In the matter of the General Data Protection Regulation

Data Protection Commission Reference: IN-19-9-3

In the matter of Maynooth University

Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act 2018

Further to an own-volition inquiry commenced pursuant to Section 110 of the Data Protection Act 2018

DECISION

Decision-Makers for the Data Protection Commission:

Dr Des Hogan,
Commissioner for Data Protection
and
Dale Sunderland,
Commissioner for Data Protection

22 November 2024

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

1. Table of Contents

A. Introduction

1. This document (**'the Decision'**) is a decision made by the Data Protection Commission (**'the DPC'**) in accordance with section 111 of the Data Protection Act 2018 (**'the 2018 Act'**). The DPC makes this Decision having considered the information obtained in the own-volition inquiry (**'the Inquiry'**) pursuant to section 110 of the 2018 Act.

2. Reference to 'the **GDPR**' in this Decision is to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

3. The GDPR elaborates on the indivisible, universal values of human dignity, freedom, equality and solidarity as enshrined in the Charter of Fundamental Rights of the EU (**'the Charter'**) and Article 8 in particular, which safeguards the protection of personal data. Article 8 of the Charter provides:

    1. Everyone has the right to the protection of personal data concerning him or her.
    2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
    3. Compliance with these rules shall be subject to control by an independent authority.

4. This Decision considers particular aspects of this fundamental right in relation to the security of processing and compliance with responsibilities arising when a personal data breach has occurred.

5. This Decision is being provided to Maynooth University (**'MU'**) pursuant to section 116(1)(b) of the 2018 Act, in order to give notice of the Decision, the reasons for it, and the decision in relation to the powers exercised pursuant to Article 58 of the GDPR.

6. This Decision contains corrective powers under section 115 of the 2018 Act and Article 58(2) GDPR arising from the infringements that have been identified herein. It should be noted in this regard that MU is required to comply with the corrective powers that are contained in this Decision, and it is open to the DPC to serve an enforcement notice on MU in accordance with section 133 of the 2018 Act.

B. Legal Framework for the Inquiry and the Decision

a) Legal Basis for the Inquiry

7. The GDPR is the legal regime covering the processing of personal data in the European Union. As a regulation, the GDPR is directly applicable in EU member states. The GDPR is given further effect in Irish law by the 2018 Act. As stated above, the Inquiry was commenced pursuant to section 110 of the 2018 Act. By way of background in this regard, under Part 6 of the 2018 Act the DPC has the power to commence an inquiry on foot of a complaint or of its own volition.

8. Section 110(1) of the 2018 Act provides that the DPC may, for the purpose of section 109(5)(e) or section 113(2) of the 2018 Act, or of its own volition, cause such inquiry as it thinks fit to be conducted, in order to ascertain whether an infringement has occurred or is occurring of the GDPR or a provision of the 2018 Act, or of any regulation under the 2018 Act that gives further effect to the GDPR. Section 110(2) of the 2018 Act provides that the DPC may, for the purposes of section 110(1), where it considers it appropriate to do so, cause any of its powers under Chapter 4 of Part 6 of the 2018 Act (excluding section 135 of the 2018 Act) to be exercised and / or cause an investigation under Chapter 5 of Part 6 of the 2018 Act to be carried out.

b) Data Controller

9. In commencing the Inquiry, the DPC considered that MU may be the controller, within the meaning of Article 4(7) GDPR, in respect of personal data that was the subject of the personal data breach notifications. In this regard, MU confirmed in its email notification of the personal data breach to the DPC on 15 November 2018 that it was the controller.[1]

c) Legal Basis for the Decision

10. The decision-making process for the Inquiry which applies to this case is provided for under section 111 of the 2018 Act. This requires that the DPC consider the information obtained during the Inquiry to decide whether an infringement is occurring or has occurred and, if so, to decide on the corrective powers, if any, to be exercised. In so doing, the DPC is required to assess all of the materials and submissions gathered during the Inquiry and any other materials that it considers to be relevant.

11. Having considered all of the information obtained in the Inquiry, the DPC is satisfied that the Inquiry has been conducted correctly and that fair procedures have been followed throughout. The DPC has had regard to the submissions that MU made in

[1] Maynooth University, Email Notification to DPC, 15 November 2018.

respect of the Draft Decision before proceeding to make this final Decision under section 111 of the 2018 Act.

C. Factual Background

12. This matter concerns a series of events whereby an unauthorised person acquired control of up to six employee email accounts of MU staff members. By means of this, the unauthorised person could access the contents of and control those email accounts. In respect of one of them, the unauthorised person implemented rule changes to prevent certain emails from being seen by the account holder, and used their access to perpetrate a fraud by means of diversion of a pension payment involving a very significant payment by a MU employee.

13. Initial contact with the DPC was made by MU's Data Protection Officer on 15 November 2018 by email stating that

> a financial fraud has occurred at Maynooth University. This fraud concerns one member of staff and did not result in a personal data breach in this instance. A fraud investigation is being conducted by An Garda Síochána and an external independent cybersecurity company.[2]

14. This was followed, on 19 November 2018, with a formal notification of a potential data breach.[3] The data breach notification concerned how an employee email account had been accessed by an unauthorised person, resulting in a fraudulent transaction being executed to the significant financial detriment of another individual. MU stated that the incident was detected on 10 October 2018 but, as the matter was still under investigation at the time of notification, there was no further information with regard to the breach.

15. On 12 February 2019 MU submitted an updated breach notification form.[4] This stated that the incident occurred in September 2018 and was detected by a staff member in October 2018. The staff member reported the matter to MU's IT services on 10 October 2018. The update also indicated that a review of eight thousand potentially affected documents was under way. MU indicated that the categories of personal data may have been disclosed were data subject identity, PPSN, contact details, economic or financial data and location data.

16. The DPC team handling the breach notification wrote to MU on 13 February 2019 with a series of thirty-six questions. MU outlined in its 27 February 2019 response that

[2] Ibid.
[3] Breach Notification Form 19 November 2018.
[4] Updated Breach Notification 12 February 2019.

logons to Microsoft Office 365 from the geographic area from which the fraud was perpetrated were analysed and a further five cases, linked to the academic and campus services business units, were discovered. MU provided a record of processing activities associated with the departments of these five accounts. The records of processing activities provided by MU show that each of the departments handles a range of personal data, including the following datasets: student and staff CVs, Medical Certificates, exam scripts, HR Data, incident / accident reports, Health and Safety reports and resident details. In relation to these additional five accounts, MU stated that '[t]he business use of these email accounts would not have any requirement to use personal data. Therefore, a review of personal data is not being conducted in these cases.'[5]

17. In its email of 25 April 2019, MU confirmed that five additional email accounts linked to the academic and campus services business units were accessed by an unauthorised third party.[6] However, according to MU there were no mailbox rules or other mailbox configuration changes made to the mailboxes[7] and '[i]n each case the password was reset and there was follow-up with the employees involved.'[8]

18. MU informed the DPC that it had commissioned a report on the email fraud from Cybersecurity and Information Resilience (Ireland) Ltd. ('BSI'). BSI's report is dated 6 November 2018 and was delivered to MU at the latest on 8 November 2019.

19. The BSI report outlined that in September 2018, a MU employee had been dealing with a colleague responsible for [redacted] and an external financial firm concerning a substantia [redacted] payment. An unauthorised third party gained access to information concerning the proposed payment and, by means of [redacted] induced the employee to make the payment into a bank account controlled by the third party, leading to a substantial financial loss.[9]

20. The employee who was the victim of the fraud discovered what had happened on 10 October 2018 and reported the matter to MU. MU re-set that employee's password on the same day. The password of the MU employee dealing with [redacted] was re-set on 23 October 2018 'when [MU] became aware of the issues relating to it'.[10] Those 'issues' included the creation of 'rules' in the staff member's email account that hid emails from the victim and the [redacted] with whom the victim was dealing. The

[5] Response to DPC Questions (9) 18 Apr 2019, page 3.
[6] Response to DPC Questions (1) 25 Apr 2019.
[7] Maynooth University Submissions 1 Dec 2020.
[8] Maynooth University Submissions 1 Dec 2020, page 2.
[9] BSI Email Fraud Investigation Report, page 3.
[10] BSI Email Fraud Investigation Report, page 4.

creation of the rules indicated that an unauthorised person had gained access to the email account of the MU employee dealing with [redacted]

21. The BSI report also included an analysis of all records from the compromised email account of the MU employee who dealt with pension matters. Following review by MU's Data Protection Office,

> 653 data subjects were identified [as having personal data in records accessible through the breach]. It was possible to positively identify 463 data subjects. Where possible, they were contacted by email or letter and advised of the issues and concerns. They were advised to change their email account password immediately.[11]

22. In reviewing the matters raised in the breach report, the DPC considered it appropriate to establish a full set of facts so that it could assess whether or not MU had discharged its obligations as data controller in connection with the subject matter of the breach and to determine whether or not any provision(s) of the Act and / or the GDPR had been contravened by MU in that context. Accordingly, the DPC took the decision to conduct an Inquiry on its own volition into the suspected infringements.

23. The DPC issued an Inquiry Commencement Letter ('**the Commencement Letter'**) by email and registered post to MU on 7 November 2019 notifying MU that the DPC had commenced an Inquiry under and in accordance with section 110(1) of the 2018 Act. The letter notified MU that a number of areas would be examined as part of the scope of the Inquiry, including breach handling processes, IT policies and measures, remedial work since the breach and an analysis of the actions undertaken by MU following the breach. The Commencement Letter also contained twenty questions seeking further information from MU in relation to the circumstances of the breach.

24. The Commencement Letter set out the facts ascertained during the personal data breach notification and handling process. It explained that the Inquiry would formally document the relevant facts based on those documents and MU's responses to the DPC's queries as they relate to the subject of the Inquiry. That in turn would lead to a Draft Inquiry Report, on which MU would be invited to make submissions, and ultimately to a Final Inquiry Report that would be submitted to the DPC's decision-making process.

[11] Response to Commencement Letter, 15 November 2019, at pages 4-5.

25. MU provided submissions in response to the Commencement Letter on 15 November 2019.[12] In its submissions, MU outlined the technical and organisational measures which MU had in place to meet the requirements of the GDPR.

26. The DPC requested a response to four queries by 6 November 2020 in relation to measures that were in place at MU at the time of the notified breach.[13] On 9 November 2020, MU provided its response to those queries[14] in which it outlined the background to the breach, the engagement of BSI to investigate the matter, MU's policies and measures in place at the time of the breach, its VPN service, anti-malware, network management and monitoring, access to its data centre, staff system access, remote access, asset management, ICT Security and breach handling process. MU also provided further clarification on the types of personal data compromised in the breach including bank account number, bank sort code, date of birth, Irish IBAN, personal email address, PPS and spouse details.

27. The DPC contacted MU on 17 November 2020 with a further series of questions.[15] The DPC also stated in this letter that specific provisions of the GDPR envisaged as falling within the scope of the Inquiry would include-

- the security of personal data – an examination of compliance with Articles 5 and 32(1) GDPR with regard to the technical and organisational measures in place to ensure that there was adequate security over personal data held in manual or electronic form;

- Records of Processing Activities - whether MU had maintained the records required pursuant to Article 30 GDPR; and

- data breach notification - an examination of compliance with Articles 33 and 34 GDPR in relation to the reporting of the breach and communication with affected data subjects.

