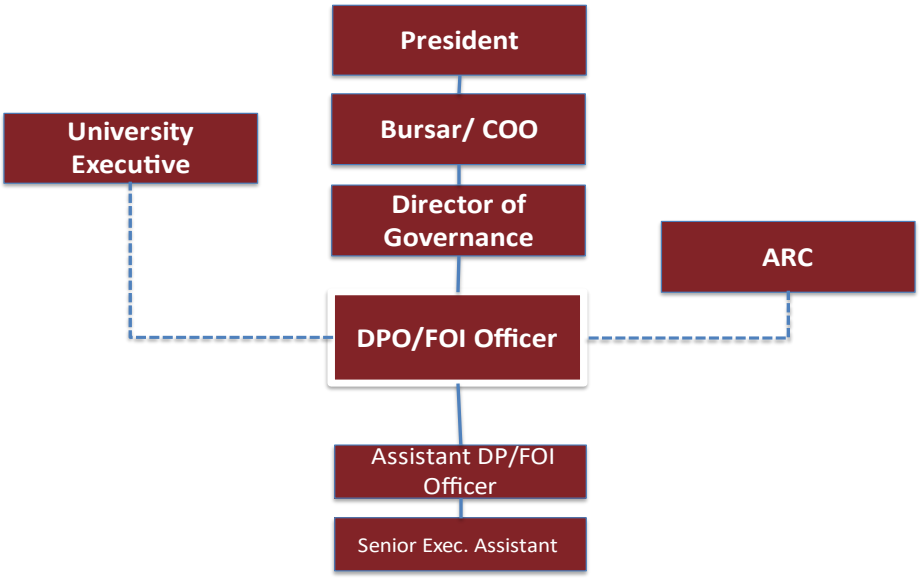
These staff play a dual role as the Office also looks after the University's Freedom Of Information (FOI) function.

Staff are appropriately trained in Data Protection and attend conferences and webinars in order to stay up to date with Data Protection developments and best practices.

The Data Protection Officer ("DPO") and Assistant DPO/FOI Officer are members of the Health Research Data Protection Network (HRDPN).

The issue of staffing levels in the office is kept under review.

Organisational Structure



What we do

'To act as a champion for Data Protection compliance and create awareness and knowledge across the University.'

Maynooth University Data Protection Office sits within the Governance Directorate and is legally responsible for ensuring the University's compliance with data protection legislation. On Data Protection issues, the DPO has the autonomy to report directly to University Executive.

Data Protection legislation impacts on many aspects of university life. The Data Protection Office supports MU's management of its responsibilities in respect of data protection. The Office is responsible for assisting staff, students and members of the public in exercising their rights under the legislation.

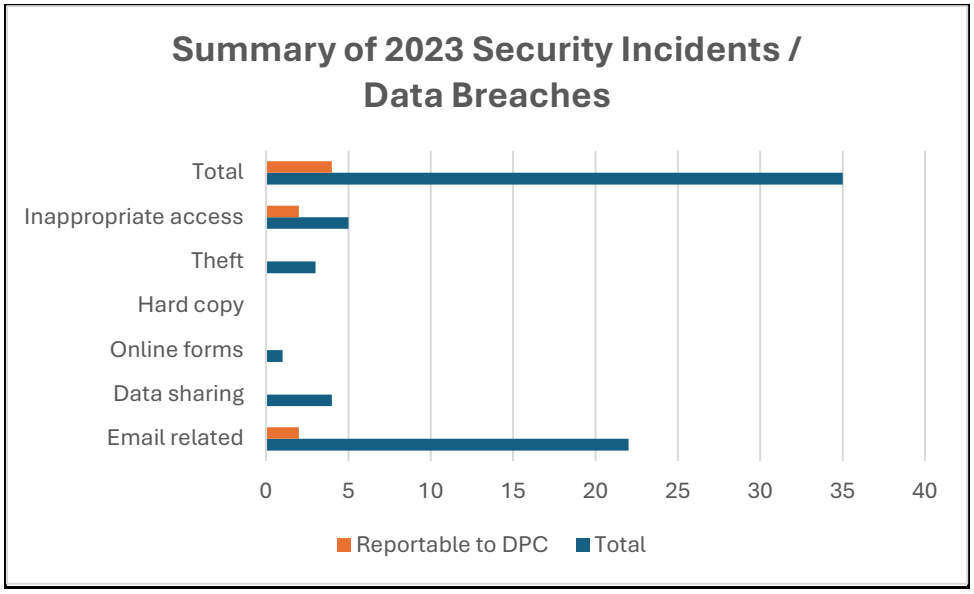
Required tasks for the office include:

- Monitoring University compliance with the legislation;
- Provision of legislative specific training to the University community;
- Updating, further development and implementation of relevant policies procedures and guidelines;
- Conducting University wide annual audits to ensure the records of processing activities is up to date and accurate;

- Reviewing and approval of Data Privacy Impact Assessments (DPIAs) and contracts for services as appropriate;
- Processing Access Requests; conducting data protection investigations, engagement with the DPC & representing the University on national committees and work groups.
- Developing resources and tools for use by the university community in managing compliance with relevant regulatory requirements and to support transparency and openness in the University's use of data and information.

