In the matter of the General Data Protection Regulation

DPC Case Reference: IN-19-7-4

In the matter of University College Dublin

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-Maker for the Commission:

Helen Dixon
Commissioner for Data Protection

17 December 2020

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Protection Commission
2 Fitzwilliam Square South
Dublin 2, Ireland

Contents

1. Introduction 3
2. Legal Framework for the Inquiry and the Decision 3
   i. Legal Basis for the Inquiry 3
   ii. Legal Basis for the Decision 4
3. Factual Background 4
4. Scope of the Inquiry 7
5. Issues for Determination 8
6. Issue 1: Articles 5(1)(f) and 32(1) of the GDPR 8
   i. Assessing Risk 9
   ii. Security Measures Implemented by UCD 11
   iii. The Appropriate Level of Security 13
   iv. Finding 15
7. Issue 2: Articles 5(1)(e) of the GDPR 15
   i. The Principle of Storage Limitation 15
   ii. Finding 16
8. Issue 3: Article 33(1) of the GDPR 17
   i. The Obligation to Notify Without Undue Delay 17
   ii. The Breach Notifications 18
   iii. Findings 19
9. Decision on Corrective Powers 19
   A. Order to Bring Processing into Compliance 20
   B. Reprimand 21
   C. Administrative Fine 22
      i. Whether Each Infringement Warrants an Administrative Fine 22
      ii. The Permitted Range 31
      iii. Calculating Administrative Fines 33
      iv. The Same or Linked Processing Operations 35
      v. The Amount of the Administrative Fine 36
   D. Summary of Corrective Powers 37
10. Right of Appeal 37

Appendix: Schedule of Materials Considered for the Purposes of this Decision 38

1. Introduction

1.1 This document (**"the Decision"**) is the decision made by the Data Protection Commission (**"the DPC"**) in accordance with Section 111 of the Data Protection Act 2018 (**"the 2018 Act"**). I make this Decision having considered the information obtained in the separate own volition inquiry (**"the Inquiry"**) conducted by Authorised Officers of the DPC (**"the Inquiry Team"**) pursuant to Section 110 of the 2018 Act. The Inquiry Team provided University College Dublin (**"UCD")** with the Draft Inquiry Report and the Final Inquiry Report.

1.2 UCD was provided with the Draft Decision on this Inquiry on 10 November 2020 to provide it with a final opportunity to make submissions. This Decision is being provided to UCD pursuant to Section 116(1)(a) of the 2018 Act in order to give UCD notice of the Decision and the reasons for it, and the corrective powers that I have decided to exercise.

1.3 This Decision contains corrective powers under Section 115 of the 2018 Act and Article 58(2) of the General Data Protection Regulation (**"the GDPR")** arising from the infringements that have been identified herein. It should be noted, in this regard, that UCD is required to comply with these corrective powers and it is open to this office to serve an enforcement notice on UCD in accordance with Section 133 of the 2018 Act.

2. Legal Framework for the Inquiry and the Decision

i. Legal Basis for the Inquiry

2.1 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 Commission has the power to commence an inquiry on several bases, including on foot of a complaint, or of its own volition.

2.2 Section 110(1) of the 2018 Act provides that the Commission 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 regulation under the Act, that gives further effect to the GDPR. Section 110(2) of the 2018 Act provides that the Commission 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.

ii. Legal Basis for the Decision

2.3 The decision-making process for this Inquiry is provided for under Section 111 of the 2018 Act, and requires that the Commission must 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. As the sole member of the Commission, I perform this function in my role as the decision-maker in the Commission. In so doing, I am required to carry out an independent assessment of all of the materials provided to me by the Inquiry Team as well as any other materials which have been furnished to me by UCD, and any other materials which I consider to be relevant, in the course of the decision-making process.

2.4 The Final Inquiry Report was transmitted to me on 8 July 2020, together with the Inquiry Team's file, containing copies of all correspondence exchanged between the Inquiry Team and UCD; and copies of all submissions made by UCD, including the submissions made by the UCD in respect of the Draft Inquiry Report. UCD made submissions on the Draft Decision on 1 December 2020. A full schedule of all documentation considered by me for the purpose of my preparation of this Decision is appended hereto. I issued a letter to UCD on 8 September 2020 to notify it of the commencement of the decision-making process.

2.5 Having reviewed the Final Inquiry Report, and the other materials provided to me by the Inquiry Team, including the submissions made by UCD, I was satisfied that the Inquiry was correctly conducted and that fair procedures were followed throughout. This includes, but is not limited to, notifications to the controller, opportunities for the controller to comment on the Draft Inquiry Report before it was submitted to me as decision-maker, and that the powers exercised by the Inquiry Team were lawfully invoked.

3. Factual Background

3.1 During the period of 8 August 2018 to 21 January 2019, UCD made 7 personal data breach notifications[1] to the DPC. The breaches all concern instances where unauthorised third parties accessed UCD email accounts, or where the login credentials for UCD email accounts were posted online, or both. UCD was able to confirm that unauthorised access had occurred in relation to 6 of the personal data breach notifications. No unauthorised access was detected in relation to breach Notification BN-18-10-38, however this concerned an instance where Google notified UCD that the login credentials of 2 UCD staff accounts were discovered on a publicly posted list of compromised accounts. In the remainder of the personal data breaches, the unauthorised access was detected using Google's intrusion detection service, by reviewing suspicious logins, and by detecting the spam emails. UCD identified the various causes of how the unauthorised third parties were able to gain access to the email accounts, including: [redacted] The unauthorised

[1] The reference numbers for those breach notifications are: BN-18-9-175, BN-18-9-306, BN-18-9-407, BN-18-10-38, BN-18-10-88, BN-18-10-423, and BN-18-01-213.

access to the email accounts resulted in access to personal data stored in emails within those accounts, including the inboxes and sent items. Therefore, the personal data at issue relates not only to the email account holders, but also a much greater number of third parties. This includes other staff members and students at UCD.

3.2 [redacted]. UCD was unable to offer any reason for the retention of the [redacted] in relation to this personal data breach. UCD notified the DPC of all of the relevant personal data breaches. However, breach notifications BN-18-10-423 and BN-19-01-213 occurred over 72 hours after UCD became aware of potential security compromises and, thus, fall to be considered in this Decision in the context of UCD's obligation to notify the DPC without undue delay under Article 33(1) of the GDPR.

3.3 The Inquiry Team informed UCD of the commencement of the Inquiry by way of a Notice of Commencement of Inquiry (**"the Notice"**) on 19 July 2019. The Notice set out the scope and legal basis of the Inquiry. The decision to commence the Inquiry was taken having regard to the circumstances of the breaches. The Notice informed UCD that the Inquiry would examine whether or not it had discharged its obligations in connection with the subject matter of the breaches and determine whether or not any provision(s) of the 2018 Act and/or the GDPR had been contravened by UCD in that context. In this regard, the scope of the Inquiry was to focus on the areas of Data Protection Governance, Training and Awareness, Records Management, Security of Personal Data, Data Sharing, Privacy Impact Assessments, and Records of Processing Activities. The Notice set out that the Inquiry would identify the facts and the data protection issues as they relate to the subject of the Inquiry. The Notice also sought certain documentation and posed a number of queries to UCD to enable the Inquiry Team to establish the relevant facts.

3.4 UCD responded to the Notice on 1 August 2019. UCD's response provided an overview of data protection compliance in the University. It also replied to the queries set out by the DPC. The response outlined how the email service in UCD is part of the *"G-Suite for Education"* provided under the terms of an agreement with Google. The service is divided into separate domains for staff (@ucd.ie), students (@ucdconnect.ie), and the foundation office (@ucdfoundation.ie). UCD also made submissions on its IT infrastructure generally, security awareness training, and other submissions, all of which were considered for the purposes of this Decision.

3.5 On 1 November 2019, the Inquiry Team wrote to UCD to notify it of its intention to carry out an on-site inspection. The decision to carry out an inspection was made after the Inquiry Team examined the documentation provided by UCD. In this regard, UCD was notified that the purpose of the inspection was to examine the cause of the breaches and any remedial action taken by UCD subsequent to the reporting of the breaches. The letter detailed that the inspection would be carried out by Authorised Officers of the DPC in exercise its powers under Section 130 of the 2018 Act. Notice was given to UCD that the inspection would occur on 21 November 2019 at 10:30am.

