In the matter of the General Data Protection Regulation
Data Protection Commission Reference: IN-19-7-1
In the matter of University of Limerick

Final 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

FINAL DECISION

Dr Des Hogan, Commissioner for Data Protection;
Mr Dale Sunderland, Commissioner for Data Protection;
and
Ms Niamh Sweeney, Commissioner for Data Protection.

10 December 2025

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Protection Commission
6 Pembroke Row
Dublin 2, Ireland

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 the University of Limerick (**'UL'**) 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 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 UL will be required to comply with any corrective powers that are contained in this Decision, and it is open to the DPC to serve an enforcement notice on UL in accordance with section 133 of the 2018 Act.

B. Personal Data Breaches

7. UL was established as a university under the University of Limerick Act 1989, and is regulated under the Universities Act 1997. In 2020 (during the period when the breaches considered in this Decision occurred) UL had 16,300 students and 1,700 staff members.[1]

8. Between 30 November 2018 and 20 January 2020, UL notified the DPC of six personal data breaches that concerned unauthorised persons gaining access to the employee email accounts of UL staff members (**'the Breaches'**). [2]

9. In each of these, access to the email accounts was gained through 'phishing', in which authorised UL users received emails which contained a link to a page created by malicious persons using UL branding and which mimicked an authentic UL login page. Users were induced to enter their UL login details (i.e. their username and password), which allowed their details to be captured and used by an unauthorised third party. Of these breaches, four were linked to emails that asked users to enter their login details via a mimicked UL login page, one was a result of a fraudulent notification of a voicemail that caused two users to enter their login details, and one was the result of an email sent to 1430 UL staff members asking them to change their passwords via a link in the email, by means of which users' UL email accounts were then compromised. In some cases, the third party that gained unauthorised access to the relevant user's UL email account set up forwarding rules that diverted emails containing certain keywords to a folder they had created in the user's mailbox.

10. 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.

11. In each of the Breaches, unauthorised persons were known to have gained access to the employee email accounts of UL staff members. That such unauthorised access to records containing personal data could occur constituted 'a breach of security' as that term is understood in Article 4(12) GDPR. The access allowed the unauthorised persons to change the configuration of email accounts to hide messages from the account holders, and to divert those messages to a hidden folder set up by the unauthorised users. The unauthorised users gained access to all data held within the compromised email

---

1 UL Submission on the Draft Inquiry Report, 26 November 2020, p.12.

2 DPC breach reference numbers: BN-18-12-2; BN-19-4-3; BN-19-4-348; BN-19-6-96; BN-19-8-135; and BN-20-1 282.

accounts. 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.

12. The Breaches concern unauthorised access to personal data processed in UL's staff email system. In the time between the GDPR taking effect on 25 May 2018 and the commencement of this inquiry in July 2019, UL notified the DPC of 12 separate data breaches, of which 6 concerned similar phishing incidents.

a) Data Controller

13. In commencing the Inquiry, the DPC considered that UL may be the data 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, UL confirmed in its notification of the personal data breach to the DPC on 30 November 2018 that it was the data controller.[3]

14. The DPC is satisfied that UL is the data controller as all information provided, including UL's own submissions, indicate that UL 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 in UL's IT Security Policy, which states that email is provided to staff and students to enable them to pursue their work as an employee or student of the University.[4]

C. Legal Framework for the Inquiry and the Decision

a) Legal Basis for the Inquiry

15. The General Data Protection Regulation[5] (**'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. 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.

16. 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

---

3 Breach Notification Form, BN-18-12-2, 30 November 2018, p.1.

4 UL submission in response to Commencement Notice, 23 July 2019, p.100.

5 Regulation (EU) 2016/679 (General Data Protection Regulation).

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) Legal Basis for the Decision

17. 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.

18. 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 submissions made by UL in respect of the draft version of this Decision sent to UL on 7 October 2025 ('**the Draft Decision**') before proceeding to make this final Decision under section 111 of the 2018 Act.