2023 Summary of Security Incidents and Data Breaches

In total there were 35 security incidents/data breaches that were reported to the DPO in 2023. These are broken down by category below. Of this number, four were reported to the DPC. There was no follow up action from the DPC.



**Theft related to two laptops and a sign in sheet from a classroom.*

In 2023, a higher number of Data Breaches and Incidents were reported to the DPO by staff from Professional Services (encompassing all non-academic units) than by Academic Departments. This may reflect a greater awareness among professional staff of the obligation to report data breaches.

2023 in Review

The office works on a balance of reactive and proactive work, utilising queries and access requests as an opportunity for upskilling, process improvement and improved quality and compliance.

A number of new governance and oversight measures were put in place to centralise information recording, place focus on deadlines and improve compliance with statutory timelines.

Template wording and Schedules of Records were introduced to improve compliance with legal obligations.

2023 Key Achievements

- Introduced promotion of annual calendar event for **Data Protection Day** on 28th January.
- Also promoted the anniversary of the introduction of **GDPR** on 25th May.

  These annual celebrations are an opportunity to thank staff for engaging with our office and considering data protection in their work.

  It is an opportunity to point staff to resources, training and informing staff of current developments and industry best practice in data protection.
- **Strengthened relationships** with HR, IT, Comms & Marketing, Procurement, Research to develop processes and awareness and commence programmes of work to create Staff Guidelines for compliance with various aspects of data protection compliance.
- Introduction and upgrade of logs and registers **to improve compliance** with our obligations under data protection legislation, eliminate inefficiencies in our ways of working and create a professional impression of the function.
- Development of data protection content for MU DP webpages.
- Led Created the **Implementation Plan for Data Protection** in line with the University Strategic plan 2023 – 2028. The Office is a key enabler of Governance, Quality and Operational Excellence for the Strategic Plan.

In terms of the main activities of the Data Protection Office in 2023, the following is an overview summary of some of the key activities. This does not include responding to queries, delivering in-person training etc.

Event Type	Total
Responding to Breaches and Security Incidents	35
Processing Data Subject Access Requests (DSARs)	16
Processing Data Subject Rights Requests	3
Responding to Garda Access Requests	3

Conducting Data Protection Impact Assessments (DPIAs)	47

2023 Challenges & Risks

- **Challenge:** The ability of the Data Protection Office to adapt to conflicting priorities and meet regulatory obligations within current staffing levels.
- **Challenge**: Conflicting demands on finite resources in all Departments and Business Units across the University results in deprioritisation of Data Protection requests and risk reduction process improvements.
- **Risk:** Ongoing regulatory activities related to a Data Protection Commission inquiry into a security incident in 2018
- **Risk:** A relatively low level of uptake and completion of Data Protection training across all Departments and Business Units in the University could result in a lack of understanding of the obligations, for example, timely reporting of breaches.

GDPR Internal Audit Findings

- The Office is working to complete outstanding internal audit findings from the GDPR 2019 Internal Review, that was completed in 2020.
- 3 of 7 recommendations from the audit have been implemented.
- The four remaining recommendations are scheduled for completion in Q4 2024 and Q2 2025.

The implementation of the remaining recommendations from the internal review have been partially implemented for some time. The completion of the implementation needs to be balanced with adhering with the strict deadlines associated with FOI requests and DSARs.

Records of Processing Activities (ROPA)

In 2023, the DPC issued a Guidance Note on Record Of Processing Activities (ROPA) under Article 30 GDPR. A ROPA should be fit for purpose and effectively evidence of the University's GDPR Compliance. The DPO is updating the University's ROPA to ensure adherence to the Guidelines.

Focus and Priorities for 2024

- To procure and implement a new compliance software platform. The DP/FOI office is leading in the procurement of a compliance software solution that will provide a

comprehensive privacy management solution to assist in operationalising compliance and in facilitating a risk-based 'privacy by design' approach to compliance. It will assist with maintaining the Record of Processing Activity ("ROPA"), management of Data Sharing Agreements and facilitating staff training for data protection.

- Improved compliance with statutory requirements.
- Continue function specific training in high-risk data processing areas.
- Continue Webpage improvements for transparency and information.
- Training plan to be developed for Data Protection training.
- Publish an annual report on Data Protection function and activities.
- Strengthen Business Continuity Plan for Data Protection function.
- Continue to strengthen communication channels.
- Standardisation and centralisation of logging of security incidents and data breaches.
- Improvements to breach notification form to capture all required information in a right first time manner to reduce non-value added follow up communications.

Links and Useful Information

- Data Protection Act 2018
- GDPR
- Data Protection Commission (DPC)
- Maynooth University Data Protection Homepage
- DPC Annual Report 2023
- dataprotection@mu.ie