MU responded on 1 December 2020[16] with further information regarding its breach procedure, staff training, the controls in place at the time of the breach to safeguard confidentiality, integrity, availability and resilience of processing systems and services, and further information regarding its ICT Security services.

[12] Response to Commencement Letter, 15 November 2019.
[13] Queries to Maynooth University 15 Oct 2020.
[14] Maynooth University Response 9 Nov 2020.
[15] Letter to Maynooth University 17 Nov 2020.
[16] Maynooth University Submissions 1 Dec 2020.

28. Having received MU's submissions, the DPC prepared a Draft Report[17] to document the relevant facts established and the issues that fell for consideration by the DPC for the purpose making a decision under section 111 of the 2018 Act in respect of this Inquiry. The DPC furnished MU with the Draft Report on 7 January 2021[18] and invited MU's submissions on any inaccuracies and/or incompleteness in the facts. On 24 February 2021, MU provided its submissions[19] on the content of the Draft Report, which were reflected in the Final Report.[20]

29. MU was provided with a copy of the Draft Decision on 20 August 2024 and invited to make submissions on it. MU responded with its submissions on 27 September 2024. The DPC has carefully considered all of MU's submissions when drafting this Decision.

30. The DPC is obliged to consider all of the information obtained in the Inquiry and to reach conclusions as to whether it identifies infringements of data protection legislation. As set out above in Section A, this document is the Decision on this matter and it includes the corrective powers that the DPC has decided to exercise arising from the infringements that are identified herein.

D. Scope of the Inquiry and the Application of the GDPR

31. The scope of the Inquiry, which was set out in the Inquiry Commencement Letter, was to examine whether or not MU had complied with its obligations in relation to the processing of the personal data of its users and in connection with the subject matter of the notified personal data breach, to determine whether or not any provision(s) of the 2018 Act and/or the GDPR have been contravened by MU, in that context.

32. The Commencement Letter stated that the scope of the Inquiry would include the breach and the subsequent measures taken by MU. It also said that the Inquiry would focus on an examination of the breach handling process and GDPR awareness within MU, the IT policies, intrusion prevention and detection measures in place, the IT infrastructure supporting the delivery of MU's email system, the technical and organisational measures in place prior to the breaches occurring, the remedial technical and organisational measures implemented as the result of the breach, and a review of the decisions made by MU not to conduct an analysis of the five identified email accounts accessed from the same geographic area from which the business email compromise breach originated. The Commencement Letter also indicated that a

[17] DPC Maynooth University Draft Inquiry Report, 07 January 2021.
[18] Maynooth University Draft Report Cover Letter, 07 January 2021.
[19] Maynooth University Response to draft report, 24 February 2021.
[20] Maynooth University Final Report, 05 March 2021.

contravention of Article 33 of the GDPR may have occurred with regard to the reporting of the data breach.[21]

33. In its submission on the Draft Decision, MU asserted that the premise of the inquiry was a fraudulent transaction being carried out to the financial detriment of an individual.[22] The DPC takes this opportunity to clarify that the premise of the inquiry is as stated in the Commencement Letter and includes a range of issues arising from, or disclosed in consequence of the notified breach, not just the incident that gave rise to the notification.

34. Article 2(1) GDPR defines the Regulation's scope as follows:

> This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

35. Article 4(1) GDPR defines 'personal data':

> '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;

36. Article 4(6) GDPR defines 'filing system':

> '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;

37. The material scope of the GDPR under Article 2 applies to processing of personal data. In this case, MU indicated that the breached data may have contained personal data, including data subject identity, PPSN, contact details, economic or financial data and location data.[23] The personal data of users that is processed by MU meets the definition for personal data under Article 4(1) GDPR. The breach concerned a number of employee accounts which were hacked, thus allowing unauthorised access to personal

[21] Inquiry Commencement Letter, 07 November 2019.
[22] Maynooth University Submission on Draft Decision, 27 September 2024 , at page 2.
[23] Updated Breach Notification 12 February 2019.

data held by MU. Therefore, the processing of personal data by MU via computing systems falls within the scope of the GDPR.

38. Article 5(1)(f) GDPR provides for the principle of integrity and confidentiality. It requires that 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 ('integrity and confidentiality').

39. Article 32(1) GDPR elaborates on the principle of integrity and confidentiality in Article 5(1)(f) GDPR by setting out criteria for assessing what constitutes 'appropriate security' and 'appropriate technical or organisational measures':

> Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
>
> a) the pseudonymisation and encryption of personal data;
>
> b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
>
> c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
>
> d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

40. Articles 5(1)(f) and 32(1) GDPR oblige controllers and processors to implement a level of security appropriate to the risks presented by the processing of personal data. There is an obligation to take into account 'the state of the art' with regard to measures

available. That term is not defined in the GDPR, but its dictionary definition is 'using the latest techniques or equipment'.[24]

41. Article 33(1) GDPR sets out obligations placed on a data controller with regard to the notification of a personal data breach:

> In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

E. Issues for Determination

42. In the Final Report[25] the Case Officer was of the view that facts and materials indicated that contraventions of the following provisions of the GDPR had occurred:

- **Article 5(1)(f)** in respect of the integrity and confidentiality of personal data processed by MU,
- **Article 32(1)** in respect of MU's obligations concerning the security of personal data that it processed, and
- **Article 33(1)** in respect of MU's obligation to notify the DPC of personal data breaches as provided in that Article.

43. Therefore, having considered the Commencement Letter, the updated Final Report including MU's submissions on it, and the other relevant materials, the DPC must determine in this Decision whether MU has complied with those aspects of its obligations under Articles 5(1)(f), 32(1) and 33(1) GDPR in respect of its processing of personal data.

F. Analysis of the Issues for Determination

a) Issue 1: Articles 5(1)(f) and 32(1) GDPR

44. Article 5(1)(f) GDPR provides for the principle of integrity and confidentiality. It requires personal data to be:

---

[24] Concise Oxford Dictionary, (8th ed., BCA & Oxford University Press, 1991).
[25] DPC Final Inquiry Report on Maynooth University, 5 March 2021.

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.

45. Article 32(1) GDPR provides:

> 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate*:*
>
> (a) the pseudonymisation and encryption of personal data;
> (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
> (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
> (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

46. In considering the technical and organisational measures that a controller or processor must implement, regard must be had to a risk assessment concerning the rights and freedoms of natural persons, the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing.

47. Article 32(2) GDPR provides:

> In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

i) Assessment of the Risks

48. The level of security that controllers and processors are obliged to implement must be appropriate to the risk posed to the rights and freedoms of natural persons by the personal data processing. Regarding MU's processing of personal data via its email and IT systems, those risks include the risk of unauthorised access or unauthorised disclosure of personal data to third parties. It also includes the risk of loss of control

over personal data, identity theft and financial loss as a result of unauthorised access or disclosure.

49. In implementing measures pursuant to Article 32 GDPR, the controller must have regard to the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing. Recital 75 to the GDPR provides examples of risks to the rights and freedoms of natural persons. These risks may include physical, material or non-material damage to natural persons.

50. In particular, Recital 75 specifies the following relevant risks to the rights and freedoms of natural persons:

> The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

51. Recital 76 GDPR provides guidance as to how risk should be evaluated:

> The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.

52. Therefore, in complying with the requirements of Article 32, controllers should start by identifying the risks to the rights of data subjects that a violation of the principles presents. They must have regard to the likelihood and severity of those risks and must implement measures to effectively mitigate them.

53. Determining the appropriate level of security requires an objective assessment of the risks presented by the processing. Risk must be assessed by reference to (i) the likelihood of the risk, and (ii) the severity of the risk to the rights and freedoms of natural persons. Hence, the risk assessment for MU's processing should have considered first the likelihood of personal data, including financial data, being subjected to unauthorised access, alteration, destruction or disclosure. It should then have assessed the severity of that risk in respect of the rights and freedoms of natural persons. These assessments should have been made by reference to the nature, scope, context and purposes of the processing. In considering these factors, regard should also have given to the quantity of personal data processed and the sensitivity of that data. Such an assessment should have been conducted when the processing was first proposed, and revised as appropriate when circumstances (such as changes in technology, usage or other relevant factors) so required. From when the GDPR came into effect, MU was obliged under Article 32 GDPR to assess the risk associated with its processing if such risk assessment had not already been conducted. (The DPC notes that similar obligations in respect of risk existed in law before the GDPR came into effect).

54. MU was asked to provide specific information about the measures in place to comply with Article 32 by reference to the principle set down in Article 5(1)(f) GDPR in terms of an assessment of the risks of varying likelihood and severity associated with the forms of data processing activities involved in the notified breach.[26] MU provided a copy of its 'Personal Data Security Incident Management Procedure'.[27] MU stated that the procedure advises staff to contact the DPO 'in any case where they suspect an incident has occurred or if there are any concerns.'[28] While this document outlines steps to be taken in respect of a security incident, it does not outline any assessment of the risks associated with MU's processing of personal data, nor does it outline any measures implemented to mitigate risk and reduce the risk of a security incident occurring in the first place.

55. MU was asked to provide details of any risk assessment undertaken with regard to the security of its email and IT systems. In response, MU stated that BSI had carried out an

[26] Queries to Maynooth University 15 Oct 2020.
[27] Personal Data Security Breach Incident Management Procedure.
[28] Personal Data Security Breach Incident Management Procedure, page 1.

investigation of the email fraud and provided MU with an incident report.[29] However, that investigation was carried out after the breach had occurred.

56. MU's email and IT systems processed data in respect of a significant number of data subjects. This included data subject identity, PPSNs, contact details, economic or financial data and location data.[30]

57. The purpose of the processing was determined by MU in order to facilitate work processes. The risks associated with unauthorised persons being able to access and use another user's email account include identity theft, fraud and financial loss.[31]

58. In the circumstances, the DPC considers that MU's processing of personal data via its email system presented a high risk in terms of likelihood of unauthorised access. The DPC makes this finding in light of the large number of email accounts, the quantity of personal data potentially stored on any given account, the broad scope of the processing. The facts disclosed during the Inquiry established that the same email system was used across MU not just for day-to-day communications, but also for highly sensitive subjects such as [redacted] and other topics deserving of particular security. The quantity of personal data processed, the number of users and the purposes of that processing together posed a significant risk in case of, for example ransomware attacks, phishing and other attacks. This underscores the need for appropriate measures to mitigate such risks.

59. The severity of the risks to the rights and freedoms of data subjects was also high. The DPC makes this finding in light of nature of the personal data processed in the email accounts, as outlined in the preceeding paragraph. This processing entailed a significant amount of personal and financial data, access to which ought to have been limited to authorised MU users, whether by means of encryption, restricted access to email services or otherwise. In the event of unauthorised access by bad actors, data subject identity, PPSNs, contact details, economic or financial data and location data could be misused to the serious detriment of data subjects. Therefore, having regard to this risk, it was incumbent on MU to implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, as required by Article 32 GDPR.

[29] BSI Email Fraud Investigation Report.
[30] Updated Breach Notification, 12 Feb 2019.
[31] See Recital 75 GDPR.

ii) Measures Implemented by MU to Address the Risks

60. The principle of integrity and confidentiality set out in Article 5(1)(f) GDPR requires that the controller 'ensures appropriate security of the personal data when processing using appropriate technical or organisational measures.' Article 32(1) GDPR requires that the controller shall assess the risk to data subjects of the particular processing and shall implement 'appropriate technical and organisational measures to ensure a level of security appropriate to the risk,' taking into account the factors listed in that Article.