D. Factual Background

19. Between 30 November 2018 and 20 January 2020, UL made 12 separate data breach notifications to the DPC.[6] Six of these breaches concern instances where unauthorised third parties gained access to UL staff email accounts and are considered in the material scope of this Inquiry. The dates of the incidents and the dates of notification to the DPC are summarised as follows:

Breach	Date of Incident	Date reported to the DPC
BN-18-12-2	19 November 2018	30 November 2018
BN-19-4-3	26 March 2019	29 March 2019
BN-19-4-348	12 April 2019	16 April 2019
BN-19-6-96	31 May 2019	06 June 2019
BN-19-8-135	02 August 2019	08 August 2019
BN-20-1-282	17 January 2020	20 January 2020

[6] In its submission on the Draft Decision, UL stated that it had lodged 11 breach notifications during this period. However, the DPC's records show 12 notifications between the dates in question.

20. **BN-18-12-2** occurred when a UL email account holder received an email from 'information-customer@boxcloud.net' stating that documents were available to download from Box, a cloud storage service. The user accepted the email as genuine and assumed they knew what documents these were. They clicked on the 'view documents' link in the email, which brought them to a fake webmail login screen that displayed a UL logo and that captured users' login credentials when submitted on that page. The user entered their login credentials which resulted in an error message stating that the password was incorrect. The user entered their login details a second time. When this did not work, the user exited the login screen. As a result, the user's UL email login credentials were compromised and were subsequently used by unauthorised persons to create a forwarding rule in their UL email account relating to 'international wire transfer'. The breach notification for this breach specified that PPSNs, contact details, identification documentation and economic or financial data were affected by it.

21. **BN-19-4-3** occurred when a UL email account holder received an email containing a link which redirected to a fake page that prompted the user to enter their UL credentials and captured those credentials. Over the course of the following 24 hours, the affected user's account was used to send emails to other accounts with this malicious link. It was found that 19 further users accessed this link. The breach notification stated that only identity information (i.e. "name, surname, birth date") was affected by this breach.

22. **BN-19-4-348** occurred when a UL email account holder received an email purporting to be from the email account of the UL President. The display name in the email was the genuine one used by the UL President, but the actual origin address was from an unrelated institution. The email contained a link which the user opened, taking them to a fake page on which the user entered their UL login credentials and those credentials were then captured. Malicious actors subsequently added forwarding rules via web client to the user's UL email account. The UL president's actual account was not found to have been compromised. As with BN-19-4-3, the breach notification identifies the affected personal data as comprising only identity information.

23. **BN-19-6-96** occurred when a UL email account holder received an email containing a link on 31 May 2019. The user assumed that the email was legitimate, clicked on the link and entered their UL login credentials on the linked page. Malicious actors subsequently added forwarding rules to the user's UL email account. The breach notification specified that personal data including data subject identification information and contact details were affected.

24. **BN-19-8-135** occurred when a phishing email was delivered to approximately 1,430 UL email account holders. The body of the email advised the users to update their accounts. The email included a link that sent users to a web site that mimicked UL's Outlook Web Access login page and captured users' login credentials. Data from 20 data subjects was

compromised as a result of this breach. The breach notification stated that data subject identification information, PPSNs, contact information and economic or financial data was affected.

25. **BN-20-1-282** occurred when a phishing email was delivered to 723 UL email account holders. The email had a subject line that read 'Voice Message' and contained a link to a website that mimicked the UL's Outlook Web Access login page. The actual address of the fake login page was in the canopy-bd domain. Two employees clicked on the link in the phishing email and provided their UL login credentials. Malicious actors subsequently added rules to the UL email account of one of the users. This account sent 14 emails to UL email users in the University Finance Department. That email contained a link again purporting to be a voice mail message, which pointed to the same canopy-bd website. The DPC notes however that none of the 14 recipients clicked that link.[7] The breach notification did not specify the types of personal data affected beyond the category 'Other'.

26. Each compromised account contained personal data and in some instances contained large volumes of sensitive personal data. The unauthorised 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 affected was not only that of the UL staff email account holders, but also that of a much greater number of third parties. This includes other staff members and students at UL, as well as persons outside UL. No evidence was provided during the course of this Inquiry regarding the identity or identities of the hackers, or that the attempts (successful or otherwise) to gain access originated from the same party.

27. Article 33(1) GDPR requires controllers to notify the competent supervisory authority of breaches without undue delay, and in any event within 72 hours of becoming aware of them. In all cases, UL notified the DPC of the Breaches. However, the breach notifications for BN-18-12-2, BN-19-6-96 and BN-19-8-135 were delivered more than 72 hours after UL became aware of those breaches and so fall to be considered in this Decision in the context of UL's obligation under Article 33(1) GDPR.