3.6 The inspection was conducted by a team of 3 authorised officers of the DPC. The authorised officers met with UCD's interim data protection officer and other members of management and staff. The authorised officers requested a number of documents from UCD during the inspection, which UCD provided by email on 27 November 2019. The authorised officers analysed the breaches during the course of the on-site inspection. In addition to the documents requested, the authorised officers gathered other relevant information during the inspection. The authorised officers viewed lists provided by Google's Intrusion Detection Service, [redacted]. During the inspection, UCD detailed how Google had notified UCD that the credentials in BN-18-10-38 had been made available online. UCD also detailed how the unauthorised access to the email account in BN-18-10-88 was identified by Google's Intrusion Detection Service[3]. [redacted]

3.7 On 10 March 2020, the Inquiry Team wrote to UCD seeking specific information on the measures that were in place at the time of the breaches to comply with Articles 5(1)(f) and 32(1) of the GDPR. UCD responded on 19 March 2020 and made further submissions on the measures that were implemented at the time of the breaches. These measures are considered in full below.

3.8 On 20 May 2020, the Inquiry Team issued UCD with the Draft Inquiry Report and invited submissions. On 18 June 2020, UCD made submissions on the Draft Inquiry Report. The submissions made a number of clarifications, made submissions on confidentiality and commercial sensitivity, provided information on measures implemented since the personal data breaches occurred, and made submissions on the University's structure with regard to data protection. The submissions also appended UCD's timelines and key costings and planning for its Cyber Security Programme Plan. The Inquiry Team had regard to these submissions in completing the Final Inquiry Report.

[2] See paragraph 57 of the Final Inquiry Report.
[3] See paragraph 86 of the Final Inquiry Report.
[4] See paragraph 96 of the Final Inquiry Report.
[5] See paragraph 108 of the Final Inquiry Report.
[6] See paragraph 122 of the Final Inquiry Report.
[7] See paragraph 58 of the Final Inquiry Report.

3.9 On 8 July 2020, the Inquiry Team completed the Final Inquiry Report and submitted it to me as decision-maker. I have considered the Inquiry Report and all relevant correspondence and submissions. UCD was provided with my Draft Decision on 10 November 2020 and was afforded the opportunity to make submissions on the proposed infringements that were provisionally identified therein and the corrective powers that I proposed to exercise. On 1 December 2020, UCD made submissions on the Draft Decision. I have had full regard to those submissions and I have reached final conclusions that infringements of data protection legislation have occurred and that it is necessary to exercise certain corrective powers. Those infringements and corrective powers are set out in this Decision.

4. Scope of the Inquiry

4.1 The scope of the Inquiry, which was set out in the Notice of the Commencement of the Inquiry, is to examine whether or not UCD has discharged its obligations in connection with the subject matter of the breaches and determine whether or not any provision(s) of the 2018 Act and/or the GDPR have been contravened by UCD in that context.

4.2 The personal data breaches concern unauthorised access to personal data concerning UCD's email service. 6 of the 7 breaches occurred where unauthorised third parties accessed UCD email accounts. BN-18-10-38 concerned an instance where email login credentials of 2 members of UCD staff and 1 corporate email address were published publicly online. UCD did not detect any unauthorised access to those accounts, however the personal data published online also included the staff members' names and passwords.

4.3 I am satisfied that UCD fulfils the role of controller in circumstances where it determines the purposes and means of the processing of personal data on its email service. The purposes of processing on the email service are set out by UCD in the *"UCD Information Technology Services Acceptable Use Policy"*, which provides that users of the network are entitled to use it for their academic requirements and that they are required to comply with UCD regulations[8]. This policy also sets out some of the essential means of processing by determining how access is issued and withdrawn. The Policy also provides that records are kept of network usage and can be made available in accordance with UCD policies. The policy provides that UCD retains ownership of all accounts, data, and services arising from accounts issued. Furthermore, UCD's Information Handling Standard, version 1.0, also outlines the means of processing strictly confidential, confidential, and controller information via email[9]. UCD submitted that Google provides its email service under the terms of the *"Google Apps for Education Agreement"* signed in 2012. It is not necessary for the purposes of this Decision to determine whether Google fulfils the role of controller, joint-controller, or processor. Pursuant to Articles 32 and 24 of the GDPR, UCD as a controller is responsible for implementing appropriate technical and organisational measures to ensure an appropriate level of security, and for demonstrating that processing is performed in accordance with the GDPR.

[8] UCD Information Technology Services Acceptable Use Policy, dated November 2013, at page 4.
[9] UCD Information Handling Standard, Version 1.0, at page 2.

5. Issues for Determination

5.1 Having reviewed the Inquiry Report and the other materials provided to me, I consider that the issues in respect of which I must make a decision are:

i. Whether UCD has complied with its obligations under Articles 5(1)(f) and 32(1) of the GDPR by implementing appropriate technical and organisational measures to ensure appropriate security of the personal data processed on its email service.

ii. Whether UCD has complied with its obligations under Article 5(1)(e) of the GDPR by ensuring that the personal data that it processes is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

iii. Whether UCD has complied with its obligations under Article 33(1) of the GDPR to notify the DPC of the relevant personal data breaches, in respect of breach notifications BN-18-10-423 and BN-19-01-213, without undue delay.

6. Issue 1: Articles 5(1)(f) and 32(1) of the GDPR

6.1 Article 5(1)(f) of the 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"*

6.2 Article 32(1) of the GDPR elaborates on the principle in Article 5(1)(f) 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."*

6.3 Articles 5(1)(f) and 32(1) of the GDPR oblige controllers and processors to implement an appropriate level of security. Not every instance of unauthorised access to personal data will necessarily constitute an infringement of Articles 5(1)(f) and 32(1). The level of security must be appropriate to the risk presented to the rights and freedoms of natural persons, and must have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing. This Decision must consider the appropriateness of the security measures implemented by UCD in respect of the processing of personal data on its email service at the time of the personal data breaches. In this regard, it is not appropriate to reason purely with the benefit of hindsight. Rather, this Decision must consider the appropriateness of the measures at the time of the personal data breaches in light of the risks that ought to have been known at the time. Therefore, the first step is to assess the risk presented to the rights and freedoms of data subjects by the processing of personal data on UCD's email service at the time of the personal data breaches. UCD did not document any such risk assessment in advance of the personal data breaches.

i. Assessing Risk

6.4 The processing of personal data on UCD's email service creates the risk that unauthorised third parties may gain access to the email accounts. The technical and organisational measures implemented must be appropriate to this risk.

6.5 Recital 76 of the 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."*

6.6 *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources and others*[10] provides further guidance on this risk assessment. In this case, the CJEU declared the Data Retention Directive[11] invalid. The Directive required electronic communication service providers to retain certain data for a period of time. The Court held that the directive did not ensure effective protection of the data retained against the risk of abuse and unlawful access in circumstances where it did not lay down specific rules in relation to (i) the vast quantity of data retained, (ii) the sensitive nature of the data, and (iii) the risk of unlawful access.

[10] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, intervener: Irish Human Rights Commission, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others, judgment of 8 April 2014 (ECLI:EU:C:2014:238).
[11] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

6.7 Risk is assessed objectively by reference to (i) the likelihood of the risk to the rights and freedoms of natural persons, and (ii) the severity of that risk. Hence, the risk assessment must consider, first, the likelihood of unauthorised access to UCD email accounts, and, second, the severity of that risk in respect of the rights and freedoms of the data subjects. These objective assessments are made by reference to the nature, scope, context and purposes of the processing. In considering these factors, regard must also be had to the quantity of personal data processed and the sensitivity of that data.