61. MU's submissions outlined the technical and organisational measures that it had in place at the time of the personal data breaches to ensure the ongoing confidentiality and integrity of personal data processing in its email system. These measures can be categorised as follows:

    a) Training and awareness

    b) Security of personal data

        (i) Technical measures

        (ii) Organisational measures

Training and Awareness

62. MU provided details of its training for staff and clarified when data protection user awareness training for staff last took place prior to the breach:

> The Data Protection Officer sourced and customised on-line training module on GDPR and Data Protection user awareness, MU and staff obligations, how to report a breach and to whom and so on. This module was made available on-line from March 2018 to all staff including all newly appointed staff. Scheduled reminders were sent to those staff who had not completed the training.[32]

63. An online GDPR training module was available to all staff and, at the time of the breach, had been undertaken by 70% of staff. MU indicated that the staff member whose email account was compromised (staff member 'Y') had completed that training on 13 April 2018. The DPC notes that MU now supports training for staff in Data Protection issues, which MU states was 'something that was only in its infancy in 2018'. In addition, MU states that it now has 'a suite of policies and procedures in place in relation to GDPR' that are regularly reviewed. However, these improvements in training practices were put in place after the breach occurred.

[32] Response to Commencement Letter, 15 November 2019, page 4.

64. MU stated that it has an agreement with a shared service provider since March 2018 for provision of user awareness training 'including training on cyber threats resulting from phishing and malware. Sign-in sheets are retained, each stating the date and time along with list of attendees at individual training sessions (available if required)'.[33]

Security of Personal Data

Technical Measures

65. MU described specific technical measures that it stated were in place at the time of the breach, including:

- At the time of the breach, [redacted] required two-factor authentication.
- All accounts were password protected, and email account holders and users were explicitly prohibited from sharing usernames, emails or passwords.
- All accounts had auditing enabled, allowing MU to check for suspicious activity performed on accounts.
- MU could check a user's sign-in location and the OS of device being used for access, as well as perform a message trace or content search on a user account for the previous 90 days.
- Anti-malware was installed on all the Windows machines and was configured to automatically update.
- Perimeter monitoring using [redacted] and logging were active and in place across the university network.
- [redacted] was in place for monitoring operating systems, mobile telephones, and terminals used for certain card payments.
- MU retained logs for [redacted].
- Access to MU's data centre was restricted and that the [redacted]
- Third-party or remote access was managed through [redacted]
- Systems used encryption at rest and in transit with SSL/TLS.

[33] Response to Commencement Letter, 15 November 2019, page 2.

[34] [redacted].

- Threat management, security monitoring, and file/data integrity check, prevented and/or detected any tampering of data.
- [redacted] provided protection against spam and malware
- There were regularly scheduled internal and external scans, penetration tests on key systems and services.

66. Article 32 GDPR states that the data processor 'shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk' including:

> (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; …
>
> (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

67. While MU did have a range of technical measures in place, as listed above, they were inadequate given the nature and type of processing being carried out. There were a number of key deficiencies with regard to the security of personal data at the time of the breach, including:

- a lack of Multi Factor Authentication ('**MFA**') for user accounts. At the time of the breach, only MU's [redacted] required two-factor authentication,[35]
- inadequate anti-spam configuration,
- a lack of rules requiring passwords to be expired after a set period of time,[36]
- no controls in place to prevent users automatically forwarding emails to external email addresses,
- no policy prohibiting or configuration preventing the creation of email forwarding rules.[37]

68. In addition, some of the devices in use by the compromised accounts had significant security issues:

- Two were running an outdated version of Java, which was no longer supported with security patches.

[35] Maynooth University Response 9 Nov 2020, page 2-3.
[36] BSI Email Fraud Investigation Report.
[37] Response to DPC Questions (36) 27 Feb 2019.

- Several machines had not applied up to date security patches.
- One PC contained four instances of a JavaScript Trojan malware variant.
- Another PC contained four Trojan malware variants associated with bitcoin mining.
- One machine was not configured to apply Windows security updates.[38]

69. An appropriate level of security includes technical measures that have, among other things, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. While MU had technical measures in place at the time of the breach, the lack of MFA, inadequate anti-spam configuration and multiple instances of malware means that the level of technical security measures was not sufficient to ensure the safety and confidentiality of the data being processed by MU via its email systems. Therefore, the DPC considers that technical security measures in place at the time of the breach did not meet the standards required by Article 5(1)(f) or Article 32(1) GDPR.

Organisational Measures

70. MU outlined its organisational measures relating to security, including:

- 'Personal Data Security Incident Management Procedure'[39]
- 'Cybersecurity Incident Register'[40]
- 'Data Incident Response for Phishing'[41]
- 'Responsible Usage Policy'[42]
- 'Code of Conduct of Users of Computing Facilities'[43]

71. However, both the 'Personal Data Security Incident Management Procedure' the 'Cybersecurity Incident Register' and the 'Data Incident Response for Phishing' document dated from 2019 – that is, after the occurrence of the breach that is the subject of the inquiry. The DPC notes that '[t]here have been significant changes in MU's capacity to prevent and/or deal with this type of incident since 2018.'[44]

[38] Report on the Examination of Certain Staff Computers.
[39] Personal Data Security Breach Incident Management Procedure.
[40] Cybersecurity Incident Register.
[41] Data Incident Response for Phishing.
[42] https://www.maynoothuniversity.ie/sites/default/files/assets/document/Responsible Computing Policy Jan 2015_0.pdf
[43] https://www.maynoothuniversity.ie/sites/default/files/assets/document//Code of Conduct for Users of Computing Facilities Jan2015.pdf
[44] Maynooth University Submission on Draft Decision, page 2.

72. MU maintained a risk register at university and department (IT Services) level and also assessed and evaluated the effectiveness of the technical and organisational measures using Internal Audit, External Audit, and Risk Assessment.[45]

73. MU also had a partnership with a shared service provider, which provided the following services:

- General ICT Security Awareness Training
- ICT Security Policy Reviews
- Security and Perimeter Assessments
- Access to Cyber Security Competence

74. However, MU indicated that at the time of the breach it had no controls in place to prevent users automatically forwarding emails to external email addresses. MU also indicated that it did not conduct reviews in relation to forwarding rules to ensure there were no unnecessary or unapproved rules.

75. MU advised that it did not have a policy in place advising employees as to what categories of data could be stored on work devices. MU stated that all email accounts were password protected and that email account holders and users were explicitly prohibited from sharing usernames, emails or passwords as set out in its 'Code of Conduct for Users of Computing Facilities 2015'.[46] However, MU also stated that '[t]here was no specific password policy in place at the time of the breach.'[47] Subsequent to the breach, in June 2019, MU developed such a policy.

76. While, as outlined above, MU had some organisational security measures in place at the time of breach, the lack of controls and reviews with regard to email forwarding, as well as the lack of a data storage policy for employees, of a password policy and of policies relating to phishing or security incidents at the time of the breach meant that adequate organisational measures were not in place to ensure the ongoing security of personal data processed by MU. Therefore, the DPC considers that organisational security measures in place at the time of the breach did not meet the standards required by Article 5(1)(f) or Article 32(1) GDPR.

[45] Maynooth University Response 9 November 2020, page 5.
[46] Code of Conduct for Users of Computing Facilities 2015.
[47] Response to DPC Questions (36) 27 February 2019, page 4.

b) Issue 2: Article 33 GDPR

i) Personal Data Breach

77. Article 4(12) GDPR defines 'personal data breach' as

> 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;

78. In the present case, an unauthorised person was known to have gained access to the employee email accounts of several MU staff members. That such unauthorised access could occur to records containing personal data demonstrated 'a breach of security' as that term is understood in Article 4(12) GDPR. The access also allowed the unauthorised person to change the configuration of email accounts to hide messages from the account holder, and to perpetrate a serious financial fraud. The DPC was therefore satisfied that all elements of the definition in Article 4(12) had been met, and that a personal data breach had occurred.

ii) The Obligation to Notify Without Delay

79. Article 33 sets out the requirements in respect of notification by a controller to the supervisory authority of a personal data breach. Article 33(1) GDPR provides:

> In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

80. The obligation to notify the DPC applies to all personal data breaches unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Under Article 4(12), a 'personal data breach':

> means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

81. Article 33(1) requires notifications to be made 'without undue delay.' This must be assessed by reference to when MU became aware of the personal data breach. In its

'Guidelines 9/2022 on Personal Data Breach Notification under GDPR' the EDPB addressed the meaning of the term 'undue delay' in the related context of the requirement to communicate a breach to affected individuals under Article 34 GDPR:

> The GDPR states that communication of a breach to individuals should be made 'without undue delay,' which means as soon as possible. The main objective of notification to individuals is to provide specific information about steps they should take to protect themselves.

82. The Guidelines further provide that:

> a controller should be regarded as having become 'aware' when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. However…the GDPR requires the controller to implement all appropriate technical protection and organizational measures to establish immediately whether a breach has taken place and to inform promptly the supervisory authority and the data subjects. It also states that the fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the breach and its consequences and adverse effects for the data subject. <u>This puts an obligation on the controller to ensure that they will be 'aware' of any breaches in a timely manner so that they can take appropriate action.</u>[48]

83. The Guidelines go on to consider cases where there is uncertainty as to whether a personal data breach has occurred:

> In some cases, it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised. However, the emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required.

84. Recital 87 of the GDPR states:

> It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was

[48] Emphasis added.

made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

85. The Breach Notification Guidelines state that:

> [T]he GDPR requires both controllers and processors to have in place appropriate technical and organizational measures to ensure a level of security appropriate to the risk posed to the personal data being processed. They should take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Also the GDPR requires all appropriate technological protection and organizational measures to be in place to establish immediately whether a breach has taken place, which then determines whether the notification obligation is engaged. Consequently, a key element of any data security policy is being able, where possible, to prevent a breach and, where it nevertheless occurs, to react to it in a timely manner.[49]

86. In considering whether MU complied with its obligation to notify a personal data breach under Article 33(1), therefore, the DPC has considered the objectives underlying this obligation and the broader context in which this obligation arises.

iii) The Breach Notification

87. According to MU, a fraudulent transaction occurred in September 2018, which was uncovered in mid-October 2018. This led MU to commission the BSI report, which MU received, at the latest, on 8 November 2018. That report determined that a personal data breach had likely occurred and recommended, among other things, that MU should notify its Data Protection Officer of the incident.[50] MU's Data Protection Officer stated that the MU Data Protection Office was informed of the incident on 12 November 2018.[51] MU's Data Protection Officer sent the DPC and email outlining the nature of the incident (concluded to be a financial fraud) on 15 November 2018.[52] That email stated that MU would review the affected email accounts to establish if any

[49] Breach Notification Guidelines, page 6.
[50] BSI Email Fraud Investigation Report, page 21.
[51] Breach Notification Form 19 November 2018, page 2.
[52] Email Notification 15 November 2018.

personal data could have been compromised. MU sent a formal breach notification on 19 November 2018.[53]

88. On 12 February 2019, MU submitted an updated breach notification form to the DPC.[54] This stated that the incident occurred in September 2018 and was detected by a staff member in October 2018. The staff member reported the matter to MU's IT services on 10 October 2018.