28. Article 34(1) GDPR requires controllers to communicate a data breach to data subjects without undue delay in cases where a personal data breach is likely to pose a high risk to rights and freedoms of natural persons. In BN-18-12-2, 379 data subjects affected by the breach (comprising persons whose data was accessible in the compromised email account) were notified of the incident, and in BN-19-4-3, 76 data subjects were similarly notified. However, in BN-19-4-348, 24 affected data subjects were not notified. In UL's

---

7 UL Submissions on Draft Decision, 25 November 2025, p. 38.

submission of 26 November 2020, it stated that it had determined that 369 data subjects were affected by the breach in BN-19-4-348, in that they had received the phishing email, but only one of these made their UL login details available to the hackers. During its breach investigation, UL determined that this compromised account held personal data of 24 individuals who were not notified of the breach. The DPC will therefore consider whether UL was obliged to notify those 24 data subjects in connection with BN-19-4-348. Regarding breaches BN-19-6-96, BN-19-8-135 and BN-20-1-282, the DPC is satisfied, based on the nature and classification of these breaches, that the data subjects' rights and freedoms were not at high risk, and accordingly that UL was not required to notify data subjects of the breaches.

29. On 8 July 2019 the DPC Inquiry Team sent UL a Notice of Commencement of Inquiry (**"the Notice"**), which set out the scope and legal basis of the Inquiry.[8] The decision to commence the Inquiry was taken having regard to the circumstances of BN-18-12-2. The Notice said that the Inquiry would examine whether or not UL had discharged its obligations in connection with that breach and determine whether or not any provision(s) of the 2018 Act and/or the GDPR had been contravened by UL 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 related to the subject of the Inquiry. The Notice also sought certain documentation and posed a number of queries to UL to enable the DPC Inquiry Team to establish the relevant facts.

30. UL responded to the Notice on 23 July 2019.[9] UL's response included a significant volume of documentation and provided an overview of data protection compliance in the University. UL's replies outlined how its email service was operated using the Exchange 2010 platform. UL also made submissions on its overall IT infrastructure, security awareness training, and other matters. UL supplied copies of relevant policy documents giving details of relevant processing and procedures. The DPC has considered all of these for the purposes of this Decision.

31. The DPC sent further queries to UL on 24 October 2019,[10] to which UL replied on 20 November 2019[11] giving further details of its processes and procedures.

---

8 DPC to UL, Notice of Commencement of Inquiry, 8 July 2019.

9 UL Submission in response to Commencement Notice, 23 July 2019.

10 DPC to UL, request for further information, 24 October 2019.

11 UL to DPC, response providing further information, 20 November 2019.

32. By email on 21 January 2020,[12] the DPC informed UL that the scope of this Inquiry was to be extended to include BN-19-4-3, BN-19-4-348, BN-19-6-96, BN-19-8-135, and BN-20-1-282, as these had all occurred in circumstances similar to those of BN-18-12-2.

33. The DPC carried out an inspection at UL's premises on 6 February 2020. The purpose of this was to gain further understanding of the organisational and technical measure in place. The inspection was conducted by four authorised officers of the DPC and was attended by six representatives of UL. This inspection provided further clarification of UL's processes and procedures and provided further insight into the Breaches. It also allowed UL to give a detailed overview of its security and data protection protocols, of other technical and organisational measures in place at the time of the Breaches, and of its plans to update security measures.

34. On 14 February 2020, UL provided the DPC with a copy of the materials presented by UL during the inspection.[13] These included an overview of the organisational and technical measures that UL had prepared to facilitate implementation of the GDPR in May 2018. It also outlined UL's IT Security Strategy both before and since the GDPR took effects, as well as planned improvements and proposed changes to policies.[14]

35. On 10 March 2020,[15] the DPC Inquiry team sought further submissions in relation to the measures in place at the time of the Breaches. This was to clarify whether or not UL had acted in accordance with Article 5(1)(f) and 32(1) GDPR in relation to the processing being examined in the Inquiry. UL responded on 7 May 2020.

36. On 16 October 2020, the DPC Inquiry Team issued the Draft Inquiry Report to UL and invited submissions on it.[16] On 26 November 2020, following a short extension, UL made its submissions.[17] These included clarifications, submissions on confidentiality and commercial sensitivity, provided information on measures implemented since the personal data breaches occurred, and made submissions on the University's governance structure with regard to data protection. The DPC Inquiry Team had regard to these submissions in completing the Final Inquiry Report.