6.8 [redacted]

6.9 The nature of the personal data processed on UCD's email service varies on the scale of sensitivity. UCD's submissions, dated 19 March 2020, outline how the number of cases resulting in a high or medium risk were [redacted] This reflects how the personal data subject to the breaches was, in many instances, limited to names and email address of data subjects. [redacted]

6.10 The scope of the processing is broad. The University is a complex, decentralised, large organisation that supports a wide range of platforms catering to teaching, learning, student, research and administrative needs[12]. This results in an extensive range of personal data falling subject to processing on the service. As outlined above, the *"UCD Information Technology Services Acceptable Use Policy"* limits the purpose of using the network to users' academic requirements. Although this purpose may justify significant processing of personal data, I am satisfied that the manner in which the processing is limited to users' academic requirements mitigates the risk.

6.11 I find that the likelihood of [redacted] I make this finding in light of the [redacted] I find that the severity of the risk to the rights and freedoms of natural persons flowing from such unauthorised access is moderate. [redacted] However, this must be balanced with the fact that

[12] See UCD's submissions on the Draft Inquiry Report, dated 18 June 2020, at page 6.

the risk levels in respect of the vast majority of the data subjects concerned in the personal data breaches were low[13].

ii. Security Measures Implemented by UCD

6.12 UCD made submissions throughout the Inquiry detailing the technical and organisational measures implemented at the time of the personal data breaches to provide for the security of its email service. UCD also made submissions on the steps that is has taken since the personal data breaches to enhance the security, including in its submissions on the Draft Decision. This Decision considers the level of security implemented at the time of the breaches. Therefore, the measures implemented since the breaches are not relevant to determining whether an infringement of Articles 5(1)(f) or 32(1) occurred at the time of the breaches. However, Part 9 of this Decision details how these measures are relevant to the issue of corrective powers.

6.13 [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

iii. The Appropriate Level of Security

6.18 Having regard to the likelihood and severity of the risk of unauthorised access to UCD email accounts, I find that an appropriate level of security includes [redacted]

6.19 [redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted]

[redacted]

iv. Finding

6.24 I find that UCD infringed Articles 5(1)(f) and 32(1) of the GDPR between 25 May 2018, when the GDPR entered into force, and the dates of the personal data breaches, by failing to process personal data on its email service in a manner that ensured appropriate security of the personal data using appropriate technical and organisational measures.

7. Issue 2: Articles 5(1)(e) of the GDPR

7.1 The personal data in breach BN-18-9-175 included [redacted] the day of the inspection, UCD could offer no reason for the retention of the [redacted]

i. The Principle of Storage Limitation

7.2 Article 5(1)(e) of the GDPR provides that personal data shall be:

> *"kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of*

the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')"

7.3 Recital 39 of the GDPR provides:

> *"…In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review…"*

7.4 In *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*[21] the CJEU held that, in the context of the principle of storage limitation amongst others, *"the controller must take every reasonable step to ensure that data which do not meet the requirements of that provision are erased or rectified"*[22]. The Court went on to hold that:

> *"It follows from those requirements, laid down in Article 6(1)(c) to (e) of Directive 95/46, that even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed. That is so in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed."*[23]

7.5 It is clear that UCD's purpose for collecting and storing [redacted] However, UCD was unable to provide any purpose for the retention of the [redacted] I am satisfied that UCD infringed Article 5(1)(e) of the GDPR by storing [redacted] after they were no longer necessary for the purpose of [redacted] I am satisfied that UCD failed to take reasonable steps to ensure that [redacted] erased when no longer necessary for their purpose.

ii. Finding

7.6 I find that UCD infringed Article 5(1)(e) of the GDPR by storing [redacted] in the email account compromised in BN-18-9-175 in a form which permitted the identification of the data subject for longer than necessary for the purpose for which the personal data were processed.

[21] Case C-131/12, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, judgment of 13 May 2014, (ECLI:EU:C:2014:317).
[22] Ibid at paragraph 72.
[23] Ibid at paragraph 93.

8. Issue 3: Article 33(1) of the GDPR

8.1 UCD notified the DPC of all of the personal data breaches considered in this Decision. However, Article 33(1) requires that such notifications must occur without undue delay. Breach notification BN-18-10-423 concerned unauthorised access to two email accounts. UCD became aware of the access to one of the email accounts on 11 October 2018, and became aware of the access to the second account on 22 October 2018. UCD notified the DPC of both personal data breaches together on 24 October 2018.

8.2 Breach notification BN-19-01-213 concerned unauthorised access to one email account. UCD became aware of a potential compromise in security on 18 January 2018 at 16:30 and notified the DPC on 21 January at 19:24. Hence, breach notifications BN-18-10-423 and BN-19-01-213 occurred over 72 hours after UCD became aware of the underlying personal data breaches. Notifying outside the 72 hour period does not per se constitute an infringement of Article 33(1) and that Article acknowledges that it will not always be feasible to notify within 72 hours. Therefore, this Decision must consider whether, in each individual case, there was an undue delay in notifying the DPC outside the 72 hour period.

i. The Obligation to Notify Without Undue Delay

8.3 Article 33(1) of the 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."*

8.4 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. Article 4(12) defines personal data breach:

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

8.5 Article 33(1) requires that notifications must occur without undue delay. What constitutes undue delay must be assessed from when UCD became aware of each personal data breach. The Article 29 Working Party Guidelines on Personal data breach notification under Regulation 2016/679[24] provide that:

[24] Article 29 Working Party, Guidelines on Personal Data breach notification under Regulation 2016/679, Adopted 6 February 2018.

"WP29 considers 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."[25]

8.6 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." [26]

ii. The Breach Notifications

8.7 In breach notification BN-18-10-423, UCD assessed the risk of the breaches for affected individuals as a medium risk. At the time of the notification, the email accounts were under review by UCD to assess what personal data had been compromised. [redacted] On 4 January 2019, UCD updated the DPC and confirmed that the personal data compromised contained mainly business-related content and that there was not a significant amount of personal data over and above email addresses and content of a work nature. [redacted]

8.8 Controllers are not under an obligation to notify the DPC if the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. However, I am satisfied that the personal data breaches concerned in BN-18-10-423 did result in such a risk and therefore UCD was obliged to notify the DPC without undue delay. In assessing risk, regard must be had objectively to both the likelihood and severity of the risk to the rights and freedoms of data subjects. The personal data in the personal breaches notified in BN-18-10-423 was not particularly sensitive personal data and this reduced this risk to data subjects. However, in assessing risk it is appropriate to have regard to [redacted] In the circumstances, I am satisfied that the personal data breaches resulted in a risk to the rights and freedoms of data subjects, including, but not limited to, [redacted] Therefore, UCD was obliged to notify the DPC of both personal data breaches without undue delay.

8.9 UCD notified the DPC of the first personal data breach in BN-18-10-423 13 days after becoming aware of it. In explaining the reason for the delay, UCD submitted that they sought to batch the notifications in pairs to help manage resources in circumstances where they are part of a wider event. I find that the existence of another similar personal data breach does not justify notifying the DPC 13 days after a personal data breach has been detected. In the circumstances, I find that this constitutes an undue delay.

[25] Ibid at page 10.
[26] Ibid at page 11.
[27] Ibid at page 26.
[28] Ibid at page 25.

8.10 In breach notification BN-19-01-213, UCD assessed the risk of the breaches for affected individuals as medium risk. [redacted] In light of the nature of some of the personal data compromised, I am satisfied that the personal data breach resulted in a risk to the rights and freedoms of data subjects. Therefore, UCD was obliged to notify the DPC of both personal data breaches without undue delay.

8.11 UCD notified the DPC of the personal data breach in BN-19-01-213 just under 75 hours after detecting what was deemed to be a potential incident at the time. The reason for the delay in notifying is explained in the breach notification. The incident was originally not categorised as a personal data breach. Instead, UCD carried out further investigations before categorising it as a personal data breach on 21 January 2019. The breach notification guidelines provide that after a controller is first informed of a potential breach:

> *"the controller may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation the controller may not be regarded as being "aware". However, it is expected that the initial investigation should begin as soon as possible and establish with a reasonable degree of certainty whether a breach has taken place; a more detailed investigation can then follow"*[29]

8.12 In the circumstances, I find that further investigations were necessary for UCD to establish whether or not a personal data breach had occurred. The detection of a potential incident occurred due to UCD's routine review of login logs. Furthermore, the account in question was a generic group account with multiple users. I am satisfied that UCD promptly undertook the investigation and became aware of a personal data breach on 21 January 2019, before notifying the DPC on the same day. Therefore, I find that UCD did not infringe Article 33(1) in respect of its notification to the DPC for the personal data breach concerned in BN-19-01-213.

iii. Findings

8.13 I find that UCD infringed Article 33(1) of the GDPR by failing to notify the DPC of the first personal data breach detailed in BN-18-10-423 without undue delay.