89. In its submissions on the Draft Decision, MU states that

> the incident could potentially involve a breach of personal data but there is no evidence that it did lead to such a breach. The only evidence of a breach of personal data is the data voluntarily provided by the victim of this crime.

Article 4(12) GDPR makes clear that personal breaches include not only issues regarding the destruction, loss or alteration of personal data, but also defines a personal data breach as including cases where a breach of security leads to 'unauthorised disclosure of, or access to, personal data'. (Emphasis added.) The DPC is of the view that there was undeniable access to personal data in or accessible through MU email accounts by unauthorised persons.

90. MU further states that

> Following review of the BSI report, and its recommendation that the incident be reported to the DPC as a breach may have taken place, the University reported the incident to the DPC without delay. It was reported within 72 hours of the MU Data Protection Officer ("DPO") becoming aware of the incident and determining that it should be reported.[55]

This is not disputed. However, Article 33(1) states that

> the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority

Therefore, the obligation to report under Article 33(1) arises when the controller becomes aware of the personal data breach. In this case, MU was, or should have been,

[53] Breach Notification Form 19 November 2018.
[54] Updated Breach Notification 12 February 2019.
[55] Maynooth University Submission on Draft Decision, 27 September 2024, page 2.

aware of the breach no later than 23 October 2018 when it became known that the MU email account of an employee had been interfered with by an unauthorised person.

91. MU in its submission further states that 'the BSI recommendation was for the IT Department in the University to report it to the MU DPO, and this was done.'[56] However, the fact remains that MU, as the controller, is responsible for reporting a data breach and the DPC remains of the opinion that there had been a notifiable breach and this was evident even before delivery of the BSI report.

92. Controllers are not under an obligation to notify the DPC if a personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. However, the DPC is satisfied that the personal data breach did result in such a risk, as evidenced by the financial fraud perpetrated. In assessing risk, regard must also be had objectively to both the likelihood and severity of the risk to the rights and freedoms of data subjects. In assessing risk it is appropriate to have regard to the number of affected individuals. It is also appropriate to have regard to whether the personal data has arrived into the possession of individuals whose intentions are unknown or potentially malicious. In this respect, the breach is likely to have occurred as a result of a phishing attack or malware such as a key logger, and led to suspicious logins from [redacted].[57]

93. MU in its submission on the Draft Decision states that, because MU compensated the victim of the financial fraud, there is no evidence that 'any detriment has fallen to any person whose personal data was compromised as of today'.[58] However, a failure to implement an appropriate level of security increases the risk of personal data breaches, which is the critical point. An increased risk of personal data breaches in turn poses a threat to the rights and freedoms of natural persons because of the potential for damage to them where personal data breaches occur, leading to, inter alia, unavailability or destruction of essential personal data or unauthorised access, alteration or disclosure of that personal data. A failure to implement an appropriate level of security is an infringement of the GDPR.

94. In the circumstances, the DPC is satisfied that the personal data breach resulted in a risk to the rights and freedoms of data subjects, including, but not limited to, the risk of phishing attacks utilising the personal data compromised. Therefore, MU was obliged to notify the DPC of the personal data breach without undue delay.

95. The [redacted] occurred in September 2018 and came to light in October 2018. MU reset the password of the victim of the fraud on her MU laptop once the fraud incident

[56] Maynooth University Submission on Draft Decision , 27 September 2024, page 2.
[57] BSI Email Fraud Investigation Report, page 4.
[58] Maynooth University Submission on Draft Decision , 27 September 2024, page 2.

was discovered.[59]MU was therefore at least on notice of a possible breach on 10 October 2018, and either was, or should have been, aware that a breach of its email system had occurred on 23 October 2018, when it discovered unauthorised access to the email account of the employee [redacted] and re-set her password.[60] In its submission on the Draft Decision MU states that

> [w]hen the incident first came to light in 2018, it was not possible for anyone to quickly determine whether any personal data was compromised within MU. The University commissioned BSI for exactly that purpose.[61]

However, the DPC finds that it was apparent at the latest by 23 October 2018 that the MU email account of the HR employee dealing with pensions had been improperly accessed and rules created on it. That by definition involved unauthorised access to personal data in or accessible through that account. The requirement to notify the DPC under Article 33 GDPR therefore arose at the latest on 23 October 2018. However, MU deferred notification pending receipt of the BSI report, which was delivered at the latest on 8 November 2018. MU's Data Protection Office was not informed of the report's findings and recommendations until 12 November 2018.

96. The DPC was not notified and given the information required under Article 33 GDPR until 19 November 2018. This was a violation of the controller's obligation under that Article to notify the supervisory authority of a personal data breach without undue delay and, where feasible, within 72 hours of MU becoming aware of the breach. In the particular circumstances, the DPC finds that it was feasible for MU to notify the DPC within 72 hours after MU definitively became aware of the breach on 23 October 2018.

G. Findings Regarding Articles 5(1)(f), 32(1) and 33(1)

97. For the reasons set out above in Section F, the DPC finds that MU

- infringed the principle of security of Article 5(1)(f) GDPR by failing to ensure appropriate security of the personal data related to its email accounts using appropriate technical and organisational measures.

- infringed Article 32(1) GDPR by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its processing of personal data within its email system.

[59] BSI Email Fraud Investigation Report, pages 3 and 4.
[60] Ibid, page 4.
[61] Maynooth University Submission on Draft Decision , 27 September 2024, page 1.

- infringed Article 33(1) GDPR by its failure to notify the DPC within 72 hours of the data breach.

H. Decision on Corrective Powers

98. The DPC has set out above, pursuant to section 111(1)(a) of the 2018 Act, its decision to the effect that MU has infringed Articles 5(1)(f), 32(1) and 33(1) GDPR.

99. Under section 111(2) of the 2018 Act, where the DPC makes a decision under section 111(1)(a), it must, in addition, make a decision as to whether a corrective power should be exercised in respect of the controller or processor concerned and, if so, the corrective power to be exercised. The remaining question for determination in this Decision is whether or not any of those infringements merit the exercise of any of the corrective powers set out in Article 58(2) GDPR and, if so, which corrective powers.

100. Article 58(2) GDPR sets out the corrective powers that supervisory authorities may exercise in respect of non-compliance by a controller or processor. In deciding whether to exercise those powers, Recital 129 provides guidance as follows:

> …each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case…

101. Having carefully considered the infringements identified in this Decision, the DPC has decided to exercise certain corrective powers in accordance with section 115 of the 2018 Act and Article 58(2) GDPR. In summary, the corrective powers that the DPC has decided are appropriate to address the infringements in the particular circumstances are:

    a. An order to MU pursuant to Article 58(2)(d) GDPR to bring its processing operations into compliance with Articles 5(1)(f) and 32(1) GDPR in the manner specified below;

    b. A reprimand to MU pursuant to Article 58(2)(b) GDPR in respect of its infringements of Articles 5(1)(f), 32(1) and 33(1) GDPR; and

    c. Administrative fines for the infringements of Articles 5(1)(f), 32(1) and 33(1) GDPR.

102. Set out below are further details in respect of each of the corrective powers that the DPC intends to exercise and the reasons why it has decided to exercise them.

I. Order to Bring Processing into Compliance

103. Article 58(2)(d) GDPR provides that a supervisory authority shall have the power

> to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period

104. In circumstances where it has found that the processing at issue was not in compliance with the GDPR, the DPC makes an order pursuant to Article 58(2)(d) GDPR. Therefore, the DPC orders MU to bring the relevant processing into compliance with Articles 5(1)(f) and 32(1) GDPR through implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risks. MU must perform the necessary risk assessment to inform the measures that it must implement.

105. It is the DPC's view that these orders are appropriate, necessary and proportionate in view of ensuring compliance with Articles 5(1)(f) and 32(1) GDPR. In this regard, the DPC acknowledges MU's on-going remedial actions, as outlined in submissions throughout the Inquiry, as well as the fact that

> MU has implemented a number of measures (both in the immediate aftermath of the incident but also in the years since 2018) to further strengthen ICT security and enhance the University's ability to fulfil its responsibilities under GDPR.[62]

106. The orders that the DPC imposes are set out below:

a) The implementation of MFA for all user accounts.

b) A review of anti-spam configuration and policies, including regular review and updates as the risk landscape changes.

c) Regular security updates of software.

d) A robust password management policy including processes, methods and techniques for secure storing of user passwords .

e) Mandatory data protection and cyber security training for all staff, appropriate to their role and level of risk, and updated as the risk landscape changes.

[62] Maynooth University Submission on Draft Decision, 27 September 2024, page 1.

f) Development of policies to respond to data breaches and data security incidents in ways that are appropriate to the risks posed and that ensure compliance with MU's obligations as a data controller under the GDPR.

107. The DPC's decision to impose the orders is made to ensure that full effect is given to MU's obligations under Articles 5(1)(f), 32(1) and 33(1) GDPR. The DPC considers that these orders are appropriate, necessary and proportionate in view of ensuring compliance with the GDPR.

108. The DPC considers that these orders are necessary to ensure that full effect is given to MU's obligations in relation to the data security infringements outlined above.

109. The substance of this order is the only way in which the defects pointed out in this Decision can be rectified, which is essential to the protection of the rights of data subjects. It is on this basis that the DPC takes the view that this power should be imposed.

110. Having regard to the non-compliance identified in this Decision, the DPC considers such orders are proportionate and are the minimum required to guarantee compliance in the future. The DPC is satisfied that the orders are necessary and proportionate.

111. The DPC therefore requires MU to comply with the above orders within three months from the date of notification of the final decision. The DPC additionally requires MU to submit a report to the DPC within a month after the date of notification of this decision, detailing the actions it has taken to comply with the orders.

J. Reprimand

112. Article 58(2)(b) GDPR provides that a supervisory authority shall have the power

> to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation

113. In its submission on the Draft Decision, MU asserts that

> GDPR responsibilities only became effective from May 2018 and MU, like other public sector bodies, was still adapting to the new regulatory landscape at the time of the incident.[63]

However, the provisions of the GDPR had been known to controllers for two years previously. MU was obliged to respond to the standards it imposed and had ample

[63] Maynooth University Submission on Draft Decision, 27 September 2024, page 1.

technical and organisational resources to do so. The facts demonstrate that it failed to meet those standards. That is a sufficient basis for the use of the DPC's corrective powers including the issuing of a reprimand.

114. The DPC is issuing MU a reprimand in respect of its infringements of Articles 5(1)(f), 32(1) and 33(1) GDPR identified in this Decision. The purpose of the reprimand is to dissuade non-compliance with the GDPR. The DPC considers that a reprimand is necessary and appropriate in respect of such non-compliance in order to recognise formally the serious nature of the infringements and to dissuade such non-compliance. The reprimand will contribute to ensuring that MU and other controllers and processors take appropriate steps in relation to current and future processing and notification obligations, in order to comply with their obligations under GDPR.

K. Decision on administrative fines

115. Article 58(2)(i) GDPR provides that a supervisory authority shall have the power

> to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case

116. The purpose of administrative fines is to strengthen the enforcement of the rules of the GDPR.[64] Fines sanction non-compliance and seek to re-establish compliance with the GDPR.

117. As the DPC has identified infringements of the GDPR above, it will decide whether to impose administrative fines in respect of those infringements. In conducting this assessment, the DPC has had regard to Article 83 GDPR, which sets out 'General conditions for imposing administrative fines.' The DPC has also had regard to EDPB guidelines which are designed to ensure a harmonised approach to fining. These include the EDPB's Guidelines on the calculation of administrative fines ('the EDPB Fining Guidelines'),[65] and the Article 29 Working Party's Guidelines on the application and setting of administrative fines ('the A29WP Fining Guidelines'),[66] which have been endorsed by the EDPB.