37. The Final Inquiry Report was issued to UL via email on 15 July 2025.

---

12 DPC to UL, letter extending scope of Inquiry, 21 January 2020.
13 UL Submission following inspection, 14 February 2020.
14 UL Submission following inspection, 14 February 2020.
15 DPC to UL, Request for further information, 10 March 2020.
16 Draft Inquiry Report, 16 October 2020.
17 UL Submissions on Draft Inquiry Report, 26 November 2020.

38. On 7 October 2025 the DPC provided UL a copy of the Draft Decision and invited UL to make submissions on it. UL responded with submissions on 7 November 2025. The DPC has carefully considered all of UL's submissions when preparing this Decision.

39. The DPC has considered the Final Inquiry Report and all relevant correspondence and submissions. Based on these, the DPC has reached conclusions that infringements of data protection legislation have occurred and that it is necessary to exercise certain corrective powers. Those infringements and corrective powers, and the DPC's reasons for reaching those conclusions, are set out in this Decision.

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

40. The scope of the Inquiry, which was set out in the Notice and the DPC's correspondence of 21 January 2020, was to examine whether or not UL had complied with its obligations in relation to the processing of the personal data of its users in connection with the subject matter of the notified personal data breaches, and whether or not any provision(s) of the 2018 Act and/or the GDPR had been contravened by UL in that context.

41. The temporal scope of this Decision ranges from the date of the application of the GDPR (25 May 2018) to 23 January 2020, the date on which UL completed its final review of the email account affected in BN-20-1-282, being the last data breach considered within the scope of this Inquiry.

F. Issues for Determination

42. Having reviewed the Inquiry Report and the other materials provided during the course of this Inquiry, the DPC considers that the issues in respect of which it must make a decision are:

- Whether UL has complied with its obligations under **Articles 5(1)(f)** and **32(1)** GDPR to implement appropriate technical and organisational measures to ensure appropriate security of the personal data processed on its email service;

- Whether UL complied with its obligations under **Article 30(1)** GDPR to maintain a record of processing activities;

- Whether UL has complied with its obligations under **Article 33(1)** GDPR to notify the DPC of the relevant personal data breaches without undue delay and, where feasible, not later than 72 hours after having become aware of them; and

- Whether UL has complied with its obligations under **Article 34(1)** GDPR to notify concerned data subjects without undue delay of personal data breaches assessed to pose a high risk.

G. Analysis of the Issues for Determination

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

43. 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.

44. Article 32(1) 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.

45. Articles 5(1)(f) and 32(1) 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 considers the appropriateness of the security measures implemented by UL 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 UL's email service at the time of the personal data breaches.

(i) Assessment of the Risks

46. 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 UL's processing of personal data via its email 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.

47. 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 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.

48. 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.

49. 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.

50. Therefore, in complying with the requirements of Article 5(1)(f) and 32 GDPR, controllers should start by identifying the risks to the rights of data subjects presented by the processing of personal data. Controllers must have regard to the likelihood and severity of those risks and must implement measures to effectively mitigate them.

51. 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 UL'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 25 May 2018, when the GDPR came into effect, UL 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.)

52. Regarding the scope of the processing, a large quantity of personal data is processed on UL's staff email system. During the temporal scope of this Inquiry, approximately 18,000 people worked and studied at UL.

53. The nature of the data processed on UL's staff email system was very broad. Similarly, it could be expected to include personal data of a range of degrees of sensitivity. In the breach notifications that relate to this Inquiry, UL listed categories of personal data made accessible to unauthorised persons including email addresses, phone numbers, CVs,

employment applications, staff discipline and mediation details (including legal correspondence), medical reports, personal injury claims, pension details, correspondence relating to Freedom of Information and data subject access requests, employee communications, passport details, PPSNs and bank account details. Some of these categories of personal data are particularly sensitive with regard to the fundamental rights and freedoms of data subjects, including special category personal data.

54. The Breaches involve personal data processed in UL's staff email system. This therefore includes not just emails sent and received by staff members, but also information stored in staff email accounts. The purpose of processing is to allow UL staff members to communicate appropriately with regards to academic and administrative matters.