8.14 I find that UCD did not infringe Article 33(1) of the GDPR in respect of notifying the DPC of the incident detailed in BN-19-01-213.

9. Decision on Corrective Powers

9.1 I have set out above, pursuant to Section 111(1)(a) of the 2018 Act, my decision to the effect that UCD has infringed Articles 5(1)(f) & 32(1), 5(1)(e), and 33(1) of the GDPR. Under Section 111(2) of the 2018 Act, where the Commission makes a decision (in accordance with 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

[29] Ibid at page 11.

Decision is whether or not those infringements merit the exercise of any of the corrective powers set out in Article 58(2) and, if so, which one(s).

9.2 Recital 129, which acts as an aid to the interpretation of Article 58, provides that *"… 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 ….*" In the circumstances of the within inquiry, and with particular reference to the findings arising therefrom, I find that the exercise of one or more corrective powers is both appropriate, necessary and proportionate for the purpose of ensuring compliance with the GDPR. Having carefully considered the infringements, I have decided to exercise corrective powers in accordance with Section 115 of the 2018 Act and Article 58(2) of the GDPR. I set out below the corrective powers that are appropriate to address the infringements in the particular circumstances, and the reasons for that decision, having considered all of the corrective powers set out in Article 58(2). In summary, the corrective powers that I have decided to exercise are:

a) Article 58(2)(d) – I have decided to order UCD to bring its processing into compliance with Articles 5(1)(f) & 32(1) of the GDPR;
b) Article 58(2)(b) – I have decided to issue a reprimand to UCD in respect of its infringements of Articles 5(1)(f) & 32(1), 5(1)(e) and 33(1) of the GDPR; and
c) Article 58(2)(i) – I have decided to impose an administrative fine, pursuant to Article 83, in respect of UCD's infringements of Articles 5(1)(f) & 32(1), 5(1)(e) and Article 33(1) of the GDPR.

A. Order to Bring Processing into Compliance

9.3 In accordance with Article 58(2)(d) of the GDPR, I order UCD to bring its processing operations regarding its email service into compliance with Articles 5(1)(f) and 32(1) of the GDPR. This order requires UCD to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

9.4 This order is made to ensure that full effect is given to UCD's obligation to implement appropriate technical and organisational measures. In deciding that an order is appropriate to achieve this end, I have had particular regard [redacted] I consider that additional technical and organisational measures are essential to protect the rights and freedoms of data subjects. UCD must perform the necessary risk assessment to inform the measures that it must implement. However, as outlined above, those measures should include:

- [redacted]
- [redacted]

[redacted]

9.5 It must be noted that implementing these measures does not relieve UCD of its obligation to continually evaluate the effectiveness of its measures and the measures that are necessary to ensure a level of security that is appropriate to the dynamic risk presented by its processing of personal data on its email service.

9.6 I direct UCD to submit a report to the DPC outlining the steps it has taken in respect of each of these measures on or before **1 July 2021**. [redacted]

B. Reprimand

9.7 I issue UCD with a reprimand in respect of its infringements of Articles 5(1)(f) & 32(1), 5(1)(e) and 33(1) of the GDPR. Article 58(2)(b) provides that a supervisory authority shall have the power to *"issue reprimands to a controller or processor where processing operations have infringed provisions of this Regulation."* I consider that a reprimand is necessary and proportionate in view of ensuring compliance with the infringed Articles as the reprimand, along with the administrative fine, will act to formally recognise the serious nature of all of the infringements. Further, the reprimand emphasises the requirement for UCD to take all relevant steps to ensure future compliance with Articles 5(1)(f) & 32(1), 5(1)(e) and 33(1) of the GDPR.

9.8 Recital 148 of the GDPR provides:

> *"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."*

9.9 Accordingly, it is clear from the GDPR that a reprimand does not have to be issued in isolation to the exercise of any other corrective power. In this respect, I find that it is necessary and proportionate to impose a reprimand in addition to the order in Part 9(A) of this Decision and the administrative fine detailed below. I have made this decision having particular regard to the nature of the infringements of Articles 5(1)(f) & 32(1), 5(1)(e) and 33(1) of the GDPR. The objective of Articles 5(1)(f) and 32(1) is to ensure that controllers and processors implement a level of security that is appropriate to the risk presented by

their processing operations. Furthermore, Article 5(1)(e) seeks to ensure that personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. In addition to the general protection to the rights and freedoms of data subjects, Article 5(1)(e) has specific relevance where personal data breaches occur, such as those under consideration in this Decision. I consider that the realisation of this principle is also essential to mitigating the effects of personal data breaches where they do occur. The objective of Article 33(1) is to ensure prompt notification of data breaches to supervisory authorities so that a supervisory authority can assess the circumstances of the data breach, including the risks to data subjects, and decide whether the interests of data subjects require to be safeguarded to the extent possible by mitigating the risks to them. Non-compliance with Article 33(1) can have adverse impacts on the rights and freedoms of data subjects and must be dissuaded. The underlying personal data breaches considered in this Decision illustrate the potential harm that can flow from UCD's infringements of Articles 5(1)(f) & 32(1), 5(1)(e) and 33(1). Therefore, I consider that the formal recognition of the seriousness of the infringements by means of a reprimand is appropriate and necessary to ensure compliance with these Articles. A reprimand is proportionate in the circumstances where it does not exceed what is required to enforce ensure compliance with the GDPR, taking into account the seriousness nature of the infringements and the potential for harm to data subjects.

C. Administrative Fine

9.10 In addition to the corrective powers under Article 58(2)(b) & (d), I have also decided that each of UCD's infringements of Articles 5(1)(f) & 32(1), 5(1)(e), and 33(1) of the GDPR warrant the imposition of administrative fines. The reason for that decision, and the method for calculating those fines, are set out below. As further detailed below, and in accordance with Article 83(3) of the GDPR, this Decision imposes one single administrative fine in respect of all of the infringements in circumstances where the distinct infringements relate to the same or linked processing operations. The amount of that fine is calculated by reference to the gravest infringement only.

i. Whether Each Infringement Warrants an Administrative Fine

9.11 Article 58(2)(i) permits the Commission to consider the imposition of an administrative fine, pursuant to Article 83, in addition to, or instead of, the other measures outlined in Article 58(2), depending on the circumstances of each individual case. This is also reflected in Section 115 of the Data Protection Act, 2018, which permits the Commission to impose an administrative fine on its own or in combination with any other corrective power specified in Article 58(2). Article 83(1), in turn, identifies that the administration of fines *"shall in each individual case be effective, proportionate and dissuasive"*. In this context, when deciding whether or not to impose administrative fines and the amount of any such fines, I must give due regard to the criteria set out in Article 83(2) GDPR, which provides that:

> *"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:

(a) 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;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) 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;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) 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;

(i) 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;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) 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."

9.12 These criteria are crucial to the decision as to whether or not to impose administrative fines and the amount of any such fines. Therefore, I will now proceed to consider each of these criteria in turn in respect of UCD's infringements of Articles 5(1)(f) & 32(1), 5(1)(e), and 33(1) respectively:

a) <u>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;</u>

9.13 The nature of UCD's infringements of Articles 5(1)(f) and 32(1) comprises a failure to comply with its obligation to implement an appropriate level of security in respect of its processing operations on its email service. The objective of Articles 5(1)(f) and 32(1) is to ensure that 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 data subjects because of the potential for damage to data subjects where personal data breaches occur. Therefore, compliance with Articles 5(1)(f) and 32(1) is essential to protecting the rights and freedoms of natural persons. As such, non-compliance with this obligation has serious consequences in that it has the potential to result in damage to data subjects. This is particularly the case in circumstances where [redacted]

9.14 The nature of UCD's infringement of Article 5(1)(e) comprises a failure to keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. The storage of personal data when no longer necessary for their purpose constitutes a serious infringement of data subjects' rights. Storing personal data constitutes the processing of personal data and as such it is essential that storage takes place for no longer than is necessary for the purposes for which the personal data are processed. Furthermore, an infringement of Article 5(1)(e) heightens the potential damage to data subjects where personal data breaches occur.