118. As a first step, the DPC will consider whether to impose a fine by applying the criteria set out in Article 83(2) GDPR. If the outcome of the assessment is that a fine should be

[64] GDPR, Recital 148.
[65] European Data Protection Board, 'Guidelines 04/2022 on the calculation of administrative fines under the GDPR', version 2.1, adopted on 24 May 2023.
[66] Article 29 Data Protection Working Party, 'Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679', WP253, adopted on 3 October 2017, endorsed by the EDPB on 25 May 2018.

imposed, then the DPC will proceed to calculate the amount by reference to the criteria in Article 83(2) GDPR and by considering the other factors set out in Articles 83(1)-(9) that apply in this case. In particular, Article 83(1) GDPR requires fines to be effective, proportionate and dissuasive. These principles have informed the calculation of the fines imposed in this Decision.

a) Whether to impose an administrative fine

119. Article 83(2) GDPR states,

> Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following…

120. Article 83(2) lists 11 criteria from (a) to (k) to be taken into account when deciding whether to impose an administrative fine. Those criteria are set out below where they are also applied to the infringements identified herein.

i) Article 83(2)(a) GDPR: the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

121. Article 83(2)(a) requires consideration of the identified criterion by reference to 'the infringement' as well as 'the processing concerned.' The phrase '**the processing concerned**' in this Article 83(2) analysis should be understood to mean all of the processing operations that MU carries out on personal data regarding the delivery of MU's email and IT systems.

122. Considering next the meaning of 'infringement', it is clear from Articles 83(3)-(5) that this means an infringement of a provision of the GDPR. The DPC has found that MU infringed Articles 5(1)(f), 32(1) and 33(1). Therefore, '**the infringement'**, for the purpose of the DPC's assessment of the Article 83(2) criteria, should be understood (depending on the context in which the term is used) to mean an infringement of Articles 5(1)(f), 32(1) and 33(1). While each is an individual 'infringement' of the relevant provision, they all relate to the processing concerned and, by reason of their common nature and purpose, are likely to generate the same, or similar, outcomes in the context of some of the Article 83(2) assessment criteria. Accordingly, and for ease of review, the DPC will assess all of these infringements simultaneously, by reference to the collective term '**infringements'** unless otherwise indicated.

123. As all of the infringements relate to the processing concerned, the considerations and assessments set out below, save where otherwise indicated, should be understood as being assessments of the individual Article 83(2) criteria in the context of the infringements generally.

Taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them

124. This section will consider the nature, scope or purpose of the processing concerned, before considering the number of data subjects affected and the level of damage suffered by them.

125. The nature of the processing can include:

> the context in which the processing is functionally based (e.g. business activity, non-profit, political party, etc.) and all the characteristics of the processing.'[67]

126. Circumstances that can lead to supervisory authorities attributing more weight to this factor include

> where the purpose is to monitor, evaluate personal aspects or to take decisions or measures with negative effects for data subjects, where there is a clear imbalance between the controller and data subjects or where the processing involves children or other vulnerable data subjects.[68]

127. The nature of the processing relating to the infringements identified herein is MU's processing of personal data via its email and IT systems.

128. The **scope** of the processing is assessed

> with reference to the local, national or cross-border scope of the processing carried out and the relationship between this information and the actual extent of the processing in terms of the allocation of resources by the data controller… The larger the scope of the processing, the more weight the supervisory authority may attribute to this factor.[69]

[67] EDPB Fining Guidelines [53.b.i].
[68] Ibid.
[69] EDPB Fining Guidelines [53.b.ii].

129. The scope of the processing relating to the infringements identified herein is broad. This is due to the large number of email accounts, the quantity of personal data potentially stored on any given account, and the broad scope of the processing on a national level. The data processed included data subject identity, PPSN, contact details, economic or financial data and location data.[70]

130. The purpose of the processing

> will lead the supervisory authority to attribute more weight to this factor. The supervisory authority may also consider whether the processing of personal data falls within the so-called core activities of the controller. The more central the processing is to the controller's or processor's core activities, the more severe irregularities in this processing will be. The supervisory authority may attribute more weight to this factor in these circumstances. There may be circumstances though, in which the processing of personal data is further removed from the core activities of the controller or processor, but significantly impacts the evaluation nonetheless (this is the case, for example, of processing concerning personal data of workers where the infringement significantly affects those workers' dignity).[71]

131. The purpose of the processing relating to the infringements identified herein is communication between staff at MU as well as with students and other stakeholders. The purpose of the processing was determined by MU in order to facilitate this communication.

132. In relation to the **number of data subjects**, the EDPB Fining Guidelines state,

> The higher the number of data subjects involved, the more weight the supervisory authority may attribute to this factor. In many cases, it may also be considered that the infringement takes on 'systemic' connotations and can therefore affect, even at different times, additional data subjects who have not submitted complaints or reports to the supervisory authority. The supervisory authority may, depending on the circumstances of the case, consider the ratio between the number of data subjects affected and the total number of data subjects in that context (e.g. the number of citizens, customers or employees) in order to assess whether the infringement is of a systemic nature.[72]

133. The number of data subjects affected by the infringements identified herein is one employee whose email account was subject to unauthorised access and five additional

[70] Updated Breach Notification 12 Feb 2019.
[71] EDPB Fining Guidelines [53.b.iii].
[72] EDPB Fining Guidelines [53.b.iv].

email accounts linked to the academic and campus services business units were potentially accessed by an unauthorised third party. Six hundred and fifty three data subjects were identified as being potentially affected by the access to the compromised account.

134. The **level of damage** is considered by reference to any harm suffered by data subjects or the 'extent to which the conduct may affect individual rights and freedoms.' The EDPB Fining Guidelines note:

> The reference to the 'level' of damage suffered, therefore, is intended to draw the attention of the supervisory authorities to the damage suffered, or likely to have been suffered as a further, separate parameter with respect to the number of data subjects involved (for example, in cases where the number of individuals affected by the unlawful processing is high but the damage suffered by them is marginal). Following Recital 75 GDPR, the level of damage suffered refers to physical, material or non-material damage. The assessment of the damage, in any case, be limited [sic] to what is functionally necessary to achieve correct evaluation of the level of seriousness of the infringement as indicated in paragraph 60 below, without overlapping with the activities of judicial authorities as tasked with ascertaining the different forms of individual harm.[73]

135. In this case, the data breach resulted in a very significant financial loss to one employee whose email account was subject to unauthorised access. Six hundred and fifty three data subjects were identified as being potentially affected by the access to the compromised account. In assessing the level of damage suffered by the data subjects, the DPC has had regard to the loss of control suffered by them over their personal data. The personal data affected by the breaches was likely to have included data subject identity, PPSN, contact details, economic or financial data, and location data. The potential risks associated with unauthorised persons being able to access another user's email account include identity theft, loss of confidentiality, fraud and financial loss.[74]

The nature of the infringements

136. The EDPB Fining Guidelines state that the nature of the infringement is 'assessed by the concrete circumstances of the case.' In this assessment, the supervisory authority may:

[73] EDPB Fining Guidelines [53.b.v].
[74] See Recital 75 GDPR.

review the interest that the infringed provision seeks to protect and the place of this provision in the data protection framework. In addition, the supervisory authority may consider the degree to which the infringement prohibited the effective application of the provision and the fulfilment of the objective it sought to protect.[75]

137. The nature, gravity and duration of the infringements are all assessed by taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them.[76]

138. The nature of the first infringement concerns Articles 5(1)(f) and 32(1) GDPR and MU's failure to comply with its obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk in respect of its processing operations via its email systems. The objective of Articles 5(1)(f) and 32(1) GDPR is to protect the rights and freedoms of natural persons by ensuring that their personal data are processed in a manner that ensures appropriate security. A failure to implement an appropriate level of security increases the risk of personal data breaches. This, in turn, poses a threat to the rights and freedoms of natural persons because of the potential for damage to them where personal data breaches occur, leading to, inter alia, unavailability or destruction of essential personal data or unauthorised access, alteration or disclosure of that personal data. Therefore, compliance with Articles 5(1)(f) and 32(1) is central to the protection of the rights and freedoms of natural persons pursuant to the GDPR. Non-compliance with this obligation has serious consequences because of the potential damage to natural persons that can result from it.

139. The nature of the second infringement concerns Article 33(1) and MU's failure to notify the DPC of a personal data breach within the appropriate time after MU, as the controller, became aware or ought to have become aware of it. The infringement must be assessed in light of the fact that it is also capped at the lower threshold under Article 83(4). However, the nature of this infringement must also be assessed in light of the purpose of Article 33(1), which is to ensure prompt notification of data breaches to supervisory authorities. This enables a supervisory authority to assess the circumstances of the data breach, including the risks to natural persons. The supervisory authority can then decide whether the interests of those persons must be safeguarded to the extent possible, by mitigating the risks to them arising from a data

[75] EDPB Fining Guidelines, [53.a]
[76] Article 83(2)(a).

breach[77], for example by ordering a controller to communicate a personal data breach to affected data subjects under Article 34(4) or 58(2)(e) of the GDPR.

The gravity of the infringements

140. The gravity (as well as the nature and duration of the infringements) is assessed taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them.[78]

141. The gravity of the infringement of Articles 5(1)(f) and 32(1) GDPR is high in circumstances where the infringement resulted in the personal data breach. MU's lack of technical and organisational measures at the time of the breach contributed to the unauthorised access to personal and financial data of potentially 653 data subjects[79] as well as a significant financial loss to one individual. The DPC considers that the gravity of MU's failure to implement sufficient and appropriate technical and organisational measures to ensure the confidentiality of its processing systems to be high.

142. The gravity of the infringement of Article 33(1) GDPR is also high. The personal data breach concerned the personal data of a significant number of data subjects and the DPC has found that there was an infringement of the GDPR in MU's failure to notify the DPC of the personal data breach at the required time. The financial fraud, occurred in September 2018 and came to light in October 2018. MU reset the password of the victim of the fraud once the fraud incident was discovered.[80] MU was therefore at least on notice of a possible breach on 10 October 2018 and was certainly aware of it on 23 October 2018, when anomalies were uncovered in the email account of the employee [redacted] and her password was reset. The requirement to notify the DPC under Article 33 GDPR within 72 hours therefore began at the latest on 23 October 2018. However, MU deferred notifying the DPC of the breach until nearly 2 weeks after receipt of the BSI report, despite its ability under Article 33(4) GDPR to provide information subsequently where it is not possible to do so at the time of the initial notification. The personal data breach resulted in a risk to the rights and freedoms of data subjects, including, but not limited to, the risk of phishing attacks utilising the personal data compromised. In those circumstances, and in light of the importance of the notification process in protecting the rights and freedoms of data subjects, the gravity of finding of an infringement of Article 33(1) is high.

[77] Recital 85 GDPR.
[78] Article 83(2)(a).
[79] Response to Commencement Letter, 15 November 2019, page 5.
[80] BSI Email Fraud Investigation Report, page 3/4.