55. The DPC considers that UL's processing of personal data in its staff email system presented a high risk in terms of both the likelihood and severity of unauthorised access or disclosure. The DPC makes this finding in light of the context and broad scope of the processing, the large number of email accounts, and the nature and quantity of personal data potentially stored on any given account. UL is a prominent academic institution with a significant profile both in Ireland and abroad. Staff email addresses are published on its website and elsewhere, and there are numerous user accounts to be maintained and supervised, each of which is a potential vector for attack. The probability element of risk is therefore clearly high. Regarding the potential consequences of unauthorised access or disclosure, as noted at paragraph 53 above, the nature of the processing was broad and affected, or potentially affected, large volumes of personal data, many categories of which are particularly sensitive. The consequences of any unauthorised disclosure of or access to the contents of the staff email system were therefore potentially grave.

56. Based on an assessment of these factors, the DPC considers that the severity of the risk to the rights and freedoms of natural persons arising from the processing of personal data was high. This takes into consideration the volume and types of personal data to which an unauthorised person might gain access, as well as the likelihood of such access being attempted. That high risk must be addressed by having appropriate measures in place, in order to maintain and further protect the rights and freedoms of data subjects.

(ii) Measures Implemented by UL to Address the Risks

57. 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 the controller to assess the risk to data subjects of the particular processing and to 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.

58. UL'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 staff email system.

(i) Technical measures

59. Article 32 GDPR requires controllers to 'implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk'.

60. UL provided information about the technical measures in place at the time of the Breaches. [18] UL's network was protected with a DNS firewall. The production firewall consisted of 2 x Fortinet Fortigate FG1500D in an active/ active cluster.[19] This blocked devices from connecting to specified malicious URLs such as known phishing sites. It also filtered for unwanted content such as malware and functions to help prevent unauthorised intrusion. UL stated that the operation of this firewall was monitored daily for malware and botnet reports in order to check for compromised systems.

61. A MailMarshal secure email gateway to filter both incoming and outgoing email traffic was in place. The MailMarshal was configured with standard and custom rules designed to block suspicious emails. UL provided the DPC with some examples of these rules. The standard rules implemented a 'whitelist/blacklist' configuration. The custom rules examples provided by UL employed text censors which scanned message content and blocked emails if the content contained references to subjects such as 'Banking' or if the email contained offensive language.

62. While UL did have a range of technical measures in place, as listed above, the DPC finds that these were not appropriate to the risk given the nature and type of processing being carried out. The DPC finds that there were several key deficiencies with regard to the security of personal data at the time of the Breaches and the DPC finds that these measures were not appropriate to the risk caused by the processing.

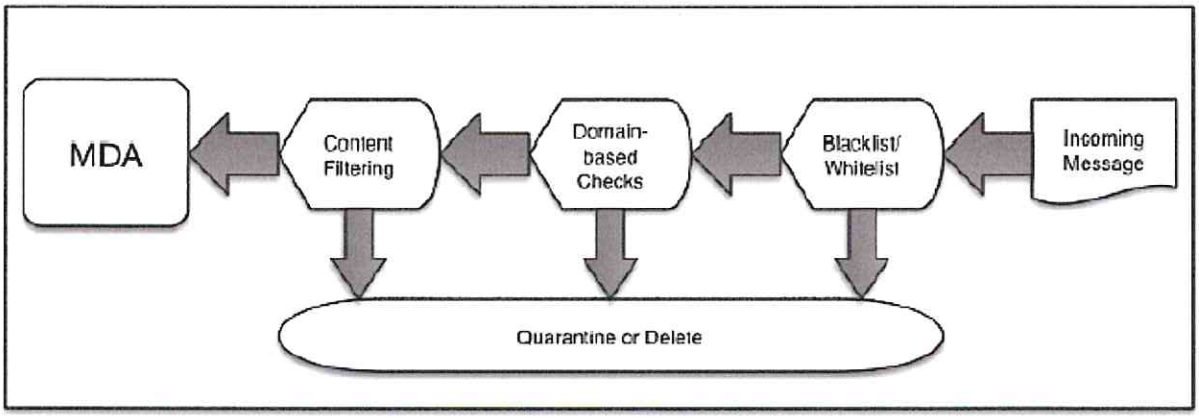
63. In terms of available technical measures regarding the security of email systems, the US-based National Institute of Standards and Technology (**'NIST'**) recommends a multi-layered approach to safeguarding organisations against unsolicited (and potentially malicious) email traffic.[20]

---

18 UL Submission in response to Commencement Notice, 23 July 2019, p.14.

19 Active/active clustering is a form of firewall configuration in which processing is shared between two or more firewall units.