9.15 The nature of UCD's infringement of Article 33(1) comprises a failure to notify the DPC of a personal data breach without undue delay. The objective of Article 33(1) is to ensure prompt notification of personal data breaches to supervisory authorities as outlined above. Non-compliance with Article 33(1) (whether in absolute terms, where there is no notification made at any point, or where there is non-compliance with the timeframe for notification) will interfere with that objective by preventing or delaying the supervisory authority from taking such enforcement action as may be appropriate in light of the risks posed by the particular data breach. This, in turn, may have an impact on the safeguards and mitigation measures which data subjects might otherwise benefit from. In other words, this may compound the potential damage suffered by data subjects – first, from the occurrence of the data breach itself and second, by stymying or delaying the taking of safeguarding actions on the part of the supervisory authority.

9.16 I therefore consider that the nature of the obligations arising from Articles 5(1)(f) & 32(1), 5(1)(e), and Article 33(1) of the GDPR are such that, compliance is central to the protection of the rights and freedoms of data subjects and to the overall functioning of the supervision and enforcement regime performed by supervisory authorities respectively. As such, non-compliance with these obligations has serious consequences in that it poses a threat to the rights and freedoms of data subjects and risks undermining the effective exercise by supervisory authorities of their functions under the GDPR. In those circumstances, I consider that the nature of the infringements of Articles 5(1)(f) & 32(1), 5(1)(e), and Article 33(1) of the GDPR are serious in the circumstances.

9.17 The gravity of the infringements of Articles 5(1)(f) and 32(1) are serious in circumstances where the infringements resulted in the personal data breaches notified in the 7 breach notifications. [redacted] For example, UCD estimated that the first personal data breach in BN-18-10-423 [redacted] For example, BN-18-9-306 included [redacted] It also included details of 7 disciplinary cases taken against staff. Furthermore, the gravity of the infringements must be assessed in light of how the personal data breaches had the potential to result in [redacted]

9.18 The gravity of the infringement of Article 5(1)(e) is moderate. This infringement concerns [redacted] linked to identifiable data subjects, for longer than necessary for the purposes for which they were being processed. While this constitutes [redacted] in assessing the gravity of the infringement, I must also have regard to the fact that none of the data subjects reported [redacted] Despite that it appears that fraud did not materialise, I consider the gravity of this infringement to be moderate in circumstances where [redacted]

9.19 The gravity of the infringement of Article 33(1) is moderate. In UCD's notification to the DPC in BN-18-10-423, UCD outlined how it was still reviewing the email accounts to assess what information was contained in them. This was 13 days after becoming aware of the first personal data breach. Therefore, I consider that UCD's infringement of Article 33(1) had real implications for the DPC's capacity to assess the circumstances of the personal data breach and to ensure that the full effects of the breach are understood and analysed expeditiously. However in assessing the gravity of this infringement, I must also have regard to the fact that it was not ultimately necessary to notify the data subjects of the personal data breach in the particular circumstances. Further, I must also have regard to how UCD implemented mitigation measures during the currency of the infringement and before notifying the DPC. On balance, I find that the gravity of this infringement is moderate.

9.20 Regarding the duration of the infringements of Articles 5(1)(f) and 32(1), it is significant that the personal data breaches occurred between 19 August 2018 and 18 January 2019. It is also clear that the infringement of Articles 5(1)(f) and 32(1) commenced at the enactment of the GDPR in May 2018. This Decision considers the security measures that UCD implemented at the time of the personal data breaches and it does not make findings in relation to the level of security that it currently implements. Therefore, the duration of the infringement, for the purposes of this Decision, must be assessed as commencing on 25 May 2018 and ending on the date of the latest personal data breach on 18 January 2019. Therefore, the duration is 7 months and 3 weeks in length.

9.21 Regarding the duration of the infringement of Article 5(1)(e), UCD has not identified precisely when the [redacted] were no longer necessary for the purpose for which they were processed. However, [redacted] I am satisfied that the infringement of Article 5(1)(e) was of significant length.

9.22 Regarding the duration of the infringement of Article 33(1), as outlined above, UCD notified the DPC of the personal data breach 13 days after becoming aware of it. In the circumstances, I find that anything over 72 hours would constitute an undue delay. Therefore, the duration of UCD's infringement of Article 33(1) was 10 days in length. In the context of Article 33(1), I find that this duration is also of significant length.

b) <u>the intentional or negligent character of the infringement;</u>

9.23 The Article 29 Working Party Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679 provide that:

> *"In general, "intent" includes both knowledge and wilfulness 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."*[30]

9.24 I recognise that UCD's infringements of Articles 5(1)(f) & 32(1), 5(1)(e), and 33(1) of the GDPR were not intentional nor deliberate acts/omissions on the part of UCD. I do not consider that there was *"intent"* on the part of UCD in respect of these infringements in the sense that there was *"knowledge"* or *"wilfulness"* on the their part in respect of their failure to implement an appropriate level of security, [redacted] in BN-18-9-175, or to notify the DPC of the first personal data breach in BN-18-10-423 without undue delay.

9.25 I find that UCD was, however, negligent within the meaning of Article 83(2)(b) in respect of these infringements. UCD is a large, complex organisation that processed a significant volume of personal data. In those circumstances, it ought to have been aware of the extent of its obligations to take appropriate steps to appropriately secure the personal data that it processes, to ensure that the personal data is stored in an identifiable form for no longer than necessary, and to ensure that it notifies the DPC of personal data breaches without undue delay where they do occur. In the circumstances, I consider that there was a negligent character to UCD's infringements of Articles 5(1)(f) & 32(1), 5(1)(e), and 33(1) of the GDPR.

[30] Article 29 Data Protection Working Party 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679' at page 11.

c) Any action taken by the controller or processor to mitigate the damage suffered by data subjects;

9.26 I am satisfied that UCD took significant action to mitigate the damage suffered by data subjects as a result of the infringements. UCD took appropriate action in respect of all of the personal data breaches to re-secure the email accounts, including [redacted] In respect of BN-18-9-175, UCD took steps to ensure that the [redacted] Despite the delay in notifying the DPC of BN-18-10-423, UCD took steps to secure the concerned email accounts prior to notifying the DPC.

d) 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;

9.27 As outlined above, the UCD infringed Articles 5(1)(f) and 32(1) of the GDPR by failing to implement appropriate technical and organisational measures regarding its processing of personal data on its email service. I consider that UCD holds a high degree of responsibility for this failure and that the absence of such measures must be deterred. However, in circumstances where this factor forms the basis for the finding of the infringements of Articles 5(1)(f) and 32(1) against UCD, this factor cannot be considered aggravating in respect of those infringements.

9.28 In breach notification BN-18-10-423, UCD submitted that additional resources are being sought to ensure that UCD can meet the 72 hour notification deadline. UCD is obliged to ensure that it has appropriate measures in place, including in relation to staffing measures, to meet its obligations under Article 33(1). Furthermore, UCD did not submit any evidence of organisational measures to ensure compliance with the storage limitation principle in respect of the [redacted] in BN-18-9-175, for example, a retention policy. I find that UCD holds a high degree of responsibility for failing to implement such measures in respect of its infringements of Articles 5(1)(e) and 33(1) of the GDPR.

e) any relevant previous infringements by the controller or processor;

9.29 There are no relevant previous infringements by UCD.

f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

9.30 UCD cooperated fully with the DPC to remedy the infringements and to mitigate their adverse effects. In its breach notifications and incident reports, UCD illustrated the steps that it had taken, and was in the course of taking, to remedy the infringements and the possible adverse effects. UCD cooperated fully with the DPC throughout the Inquiry, including on the day of the inspection, in seeking to remedy the infringements.