The duration of the infringement

143. In relation to the duration of an infringement, the EDPB Fining Guidelines state,

> a supervisory authority may generally attribute more weight to an infringement with longer duration. The longer the duration of the infringement, the more weight the supervisory authority may attribute to this factor.[81]

144. The A29WP Fining Guidelines note that duration may be illustrative of:

a) wilful conduct on the data controller's part, or

b) failure to take appropriate preventive measures, or

c) inability to put in place the required technical and organisational measures.[82]

145. The duration (as well as the nature and gravity of the infringements) is assessed taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them.[83]

146. In this case, the duration of MU's infringement of Articles 5(1)(f) and 32(1) GDPR regarding the processing commenced at the application of the GDPR on 25 May 2018. The obligation to implement and be able to demonstrate the appropriate organisational and technical measures applied from 25 May 2018. The infringement of Article 5(1)(f) and 32(1) found here was ongoing throughout the temporal scope in circumstances where MU failed to implement appropriate measures required by those provisions for the entirety of that time frame. Therefore, for the purposes of deciding whether to impose an administrative fine, and for calculating the appropriate amount if applicable, the DPC proceeds on the basis that the infringement of Articles 5(1)(f), 5(2) GDPR lasted from 25 May 2018 until 15 January 2020, when MFA was enforced on all MU email accounts.[84]

147. Regarding the duration of the infringement of Article 33(1), as outlined above, the DPC finds that there are no circumstances concerning this breach that justify a failure to notify the DPC within 72 hours of when MU became aware of it. While the discovery of the fraud and MU's actions in re-setting the password of the victim of the fraud on 10 October 2018 may only have given grounds for suspecting a possible data breach, the discovery of anomalies in the email account of the employee [redacted]

[81] EDPB Fining Guidelines [53.c].
[82] A29WP Fining Guidelines, p11.
[83] Article 83(2)(a).
[84] Response to Commencement Letter, 15 November 2019, page 6.

clearly indicated unauthorised access to the personal data in and accessible through that account.

148. The DPC therefore respectfully disagrees with the view expressed in the Final Report of the Inquiry that MU became aware of the breach when it was pointed out in the BSI report on 8 November 2018. MU's awareness of those 'issues' relating to that employee's account shows that a breach was, or should have been, apparent to MU on 23 October 2018. The infringement therefore began at the latest on 27 October 2018 (that is, 72 hours after midnight on 23 October) and ceased on 19 November 2018, when the DPC received MU's notification under Article 33 GDPR. Therefore, the duration of this infringement is at least 22 days in length. The DPC finds the duration of this infringement is at the moderate end of the scale of culpability in the circumstances.

Assessment of Article 83(2)(a)

149. Taking account of all of the factors assessed in this section, the DPC assesses the infringement of Articles 5(1)(f) and 32(1) GDPR to be serious and of a substantial duration. MU's processing of personal data via its email and IT systems resulted in unauthorised access or unauthorised disclosure of personal data to third parties and subsequent fraud. It also included loss of control over personal data, identity theft and financial loss as a result of unauthorised access. With regard to the infringement of Article 33(1), the personal data breach resulted in a risk to the rights and freedoms of natural persons, as evidenced by the financial fraud perpetrated and so should have been notified to the DPC within 72 hours of becoming aware of it. Such notifications are crucial for enabling supervisory authorities to assess the circumstances of the data breach, including the risks to data subjects, and decide whether action is required to mitigate those risks. Furthermore, the infringement was moderate in duration. Taking account of all of the factors assessed in this section, the DPC assesses the infringements to be of a serious nature.

ii) Article 83(2)(b) GDPR: the intentional or negligent character of the infringement;

150. The A29WP Fining Guidelines state,

> in general, intent includes both knowledge and willfulness in relation to the characteristics of an offence, whereas 'unintentional' means that there was no

intention to cause the infringement although the controller/processor breached the duty of care which is required in the law.[85]

151. The EDPB Fining Guidelines state:

> The intentional or negligent character of the infringement (Article 83(2)(b) GDPR) should be assessed taking into account the objective elements of conduct gathered from the facts of the case. The EDPB highlighted that it is generally admitted that intentional infringements, 'demonstrating contempt for the provisions of the law, are more severe than unintentional ones'.[86] In case of an intentional infringement, the supervisory authority is likely to attribute more weight to this factor. Depending on the circumstances of the case, the supervisory authority may also attach weight to the degree of negligence. At best, negligence could be regarded as neutral.

152. In this case, the DPC finds that the infringements indicate negligence on the part of MU. MU's infringement of Articles 5(1)(f) and 32(1) GDPR regarding the processing, concerns its failure to implement appropriate measures to protect the rights and freedoms of natural persons by ensuring that their personal data are processed in a manner that ensures appropriate security and to integrate the necessary safeguards into the processing. Hence, the characteristics of this infringement concerns that lack of appropriate technical and organisational measures for the duration of the infringement. In order to classify this infringement as intentional, the DPC must be satisfied that (i) MU wilfully omitted to implement appropriate technical and organisational measures and (ii) that it knew at the time that the measures that it implemented were not sufficient to meet the standards required by Articles 5(1)(f) and 32(1) GDPR.

153. While MU's attempts to implement appropriate measures were not sufficient for the purposes of Articles 5(1)(f) and 32(1) GDPR), the DPC does not consider that MU knew that the measures implemented were not sufficient at the time. However, in the circumstances, MU ought to have been aware that it was falling short of the duty owed under Article 5(1)(f) and 32(1). For example, MU ought to have been aware that its failure to implement MFA and its inadequate anti-spam configuration greatly and inappropriately increased the risk of a cyber or malware attack. Similarly, MU should have been aware that some essential security policies and procedures were inadequate or non-existent. The infringement was negligent to a medium degree because MU ought to have been aware that it was falling short of the duty owed under Articles

[85] A29WP Fining Guidelines, p11.
[86] Footnote from EDPB Fining Guidelines: *Guidelines WP 253,* p. 12.

5(1)(f) and 32(1) GDPR. The DPC finds that MU was also negligent to a medium degree in the extent of its infringement of Article 33(1) where it ought to have been aware of its obligation to inform the DPC within 72 hours of becoming aware of a data breach.

iii) Article 83(2)(c) GDPR: any action taken by the controller or processor to mitigate the damage suffered by data subjects;

154. According to the A29WP Fining Guidelines,

> This provision acts as an assessment of the degree of responsibility of the controller after the infringement has occurred. It may cover cases where the controller/processor has clearly not taken a reckless/ negligent approach but where they have done all they can to correct their actions when they became aware of the infringement.[87]

155. MU put in place various mitigation measures after it discovered the data breach. However, it is not always possible to correct a lack of control retrospectively, and these actions did not mitigate the risk to the confidentiality of the data belonging to the affected data subjects, nor did it mitigate the financial loss suffered as a result of the data breach.

156. MU made a number of substantial technical and organisational changes as a result of this data breach. This included hiring an independent security consultant, BSI, to carry out an investigation of the email fraud, accelerating its planned roll out of MFA for email accounts, reviewing and revising password policies, improved anti-spam ware, Security Awareness Training for staff, developing a documented cybersecurity incident response, having a 'Cybersecurity Incident Register' in place to track incidents and contacting potentially affected data subjects. Despite the delay in notifying the DPC of the breach, MU took steps to investigate the security incident prior to notifying the DPC. Having regard to these actions for the purpose of Article 83(2)(c) GDPR, the DPC takes the view that the actions provided limited mitigation of the damage to data subjects.

[87] A29WP Fining Guidelines, pp12-13.

iv) Article 83(2)(d) GDPR: the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

157. The key question in relation to this provision is whether MU 'did what it could be expected to do' given the nature, the purposes or the size of the processing, seen in light of the obligations imposed on them by the Regulation.[88]

158. In its submissions, MU outlined the measures that it had in place to prevent any potential breach of data protection. The DPC has had full regard to those measures in this Decision. This Decision assesses whether MU complied with its obligations under Articles 5(1)(f) and 32(1) GDPR by implementing appropriate technical and organisational measures to ensure appropriate security of the personal data processed in MU's email system. As stated above, the DPC finds that MU infringed those two provisions.

159. Regarding the infringement of Article 33(1), the DPC notes that MU had a DPO in place who notified the DPC of the personal data breach. MU's Personal Data Security Incident Management Procedure[89], created on 17 March 2018, states that 'all incidents in which personal data has been put at risk must be reported to the Data Protection Commissioners Officer "without undue delay" and where feasible within 72 hours of becoming aware of the breach.' MU is obliged to ensure that it has appropriate measures in place to meet its obligations under Article 33(1).

160. Against this backdrop, the DPC considers that MU holds a high degree of responsibility for this infringement and that the absence of sufficiently robust technical and organisational measures must be deterred. It is clear that MU did not do 'what it could be expected to do' in the circumstances assessed in this Decision.

161. However, in circumstances where this factor forms the basis for the finding of the infringement of Article 32 GDPR against MU, this factor cannot be considered aggravating in respect of the infringements. Therefore, the DPC considers that this factor is neither aggravating nor mitigating in the circumstances.

[88] EDPB Fining Guidelines, [77].
[89] Personal Data Security Incident Management Procedure.

v) Article 83(2)(e) GDPR: any relevant previous infringements by the controller or processor;

162. In line with the EDPB Fining Guidelines, prior infringements are those already established before the decision (in the sense of Article 60 GDPR) is issued.[90]

163. According to the A29WP Fining Guidelines, '[t]his criterion is meant to assess the track record of the entity committing the infringement.'[91]

164. In this case, MU has not been found to have committed any relevant previous infringements of the GDPR by the DPC or another supervisory authority.

vi) Article 83(2)(f) GDPR: the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

165. The extent to which MU has cooperated with the inquiry is relevant to consider under this heading.[92] MU submitted breach notification forms in respect of the personal data breaches to the DPC and gave updates regarding MU's progress in remediating the breaches. The DPC acknowledges MU's cooperation with the DPC during the course of the Inquiry. However, the DPC notes that MU was, in any event, under a duty, in light of Article 31 GDPR, to cooperate on request with the supervisory authority in the performance of its tasks.

166. The DPC notes that MU has made a number of substantial technical and organisational improvements to security as a result of this data breach and to mitigating its possible adverse effects. MU's submissions during the Inquiry detailed the measures that MU has implemented, and is in the course of implementing, to provide an appropriate level of security in respect of its email service. This has separately been taken into account as a mitigating factor under Article 83(2)(c) above.

vii) Article 83(2)(g) GDPR: the categories of personal data affected by the infringement;

167. By way of example of the categories that may be relevant to consider here, the A29WP Fining Guidelines suggest considering whether the infringements concern Article 9 or 10 data, whether the data are directly or indirectly identifiable, whether the data are

[90] EDPB Fining Guidelines, [82].
[91] A20WP Fining Guidelines, p14.
[92] A29WP Fining Guidelines, p14.

encrypted or whether the processing involves data whose dissemination would cause immediate damage or distress to the individual.[93]

168. Six hundred and fifty three data subjects were identified as being potentially affected[94] and the personal data affected by the breaches was likely to have included data subject identity, PPSN, contact details, economic or financial data, and location data. These personal data, by their nature, carry a risk with regard to the fundamental rights and freedoms of data subjects, in particular in relation to financial fraud and/or identity theft.

viii) Article 83(2)(h) GDPR: the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

169. According to the A29WP Fining Guidelines, this section can be used to consider whether the DPC became aware of the infringement 'as a result of investigation, complaints, articles in the press, anonymous tips or notification by the data controller.'[95]

170. The A29WP Fining Guidelines also note that,

> The controller has an obligation according to the Regulation to notify the supervisory authority about personal data breaches. Where the controller merely fulfils this obligation, compliance with the obligation cannot be interpreted as an attenuating/ mitigating factor. Similarly, a data controller/processor who acted carelessly without notifying, or at least not notifying all of the details of the infringement due to a failure to adequately assess the extent of the infringement may also be considered by the supervisory authority to merit a more serious penalty i.e. it is unlikely to be classified as a minor infringement.[96]

171. In this case, the DPC received notification of a personal data breach from MU on 19 November 2018. This was found to be an undue delay and in breach of Article 33(1) GDPR.