Furthermore, UCD's submissions during the Inquiry detailed the measures that UCD has implemented, and is in the course of implementing, to provide an appropriate level of security in respect of its email service. [redacted]

9.31 In respect of UCD's infringement of Article 5(1)(e), UCD outlined that [redacted] In respect of UCD's infringement of Article 33(1), UCD's DPO has sought additional staff resources to ensure that personal data breaches are notified without undue delay.

g) <u>the categories of personal data affected by the infringement;</u>

9.32 I consider that the categories of personal data affected by the infringements of Articles 5(1)(f) and 32(1) included sensitive personal data. As outlined in Part 6 of this Decision, [redacted] Some of this personal data is by its very nature particularly sensitive with regard to the fundamental rights and freedoms of data subjects. I find that the sensitivity of these categories of personal data aggravates the infringements of Articles 5(1)(f) and 32(1) in circumstances where unauthorised access to these categories of personal data can cause immediate damage and distress to data subjects. In particular, [redacted]

9.33 Regarding the infringement of Article 5(1)(e), this infringement also concerned [redacted] However, I acknowledge that this infringement did not include other sensitive personal data. Regarding the infringement of Article 33(1), despite the quantity of personal data and the number of data subjects concerned, I consider that the categories of personal data affected were on the lower scale of sensitivity in circumstances where the underlying breach was limited to [redacted]

h) <u>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;</u>

9.34 The Inquiry was conducted to examine whether or not UCD has discharged its obligations in connection with the subject matter of the breaches and determine whether or not any provision(s) of the 2018 Act and/or the GDPR had been contravened by UCD in that context. Hence, UCD's notification of the personal data breaches indirectly contributed to the infringements becoming known to the DPC.

9.35 The Administrative Fines Guidelines consider the relevance of such notifications regarding administrative fines:

> *"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."*[31]

9.36 UCD's compliance with its own obligation to notify personal data breaches under Article 33(1) cannot be considered mitigating in respect of the infringements of Articles 5(1)(f), 32(1) and 5(1)(e). Similarly, UCD's undue delay in notifying the DPC of the first personal data breach notified in BN-18-10-423 is not aggravating in circumstances where that infringement is the subject of consideration for this corrective power.

i) <u>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;</u>

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

j) <u>adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42;</u>

9.38 Not applicable.

k) <u>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.</u>

[31] Article 29 Data Protection Working Party 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, at page 15.

9.39 I consider that the matters considered under Article 83(2)(a) – (j) reflect an exhaustive account of both the aggravating and mitigating factors applicable in the circumstances of the case.

9.40 When imposing corrective measure(s), I am obliged to select the measure(s) that are effective, proportionate and dissuasive in response to the particular infringements. The assessment of what is effective, proportionate and dissuasive must be made in the context of the objective pursued by the corrective measures. The Administrative Fines Guidelines provide that:

> *"The assessment of what is effective, proportional and dissuasive in each case will have to also reflect the objective pursued by the corrective measure chosen, that is either to reestablish compliance with the rules, or to punish unlawful behavior (or both)."*[32]

9.41 I find that administrative fines are necessary and appropriate in respect of the infringements in order to effectively pursue the objective of re-establishing compliance with the Articles 5(1)(f) & 32(1), 5(1)(e), and 33(1) of the GDPR and in providing an effective, proportionate and dissuasive response in the particular circumstances of this case.

9.42 Regarding UCD's infringements of Articles 5(1)(f) & 32(1) and 5(1)(e), I consider that the reprimand made in Part 9(B) of this Decision is of significant value in dissuading future non-compliance. This formal recognition of the seriousness of UCD's infringements is likely contribute somewhat to ensuring an appropriate level of security and compliance with the principle of storage limitation going forward. Furthermore, in relation to UCD's infringements of Articles 5(1)(f) & 32(1), I have had regard to the order made in Part 9(A) of this Decision. This order has significant value in re-establishing compliance with Articles 5(1)(f) and 32(1) because it obliges UCD to take certain specified steps in implementing technical and organisational measures. However, having regard to circumstances of the infringements of Articles 5(1)(f) & 32(1) and 5(1)(e), I find that the order and reprimand alone are not effective and proportionate in re-establishing compliance and in dissuading future non-compliance. Articles 5(1)(f) and 32(1) place a continuous obligation on controllers and processors to regularly test, assess and evaluate the effectiveness of the technical and organisational measures implemented. Furthermore, the appropriate level of security must be continually re-assessed in light of the dynamic risk presented by UCD's processing of personal data and the state of the art. Therefore, compliance with the order in Part 9(A) of this Decision alone cannot ensure perpetual compliance with Articles 5(1)(f)and 32(1) going forward, as the risk changes and as new measures emerge in respect of these processing operations. Similarly, the obligation in Article 5(1)(e) of the GDPR places a continuous obligation on controllers to assess when it is no longer necessary to store certain personal data in respect of the purposes for which the personal data are processed. I do not consider that the order and reprimand alone constitute a sufficiently effective, proportionate and dissuasive response to the infringements of Articles 5(1)(f) & 32(1), and

[32] Article 29 Data Protection Working Party 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, at page 11.

5(1)(e) in light of the need to re-establish compliance and to dissuade non-compliance. In coming to the conclusion that administrative fines are also necessary, I have particular regard to how the categories of personal data concerned in the infringements [redacted] Providing an appropriate level of security in respect of the concerned personal data and limiting the storage of such personal data are essential to protecting the rights and freedoms of data subjects. In light of the negligent character and serious nature of the infringements, I consider that administrative fines are appropriate, necessary and proportionate to ensure compliance with Articles 5(1)(f) & 32(1), and 5(1)(e) and to dissuade non-compliance.

9.43 Regarding UCD's infringement of Article 33(1) of the GDPR, I consider that re-establishing compliance must encompass dissuading non-compliance. Article 33(1) of the GDPR necessitates prompt action from data controllers in notifying supervisory authorities. In many instances, such action is essential to protecting the rights and freedoms of data subjects. I consider that the reprimand alone is not sufficient to effectively and proportionately re-establish compliance and dissuade non-compliance. In particular, in light of [redacted] and the negligent character of the infringement, I consider that an administrative fine is necessary in order to dissuade future undue delays of this nature. In light of these factors, having considered all of the corrective powers available to me as set out in Article 58(2) of the GDPR, I find that an administrative fine is appropriate, necessary and proportionate to ensure compliance with Article 33(1).

9.44 I have had regard to all of the corrective powers available to me as set out in Article 58(2) of the GDPR. For the reasons set out above, and having particular regard to the matters discussed under Article 83(2)(a) – (j) cumulatively, I find that it is appropriate to impose an administrative fine in respect of each of the infringements of Articles 5(1)(f) & 32(1), 5(1)(e), and 33(1) of the GDPR in addition to the order and reprimand imposed at parts 9(A) & (B) of this Decision.

ii. The Permitted Range

9.45 Having decided that each of the infringements of Articles 5(1)(f) & 32(1), 5(1)(e), and 33(1), warrant the imposition of an administrative fine in the circumstances of this case, I must next proceed to decide on the amount of each of those fines. First, it is necessary to consider the appropriate cap for the fines as a matter of law. The cap determines the permitted range for the fines, from a range of zero to the cap. However, the cap is not a starting point for a fine. After identifying the permitted range, it is necessary to then calculate each fine.

9.46 Section 141(4) of the 2018 Act provides a cap on administrative fines concerning public authorities and public bodies that do not act as undertakings:

"Where the Commission decides to impose an administrative fine on a controller or processor that—

(a) is a public authority or a public body, but

(b) is not a public authority or a public body that acts as an undertaking within the meaning of the Competition Act 2002,

the amount of the administrative fine concerned shall not exceed €1,000,000."

9.47 Firstly, in order for this cap to apply, the controller or processor in question must be a public authority or a public body. *"Public authority"* is defined in Section 2 of the 2018 Act and this definition includes *"any other person established by or under an enactment (other than the Act of 2014 or a former enactment relating to companies within the meaning of section 5 of that Act)"*. UCD was reconstituted as a constituent university pursuant to the Universities Act 1997. Therefore, I am satisfied that UCD is a public authority for the purposes of the 2018 Act.