---

[93] A29WP Fining Guidelines, p14.
[94] Response to Commencement Letter, 15 November 2019, page 5.
[95] A29WP Fining Guidelines, p15.
[96] A29WP Fining Guidelines, p15.

ix) Article 83(2)(i) GDPR: where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

172. The A29WP Fining Guidelines state

> As opposed to the criteria in (e), this assessment criteria only seeks to remind supervisory authorities to refer to measures that they themselves have previously issued to the same controller or processors 'with regard to the same subject matter'.[97]

173. Corrective powers have not previously been ordered against MU with regard to the subject-matter of this Decision.

x) Article 83(2)(j) GDPR: adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42

174. Such considerations do not arise in this case.

xi) Article 83(2)(k) GDPR: any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

175. The DPC is of the view that there are no other aggravating or mitigating factors in respect of the infringements of Articles 5(1)(f), 32(1) or 33(1) GDPR.

xii) Decisions on whether to impose administrative fines

176. The decision to impose an administrative fine 'needs to be taken on a case-by-case basis, in light of the circumstances of each individual case.'[98]

177. Taking into account the assessment of the criteria at (a) to (k) above, the DPC has decided to impose an administrative fine. The infringements were considered above to be of a high seriousness by reference to their nature, gravity and duration in line with Article 83(2)(a). This is an aggravating factor, which indicates that a fine should be imposed. Under Articles 83(2)(b) and (g), the DPC found that MU was negligent to a medium degree with respect to the infringements and that the infringements affected personal data that, by their nature, carry a risk with regard to the fundamental rights

[97] A29WP Fining Guidelines, p15.
[98] EDPB, Binding Decision 1/2023.

and freedoms of data subjects, in particular in relation to financial fraud and/or identity theft. These are aggravating factors indicating that a fine should be imposed. The DPC considers that the measures adopted by MU under Article 83(2)(c) to mitigate the damage to data subjects are mitigating to a low degree, and this factor does not negate the need for administrative fines in this Inquiry. The DPC considers that the factors assessed in relation to Articles 83(2)(e), (f), (h), (i), (j) and (k) are neither mitigating nor aggravating.

178. In order to ensure compliance with the GDPR, it is necessary to dissuade non-compliance. Depending on the circumstances of each individual case, dissuading non-compliance can entail dissuading the entity concerned with the corrective measures, or dissuading other entities carrying out similar processing operations, or both. Where a serious infringement of the GDPR occurs, a reprimand may not be sufficient to deter future non-compliance. In this regard, by imposing financial penalties, administrative fines are effective in dissuading non-compliance. This is recognised by the requirement in Article 83(1) GDPR for a fine, when imposed, to be effective, proportionate and dissuasive. Recital 148 GDPR acknowledges that, depending on the circumstances of each individual case, administrative fines may be appropriate in addition to, or instead of, reprimands and other corrective powers:

> In order to strengthen the enforcement of the rules of this Regulation, penalties, including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine.

179. While the reprimand will assist in dissuading MU and other entities from similar future non-compliance, in light of the seriousness of the infringement, the DPC does not consider that the reprimand alone is proportionate or effective to achieve this end. The DPC finds that administrative fines are necessary in respect of each of the infringements to deter other future serious non-compliance on the part of MU and other controllers or processors carrying out similar processing operations. The reasons for this finding include:

    a. Each infringement is serious in nature and gravity as set out pursuant to Article 83(2)(a) GDPR. Infringements that are of a serious nature and gravity must be strongly dissuaded both in respect of the individual controller and in respect of other entities carrying out similar processing.

    b. Regarding the infringements of Articles 5(1)(f), 32(1) and 33(1) GDPR, the DPC considers that MU's non-compliance with its obligations under these Articles

must be strongly dissuaded. Such dissuasive effect is crucial for protecting the rights and freedoms of those data subjects by implementing appropriate measures.

Therefore, the DPC considers that an administrative fine is appropriate and necessary in order to dissuade non-compliance.

180. Having regard to the nature, gravity and duration of the infringements, the DPC also considers that administrative fines are proportionate for ensuring compliance. MU's infringements of Articles 5(1)(f) and 32(1) GDPR were a primary cause of the data breach. In light of this damage, the DPC considers that administrative fines are proportionate in response to MU's infringement of Articles 5(1)(f), 32(1) and 33(1) GDPR with a view to ensuring future compliance. The DPC considers that administrative fines do not exceed what is necessary to enforce compliance in respect of the infringements identified in this Decision.

181. The DPC considers that the negligent character of MU's infringements of Articles 5(1)(f), 32(1) and 33(1) GDPR carries weight when considering whether to impose administrative fines, and if so, the amount of those fines. This negligence suggests that administrative fines are necessary to ensure that MU directs sufficient attention to its obligations under Articles 5(1)(f) and 32(1) GDPR in the future.

182. The DPC considers that administrative fines would help to ensure that MU and other similar controllers take the necessary action to ensure the utmost care is taken to avoid infringements of the GDPR in respect of users' data.

183. The DPC has had regard to the lack of previous relevant infringements by MU, which is a slightly mitigating factor. The DPC has also had regard to the actions and attendant costs taken on by MU as a result of the breach, as raised in MU's submission on the Draft Decision, including reimbursing the misdirected funds, commissioning the BSI report, adopting additional IT security measures and recruiting additional personnel. However, these are costs arising from MU's infringements, while imposing administrative fines is a dissuasive measure. In light of the negligent character of the infringements and of MU's failure to comply with its obligations with regard to data protection, the DPC considers that dissuasive administrative fines are necessary in the circumstances to ensure future compliance.

b) Decision on the amount of the administrative fine

184. Above, it was determined that it was necessary to impose an administrative fine. This section calculates the amount of that fine, taking into account the methodology required to be applied by the EDPB Fining Guidelines, based on the assessments of the individual Article 83(2) GDPR criteria that are recorded above.

i) Article 83(3) GDPR

185. In accordance with Article 83(3) GDPR:

> If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

186. As outlined previously, the infringements identified herein all relate to the processing concerned, i.e. via MU's email and IT systems.

187. In respect of the interpretation of Article 83(3) GDPR, the DPC is mindful of its obligations of cooperation and consistency in, *inter alia*, Articles 60(1) and 63 GDPR. Accordingly, it is necessary to follow the EDPB's interpretation of Article 83(3) GDPR which was set out in the EDPB's binding decision 1/2021, which was made in relation to an inquiry conducted by the DPC.[99]

188. The relevant passages of the EDPB decision are as follows:

> 315. All CSAs argued in their respective objections that not taking into account infringements other than the 'gravest infringement' is not in line with their interpretation of Article 83(3) GDPR, as this would result in a situation where WhatsApp IE is fined in the same way for one infringement as it would be for several infringements. On the other hand, as explained above, the IE SA argued that the assessment of whether to impose a fine, and of the amount thereof, must be carried out in respect of each individual infringement found and the assessment of the gravity of the infringement should be done by taking into account the individual circumstances of the case. The IE SA decided to impose only a fine for the infringement of Article 14 GDPR, considering it to be the gravest of the three infringements.
>
> 316. The EDPB notes that the IE SA identified several infringements in the Decision for which it specified fines, namely infringements of Article 12, 13 and 14 GDPR, and then applied Article 83(3) GDPR.
>
> 317. Furthermore, the EDPB notes that WhatsApp IE agreed with the approach of the IE SA concerning the interpretation of Article 83(3) GDPR. In

[99] Inquiry IN-18-12-2.

its submissions on the objections, WhatsApp IE also raised that the approach of the IE SA did not lead to a restriction of the IE SA's ability to find other infringements of other provisions of the GDPR or of its ability to impose a very significant fine. WhatsApp IE argued that the alternative interpretation of Article 83(3) GDPR suggested by the CSAs is not consistent with the text and structure of Article 83 GDPR and expressed support for the IE SA's literal and purposive interpretation of the provision.

318. In this case, the issue that the EDPB is called upon to decide is how the calculation of the fine is influenced by the finding of several infringements under Article 83(3) GDPR.

319. Article 83(3) GDPR reads that if 'a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.'

320. First of all, it has to be noted that Article 83(3) GDPR is limited in its application and will not apply to every single case in which multiple infringements are found to have occurred, but only to those cases where multiple infringements have arisen from 'the same or linked processing operations'.

321. The EDPB highlights that the overarching purpose of Article 83 GDPR is to ensure that for each individual case, the imposition of an administrative fine in respect of an infringement of the GDPR is to be effective, proportionate and dissuasive. In the view of the EDPB, the ability of SAs to impose such deterrent fines highly contributes to enforcement and therefore to compliance with the GDPR.

322. As regards the interpretation of Article 83(3) GDPR, the EDPB points out that the *effet utile* principle requires all institutions to give full force and effect to EU law. The EDPB considers that the approach pursued by the IE SA would not give full force and effect to the enforcement and therefore to compliance with the GDPR, and would not be in line with the aforementioned purpose of Article 83 GDPR.

323. Indeed, the approach pursued by the IE SA would lead to a situation where, in cases of several infringements of the GDPR concerning the same or linked processing operations, the fine would always correspond to the same amount that would be identified, had the controller or processor only

committed one – the gravest – infringement. The other infringements would be discarded with regard to calculating the fine. In other words, it would not matter if a controller committed one or numerous infringements of the GDPR, as only one single infringement, the gravest infringement, would be taken into account when assessing the fine.

324. With regard to the meaning of Article 83(3) GDPR the EDPB, bearing in mind the views expressed by the CSAs, notes that in the event of several infringements, several amounts can be determined. However, the total amount cannot exceed a maximum limit prescribed, in the abstract, by the GDPR. More specifically, the wording 'amount specified for the gravest infringement' refers to the legal maximums of fines under Articles 83(4), (5) and (6) GDPR. The EDPB notes that the Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 state that the 'occurrence of several different infringements committed together in any particular single case means that the supervisory authority is able to apply the administrative fines at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement'. The guidelines include an example of an infringement of Article 8 and Article 12 GDPR and refer to the possibility for the SA to apply the corrective measure within the limit set out for the gravest infringement, i.e. in the example the limits of Article 83(5) GDPR.

325. The wording 'total amount' also alludes to the interpretation described above. The EDPB notes that the legislator did not include in Article 83(3) GDPR that the amount of the fine for several linked infringements should be (exactly) the fine specified for the gravest infringement. The wording 'total amount' in this regard already implies that other infringements have to be taken into account when assessing the amount of the fine. This is notwithstanding the duty on the SA imposing the fine to take into account the proportionality of the fine.

326. Although the fine itself may not exceed the legal maximum of the highest fining tier, the offender shall still be explicitly found guilty of having infringed several provisions and these infringements have to be taken into account when assessing the amount of the final fine that is to be imposed. Therefore, while the legal maximum of the fine is set by the gravest infringement with regard to Articles 83(4) and (5) GDPR, other infringements cannot be discarded but have to be taken into account when calculating the fine.

> 327. In light of the above, the EDPB instructs the IE SA to amend its Draft Decision on the basis of the objections raised by the DE SA, FR SA and PT SA with respect to Article 83(3) GDPR and to also take into account the other infringements – in addition to the gravest infringement – when calculating the fine, subject to the criteria of Article 83(1) GDPR of effectiveness, proportionality and dissuasiveness.

189. The impact of this interpretation is that administrative fines are imposed cumulatively, as opposed to imposing only the proposed fine for the gravest infringement. Under this interpretation, the only applicable limit for the total fine imposed is the overall 'cap'. By way of example, in a case of multiple infringements, if the gravest infringement was one that carried a maximum administrative fine of 2% of the turnover of the undertaking, the cumulative fine imposed could also not exceed 2% of the turnover of the undertaking.

In this case, infringements of Articles 5(1)(f), 32(1) and 33(1) GDPR were identified. The gravest infringement is that of Article 5(1)(f), as it is an infringement of a core principle of the GDPR.

ii) Categorisation of the infringements

190. As noted in the EDPB Fining Guidelines, Articles 83(4)-(6) GDPR indicate the degrees of seriousness accorded to different categories of infringement. Those Guidelines note that

> With this distinction, the legislator provided a first indication of the seriousness of the infringement in an abstract sense. The more serious the infringement, the higher the fine is likely to be.[100]

191. The categorisation of infringements under Articles 83(4) or (5) is a relevant consideration in assessing the seriousness of the infringements in this case. The infringement of Article 5(1)(f) found in this case relates to the basic principles of processing and is ascribed considerably greater significance, with the legislator providing for, in general, maximum administrative fines double those applicable to the infringements of Articles 32(1) and 33(1).

[100] EDPB Fining Guidelines [50].

iii) Seriousness of the infringement pursuant to Articles 83(2)(a), (b) and (g) GDPR

192. The EDPB Guidelines state that the factors assessed in relation to Articles 83(2)(a), (b) and (g) GDPR indicate the seriousness of the infringement.[101] These factors were assessed in paragraphs 136 to 152 and 167 to 168 above. The guidelines also state that

> This assessment is no mathematical calculation in which the abovementioned factors are considered individually, but rather a thorough evaluation of the concrete circumstances of the case, in which all of the abovementioned factors are interlinked. Therefore, in reviewing the seriousness of the infringement, regard should be given to the infringement as a whole.[102]

193. Having regard to these factors as a whole, the infringements are of a medium level of seriousness. Under Article 83(2)(a) the infringements were found to be of a serious nature and have a high degree of gravity. The infringements were also found to have been of moderate duration. The infringements affected personal data which, by their nature, carry a risk with regard to the fundamental rights and freedoms of data subjects, as assessed under Article 83(2)(g). MU were also negligent to a medium degree with respect to the infringements, as assessed under Article 83(2)(b). Therefore, balancing these factors, the DPC considers that the infringements were of medium seriousness.

iv) Imposing an effective, dissuasive and proportionate fine

194. Article 83(1) GDPR requires a fine to be effective, proportionate and dissuasive in each individual case. As the guidelines also say that this doesn't 'dismiss a supervisory authority from the responsibility to carry out a review of the effectiveness, dissuasiveness and proportionality at the end of the calculation.'[103] Article 83(1) will be considered again at the end of this calculation.

v) Aggravating and mitigating circumstances

195. Articles 83(2)(a), (b) and (g) GDPR were considered above. This section considers the aggravating or mitigating impact of the remaining criteria in Article 83(2) GDPR. In relation to Article 83(2)(c), it was noted that MU had not adopted measures to mitigate the damage to data subjects. However, MU made a number of substantial technical and organisational changes as a result of this data breach and also took steps to investigate

[101] EDPB Fining Guidelines, [51].
[102] EDPB Fining Guidelines, [59].
[103] EDPB Fining Guidelines, [64].

the security incident prior to notifying the DPC. The DPC considers this a mitigating factor of low weight.

196. In relation to Article 83(2)(d), it was noted that MU had a high degree of responsibility for the infringements. MU did not do 'what it could be expected to do' in the circumstances assessed in this Decision. However, in circumstances where this factor forms the basis for the finding of the infringement of Article 32 GDPR against MU, this factor cannot be considered aggravating in respect of the infringements. Therefore, the DPC considers this neither aggravating nor mitigating in the circumstances.

197. In relation to Article 83(2)(e), it was noted that MU did not have any previous relevant infringements. The DPC considers this factor neither mitigating nor aggravating.

198. In relation to Article 83(2)(f), it was noted that MU had cooperated with the DPC. As MU has a general obligation to cooperate under Article 31 GDPR, the DPC considers this factor neither mitigating nor aggravating.

199. In relation to Article 83(2)(h), it was noted that the manner in which the infringement became known to the DPC was via notification of a personal data breach from MU. The DPC considers this factor neither aggravating nor mitigating in the circumstances.

200. In relation to Article 83(2)(i), it was noted that orders had not been previously ordered by the DPC[104] with regard to the same subject matter. The DPC considers this factor neither mitigating nor aggravating.

201. In relation to Article 83(2)(j), it was found that there were no relevant approved codes of conduct or approved certification mechanisms for consideration. The DPC considers this factor neither mitigating nor aggravating.

202. In relation to Article 83(2)(k), it was noted that there were no additional aggravating or mitigating factors for consideration.

203. Taking into account all of the matters arising for consideration as part of the individual assessments required to be carried out pursuant to Article 83(2), together with the requirements of the Fining Guidelines as detailed above, the DPC has decided to impose an administrative fine of €25,000 in respect of MU's infringement of Article 5(1)f and 32(1) GDPR. In respect of MU's infringement of Article 33(1) GDPR, the DPC has decided to impose an administrative fine of €15,000.

[104] Paragraph 101 of the EDPB Fining Guidelines says 'as opposed to Article 83(2)(e) GDPR, this assessment only refers to measures that supervisory authorities themselves have previously issued to the same controller or processor with regard to the same subject matter.'

vi) The relevant legal maximum for administrative fines

204. The DPC notes that MU is a public authority (as defined in section 2(1) of the 2018 Act), having been established under section 43 of the Universities Act 1997. Section 141(4) of the 2018 Act provides that any administrative fine that the DPC decides to impose on a public authority or public body shall not exceed €1,000,000 unless that authority or body acts as an undertaking within the meaning of the Competition Act 2002. As the administrative fines imposed in this Decision do not exceed that amount, it is not necessary for the DPC to determine whether MU acts as an undertaking for the purpose of the processing concerned

vii) Article 83(1) GDPR: Effectiveness, proportionality and dissuasiveness

Effectiveness

205. It is the DPC's view that for a fine to be effective, it must be large enough to have a significant effect on the controller or processor such that GDPR compliance, motivated by avoiding such fines in the future, becomes a factor in the entity's governance and management decision-making at the highest level. Furthermore, a sufficiently large fine is necessary to ensure that the fine is not a mere insignificant expense for the controller or processor concerned, and to ensure that the entity does not enjoy an unfair advantage by its ability to absorb even large fines for its infringements of the GDPR. The infringements concern personal data including data subject identity, PPSN, contact details, economic or financial data, and location data. These personal data, by their nature, carry a risk with regard to the fundamental rights and freedoms of data subjects, in particular in relation to financial fraud and/or identity theft. In that context, the DPC considers that the level of the fines ensure sufficiently effective fines, and no further adjustment is required.

Dissuasiveness

206. In order for a fine to be 'dissuasive', it must dissuade both the controller or processor concerned as well as other controllers or processors carrying out similar processing operations from repeating the conduct concerned. The DPC considers that the fines are dissuasive for both. The DPC considers the monetary value of the fines to be sufficient to have such a deterrent effect.

207. Each infringement is serious in nature and gravity as set out pursuant to Article 83(2)(a) GDPR. Infringements that are of a serious nature and gravity must be strongly dissuaded both in respect of the individual controller and in respect of other entities carrying out similar processing. Regarding the infringements of Articles 5(1)(f), 32(1) and 33(1) GDPR, the DPC considers that MU's non-compliance with its obligations

under these Articles must be strongly dissuaded. Such dissuasive effect is crucial for protecting the rights and freedoms of those data subjects by implementing appropriate measures. Therefore, the DPC considers that the administrative fines are appropriate and necessary in order to dissuade non-compliance.

208. The DPC considers that the negligent character of MU's infringements of Articles 5(1)(f), 32(1) and 33(1) GDPR carries weight when considering the amount of those fines. This negligence suggests that the administrative fines are necessary to ensure that MU directs sufficient attention to its obligations under Articles 5(1)(f) and 32(1) GDPR in the future.

209. The DPC considers that the amounts of the administrative fines would help to ensure that MU and other similar controllers take the necessary action to ensure the utmost care is taken to avoid infringements of the GDPR in respect of users' data.

210. The DPC has had regard to the lack of previous relevant infringements by MU, which is a slightly mitigating factor. It has also had regard to the actions taken by MU as a result of the breach. In light of the negligent character of the infringements, and MU's failure to comply with its obligations with regard to data protection, the DPC considers that dissuasive administrative fines to the extent imposed are necessary in the circumstances to ensure future compliance.

Proportionality

211. Proportionality is a principle of EU law that requires a measure to pursue a legitimate objective, be appropriate to attain that objective, and not go beyond what is necessary to achieve the objective. The objectives of the administrative fines in this case are to both re-establish compliance with the rules, and to sanction MU's infringements. As regards the requirement for any fine to be necessary to these objectives, this requires the DPC to adjust the quantum of any fines to the minimum amount necessary to achieve the objectives pursued by the GDPR.

212. Having regard to the nature, gravity and duration of the infringements, the DPC considers that the administrative fines are proportionate in the circumstances in view of ensuring compliance. MU's infringements of Articles 5(1)(f) and 32(1) GDPR were a primary cause of the data breach. In light of this damage, the DPC considers that the administrative fines are proportionate to responding to MU's infringement of Articles 5(1)(f), 32(1) and 33(1) GDPR with a view to ensuring future compliance. The DPC considers that administrative fines do not exceed what is necessary to enforce compliance in respect of the infringements identified in this Decision.

L. Summary of Envisaged Action

213. In summary, the corrective powers that the DPC intends to exercise are:

- a Reprimand to MU pursuant to Article 58(2)(b) GDPR regarding the infringements identified in this Decision; and
- an Order to bring processing into compliance in respect of MU's infringement of Article 32(1) GDPR; and,
- two administrative fines, as follows:
    1. a fine of €25,000 in respect of MU's infringement of Article 5(1)f and 32(1) GDPR.
    2. a fine of €15,000 in respect of MU's infringement of Article 33(1) GDPR.

M. Right of Appeal

214. This Decision is issued in accordance with section 111 of the 2018 Act. Pursuant to section 150(5) of the 2018 Act, MU has the right to appeal against this Decision within 28 days from the date on which notice of the Decision is served on it. Pursuant to section 142 of the 2018 Act, as this Decision imposes an administrative fine, MU also has the right to appeal under that section within 28 days from the date on which notice of this Decision was provided to it.

Dr. Des Hogan
Commissioner for Data Protection
Chairperson

Dale Sunderland
Commissioner for Data Protection