9.48 Secondly, in order for the cap to apply, the controller of processor must not act as an undertaking within the meaning of the Competition Act 2002. Section 3 of the Competition Act 2002, as amended by Section 47 of the Competition and Consumer Protection Act 2014, defines *"undertaking"* as:

"a person being an individual, a body corporate or an unincorporated body of persons engaged for gain in the production, supply or distribution of goods or the provision of a service and, where the context so admits, shall include an association of undertakings."

9.49 UCD submitted that it does not fulfil the definition of undertaking[33]. It is established that UCD is engaged in the provision of educational services. Furthermore, the pursuit of profit is not necessary in order to fulfil the definition of undertaking[34]. However, in *Belgium v Humble and Edel*[35] the European Court of Justice held that the provision of the national education system does not constitute gainful activity, but rather concerns the State "*fulfilling its duties towards its own population in the social, cultural and educational fields"*[36]. The Court held that students paying teaching or enrolment fees does not affect the nature of this activity. I am satisfied that UCD's provision of educational services does not constitute an economic activity and there is no evidence to suggest that UCD conducts a separate economic activity that would bring it within the definition of *"undertaking"*. I accept UCD's submission that is not an *"undertaking"* for the purposes of section 141(4) of the 2018 Act. I find that the permitted range for the administrative fines in this case must be calculated by reference to the cap in Section 141(4) of the 2018 Act. Therefore, the permitted range in respect of each fine is €0 - €1,000,000.

[33] UCD submissions on the Draft Decision, dated 1 December 2020, at page 1.
[34] Deane and others v VHI [1992] 2 I.R. 319.
[35] Case C263/86, Humble and Edel, E.C.R. 1988, p.5365.
[36] Ibid at paragraph 18.

iii. Calculating Administrative Fines

9.50 In the absence of specific EU-level guidelines on the calculation of fines in this context, I am not bound to apply any particular methodology[37]. The methodology that I have followed is intended to clearly and unequivocally set out the elements taken into account in calculating the fine, thereby allowing UCD, as the addressee, to understand the basis for the fine and ensuring that the fine is calculated in a rational manner.

9.51 The methodology that I have followed in calculating the administrative fines is as follows. The first step in calculating each administrative fine is to consider the permitted range and to locate the infringement on that permitted range. In this regard, the cap of €1,000,000 provided for in Section 141(4) of the 2018 Act is not a starting point. Rather, this cap is relevant to determining the permitted range. The determination of where on the permitted range the appropriate figure lies is made by reference to nature, gravity, and duration of each infringement, as considered in relation to Article 83(2)(a) above, and the other aggravating factors. The determination is made in the context of the objectives of re-establishing compliance, including through deterrence, and to provide a proportionate response to the unlawful behaviour. The second step in calculating each administrative fine is to apply the mitigating factors to reduce the fine where applicable. Finally, the third step is to consider whether the figure arrived at is *"effective, proportionate and dissuasive"* in the circumstances in accordance with Article 83(1) of the GDPR.

9.52 The Draft Decision set out proposed ranges for the administrative fines and the factors to be considered, and the methodology to be used when calculating the fines, in order to provide UCD with the opportunity comment in accordance with fair procedures. In its submissions on the Draft Decision, UCD highlighted its cooperation and the positive manner in which it engaged with the Inquiry. It also highlighted the investment that the University is making in providing for the security of the personal data that it processes. As outlined above, I consider these factors relevant to assessing the amount of the fines and I have had due regard to them in calculating the administrative fines below.

The infringements of Articles 5(1)(f) and 32(1) of the GDPR

9.53 As outlined above, the permitted range is €0 - €1,000,000. In locating the fine on the permitted range, I have had regard to the nature, gravity and duration of the infringement as assessed in accordance with Article 83(2)(a) above. I have also had regard to the aggravating factors, specifically the negligent character of the infringement and the sensitive categories of personal data affected by the infringement as assessed in accordance with Article 83(2)(b)&(g) above. I consider that the figure of **€145,000** is appropriate in the circumstances of this case before applying mitigation.

[37] See by analogy Electrabel v Commission, T 332/09, ECLI:EU:T:2012:672, para 228, Marine Harvest ASA v Commission, T-704/14, ECLI:EU:T:2017:753, para 450.

9.54 I find that the mitigating factors warrant a significant reduction in the fine. Specifically, I consider the factors identified above under Articles 83(2)(c), 83(2)(e), and 83(2)(f) of the GDPR mitigating. To account for the action taken by UCD to mitigate the damage suffered by the data subjects, I have reduced the fine by **€20,000** in accordance with Article 83(2)(c). To account for UCD's lack of previous infringements, I have reduced the fine by **€20,000**, in accordance with Article 83(2)(e). To account for the cooperation that UCD engaged with the DPC to remedy the infringement, I have reduced the fine by **€35,000** in accordance with Article 83(2)(f). Thus, the total reductions in light of the mitigating factors is **€75,000**. Therefore, the final figure for the administrative fine is **€70,000**.

The infringement of Article 5(1)(e) of the GDPR

9.55 As outlined above, the permitted range is €0 - €1,000,000. In locating the fine on the permitted range, I have had regard to the nature, gravity and duration of the infringement as assessed in accordance with Article 83(2)(a) above. I have also had regard to the aggravating factors, specifically the negligent character of the infringement, the degree of responsibility of UCD taking into account the lack of organisational measures to ensure compliance with the storage limitation principle in respect of the [redacted] affected by the infringement, as assessed in accordance with Article 83(2)(b), (d) &(g) above. I consider that the figure of **€50,000** is appropriate in the circumstances of this case before applying mitigation.

9.56 I find that the mitigating factors warrant a significant reduction in the fine. Specifically, I consider the factors identified above under Articles 83(2)(c), 83(2)(e), and 83(2)(f) of the GDPR mitigating. To account for the action taken by UCD to mitigate the damage suffered by the data subjects, I have reduced the fine by **€15,000** in accordance with Article 83(2)(c). To account for UCD's lack of previous infringements, I have reduced the fine by **€5,000**, in accordance with Article 83(2)(e). To account for the cooperation that UCD engaged with the DPC to remedy the infringement, I have reduced the fine by **€10,000** in accordance with Article 83(2)(f). Thus, the total reductions in light of the mitigating factors is **€30,000**. Therefore, the final figure for the administrative fine is **€20,000.**

The infringement of Article 33(1) of the GDPR

9.57 As outlined above, the permitted range is €0 - €1,000,000. In locating the fine on the permitted range, I have had regard to the nature, gravity and duration of the infringement as assessed in accordance with Article 83(2)(a) above. I have also had regard to the aggravating factors, specifically the negligent character of the infringement and the degree of responsibility of UCD taking into account its lack of measures to ensure that personal data breaches are notified without undue delay, in accordance with Article 83(2)(b) & (d) above. I consider that the figure of **€70,000** is appropriate in the circumstances of this case before applying mitigation.

9.58 I find that the mitigating factors warrant a significant reduction in the fine. Specifically, I consider the factors identified above under Articles 83(2)(c), 83(2)(e), 83(2)(f) and 83(2)(g)

of the GDPR mitigating. To account for the action taken by UCD to mitigate the damage suffered by the data subjects, I have reduced the fine by **€5,000** in accordance with Article 83(2)(c). To account for UCD's lack of previous infringements, I have reduce the fine by **€7,500**, in accordance with Article 83(2)(e). To account for the cooperation that UCD engaged with the DPC to remedy the infringement, I have reduced the fine by **€5,000** in accordance with Article 83(2)(f). To account for how the categories of personal data affected by the underlying personal data breach were on the lower scale of sensitivity, I have reduced the fine by **€15,000.** Thus, the total reductions in light of the mitigating factors is **€32,500**. Therefore, the final figure for the administrative fine is **€37,500**.

iv. The Same or Linked Processing Operations

9.59 Article 83(3) of the GDPR provides:

> *"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."*

9.60 The findings of infringements of Articles 5(1)(f) and 32(1) both relate to the same processing operations regarding UCD's processing of personal data on its email service. Article 32(1) elaborates on the requirement for appropriate security in Article 5(1)(f). In the circumstances, the infringements of Articles 5(1)(f) and 32(1) arise from the same omission on the part of UCD to implement an appropriate level of security. Therefore, the limit in Article 83(3) is applicable and the total amount of the administrative fine must not exceed the amount for the gravest infringement.

9.61 The finding of an infringement of Article 5(1)(e) relates to UCD's storage of [redacted] on its email service in a form which permitted the identification of data subjects for longer than was necessary for the purposes for which they were processed. Therefore, the processing operation under consideration entails UCD's storage of personal data on its email service. The storage of personal data on UCD's email service is encompassed within the processing operations considered in respect of the findings of infringements of Articles 5(1)(f) and 32(1) in this Decision. Therefore, UCD's infringement of Article 5(1)(e) concerns the same processing operations as UCD's infringement of Article 5(1)(f) and 32(1).

9.62 Regarding UCD's infringement of Article 33(1), the underlying personal data breach concerning that infringement relates to unauthorised access to a UCD staff email account. Therefore, the underlying personal data breach relates to UCD's processing of personal data on its email service, including its storage of personal data. Therefore, it involves the same processing operations that are subject to findings of infringements of Articles 5(1)(f) and 32(1) in this Decision. It follows that this infringement of Article 33(1) relates to the same or linked processing operations as the infringements of Articles 5(1)(f) & 32(1) and 5(1)(e).

9.63 In light of the above, I am satisfied that the infringements of Articles 5(1)(f) & 32(1), 5(1)(e), and 33(1) found in this Decision concern the same or linked processing operations. Therefore, the amount of the fine which is to be imposed in respect of these infringements must not exceed the amount specified for the gravest infringement. I consider that UCD's infringement of Article 5(1)(f) & 32(1) is the gravest such infringement. This infringement directly resulted in all of the personal data breaches considered in this Decision. Those personal data breaches included a [redacted] UCD's failure to implement an appropriate level of security in respect of its email service has the potential to cause [redacted] in the absence of appropriate measures.

v. The Amount of the Administrative Fine

9.64 I find that the total amount of the administrative fine imposed in this Decision must not exceed the amount specified for the gravest infringement. On this basis, the fine to be imposed is limited to that specified for the infringements of Article 5(1)(f) & 32(1). Therefore, the amount of the administrative fine is **€70,000**.

9.65 The final step is to consider whether the figure arrived at is *"effective, proportionate and dissuasive"* in the circumstances in accordance with Article 83(1) of the GDPR. I consider that the figure of **€70,000** meets these requirements. In order for any fine to be effective, it must reflect the circumstances of the individual case. As outlined above, the infringements of Articles 5(1)(f) and 32(1) are serious. The underlying personal data breaches affected a [redacted] and UCD's failure to implement an appropriate level of security put the personal data of an [redacted] The potential consequences of the infringements are severe in circumstances where UCD processed [redacted] on its email service. In order for a fine to be dissuasive, it must dissuade both the controller/processor concerned as well as other controllers/processors carrying out similar processing operations from repeating the conduct concerned. I am satisfied that the amount of the fine would be dissuasive to both UCD and to similar controllers.

9.66 As regards the requirement for any fine to be proportionate, this requires me to adjust the quantum of any fine to the minimum amount necessary to achieve the objectives pursued by the GDPR. I am satisfied that the amount of the fine does not exceed what is necessary to enforce compliance with the GDPR, taking into account the impact of the infringements on the data subject rights enshrined in the GDPR and how UCD is a complex, decentralised, large University that supports a wide range of platforms catering to teaching, learning, student, research and administrative needs. The figure of €70,000 amounts to 7% of the

cap available and 0.01% of UCD's turnover[38]. Accordingly, I am satisfied that the amount of the fine is effective, proportionate and dissuasive, taking into account all of the circumstances of the Inquiry.

D. Summary of Corrective Powers

9.67 By way of summary, this Decision imposes the following corrective action:

a) **An order to UCD to bring its processing operations regarding its email service into compliance with Articles 5(1)(f) and 32(1) of the GDPR as detailed in Part 9(A) of this Decision. This order requires UCD to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.**

b) **A reprimand in respect of UCD's infringements of Articles 5(1)(f) & 32(1), 5(1)(e) and 33(1) of the GDPR as detailed in Part 9(B) of this Decision.**

c) **One administrative fine addressed to UCD of an amount €70,000 as detailed in Part 9(C) of this Decision.**

10. Right of Appeal

10.1 This Decision is issued in accordance with Section 111 of the 2018 Act. Pursuant to Section 150(5) of the 2018 Act, UCD has the right to appeal against this Decision within 28 days from the date on which notice of the Decision is received by it. Furthermore, as this Decision includes a decision to impose an administrative fine, pursuant to Section 142 of the 2018 Act, UCD also has the right to appeal against that decision to impose an administrative fine within 28 days from the date on which notice of the decision is given to it.

[38] The turnover of UCD in 2019 was €591,602,000, which is calculated by reference to the total reported income stream in UCD's Annual Report and Consolidated Financial Statements, year ended 30 September 2019, these being the most recently available figures.

Appendix: Schedule of Materials Considered for the Purposes of this Decision

The Inquiry Team delivered the Final Inquiry Report to me on 8 July 2020. I also had regard to all of the correspondence, submissions, and documentation gathered during the Inquiry and the decision-making stage, including:

i. The DPC's Final Inquiry Report, Inquiry Reference IN-19-7-4;
ii. UCD's Academic Structure document;
iii. DPC Notice of Commencement of an Inquiry, dated 19 July 2019;
iv. UCD's Response to the Commencement letter, dated 1 August 2019;
v. UCD IT Security screenshots;
vi. DPC Notice of Inspection, dated 1 November 2019;
vii. Email from UCD, dated, 27 November 2019, enclosing further documentation;
viii. DPC Letter to UCD, dated 10 March 2020;
ix. UCD's Submissions, dated 19 March 2020;
x. UCD's IT Security Incident Response Procedure, version 1.0, dated 1 November 2019;
xi. UCD's IT Services Disaster Recovery Policy, version 1.0, dated 6 November 2008;
xii. UCD's IT Services Remote Access Procedures , version 1.5, dated May 2017;
xiii. UCD's Password Protection Policy, version 2.4, dated October 2018;
xiv. UCD's Information Handling Standard, version 1.0;
xv. UCD's Information Security Management Policy, version 1.0, dated 7 May 2008;
xvi. UCD's IT Acceptable Use Policy, dated November 2013;
xvii. [redacted]
xviii. [redacted]
xix. UCD screenshots showing the difference between Administration and user's login details;
xx. UCD's document titled, "UCD Organisational Measures to enhance Data Protection Compliance", dated November 2019;
xxi. Documentation concerning the breach notification BN-18-9-175, including the breach notification form and updates, the emails between UCD and DPC, and UCD's IT Security Incident Report;
xxii. Documentation concerning the breach notification BN-18-9-306, including the breach notification form and updates, the emails between UCD and DPC, and UCD's IT Security Incident Report;
xxiii. Documentation concerning the breach notification BN-18-9-407, including the breach notification form and updates, the emails between UCD and DPC, and UCD's IT Security Incident Report;
xxiv. Documentation concerning the breach notification BN-18-10-38, including the breach notification form and updates, the emails between UCD and DPC, and UCD's IT Security Incident Report;

xxv. Documentation concerning the breach notification BN-18-10-88, including the breach notification form and updates, the emails between UCD and DPC, and UCD's IT Security Incident Report;

xxvi. Documentation concerning the breach notification BN-18-10-423, including the breach notification form and updates, the emails between UCD and DPC, and UCD's IT Security Incident Report;

xxvii. Documentation concerning the breach notification BN-19-1-213 including the breach notification form and emails between UCD and DPC;

xxviii. UCD'S Submissions, dated 18 June 2020;

xxix. UCD's Statement on Academic Freedom, dated November 2011;

xxx. University College Dublin National University of Ireland, Dublin, Annual Report and Consolidated Financial Statements, year Ended 30 September 2019; and

xxxi. UCD Response to the Data Protection Commissioner's Draft Decision on IN-19-7-4, dated 1 December 2020.