20 NIST, 'Trustworthy Email', Special Publication (NIST SP) - 800-177 Rev. 1, p.89.Available at https://www.nist.gov/publications/trustworthy-email-0.



NIST, 'Trustworthy Email', p. 75

64. As illustrated in the diagram above, this approach comprises 3 lines of defence before an email is delivered to an end user. The first of these, whitelisting/blacklisting, involves maintaining a database of known malicious domains and allowing or rejecting emails on that basis.

65. Domain-based authentication employs three techniques which NIST consider to be standard counter-measures against spam and phishing threats. Sender Policy Framework (SPF) is an email authentication protocol that can be used to prevent spammers and attackers from sending messages that appear to come from a trusted domain. Using the SPF email protocol, an organisation can publish a list of authorised mail servers in an SPF record that appears in its DNS record. Receiving mail servers can perform an SPF test on every inbound email, checking to see if the IP address from which the email is sent matches an IP address in the domain's Sender Policy Framework record.[21]

66. While SPF can enhance an organisation's ability to block potentially malicious email traffic, use of it on its own has its limitations. For example, forwarded emails and 'spoofing' emails will evade SPF tests.

67. DomainKeys Identified Mail (DKIM) applies digital signatures to emails which can further enhance the ability to verify the legitimacy of incoming emails.

68. Domain-based Message Authentication, Reporting and Conformance (DMARC) augments the capabilities provided by SPF and DKIM. This feature specifies policy on how receiving email servers can verify the authenticity of incoming email. DMARC also enables receiving email servers to compare the domain in an email's message-From:

---

21 Mimecast, 'Sender Policy Framework', available at https://www.mimecast.com/content/sender-policy-framework/ (retrieved 10 September 2024).

address to the results of the SPF and DKIM processes. The DMARC policy can then dictate how the email is to be handled based on the result of the comparison.

69. Another method of email filtering is Content Filtering. This entails analysis of the content of an email by techniques such as word filtering and scanning for potentially malicious content such as URLs and malware. The final line of defence is educated end users. NIST recommends that organisations make staff aware of risks such as fraud and social engineering, which often use email as an attack vector.

70. As outlined in paragraph 61, UL had a MailMarshal secure email gateway that used rules to screen incoming and outgoing email traffic. A custom rule was implemented to block emails with HTML links. The information provided by UL on this rule indicates that the rule was triggered by a 'text censor'. A further rule – 'Block Spam-URL Censor' was triggered if a URL was on a 'blacklist', that is, a database of known spam senders.

71. Blacklisting is effective only if the sender is a known source of spam. The phishing email in BN-18-12-2 originated from an account impersonating the Box cloud service. That domain is known to have been used by spam operators.[22] Moreover, UL employed a text censor tool to flag emails containing HTML links. However, the description of the Breaches indicates that the malicious links were embedded in images rather than in the text content, and so were not recognised by the filter.

72. The DPC finds that, having regard to the risks of the processing, appropriate technical measures in the circumstances required UL to implement SPF, DKIM and DMARC, as set out above. In particular, these measures could have quarantined the emails before they were delivered to the end users. However, UL failed to implement these measures during the temporal scope of this inquiry. This is of particular relevance to BN-19-4-3 and BN-19-4-348, where the users were deceived into believing the malicious emails originated from trusted senders. While UL provided limited protection by implementing blacklisting and content filtering, it failed to implement the domain-based checks such as SPF, DKIM and DMARC outlined in paragraphs 65 – 69. Accordingly, the DPC finds that measures implemented by UL during the temporal scope of the Inquiry fell short of the multi-layered standards required in the circumstances.

73. UL also failed to implement multi-factor authentication ('**MFA**') for all users at the time of the breaches.[23] MFA was supported on the Exchange 2010 system used for the staff email service at the time of the Breaches, and was in fact implemented using the Cisco

---

22 SpamFighter.com, 'Spam Email Campaign Leverages "Box" Cloud Service Name, 28 June 2014, available at https://www.spamfighter.com/News-19053-Spam-Email-Campaign-Leverages-Box-Cloud-Service-Name.htm

23 UL Submission in response to Commencement Notice, 23 July 2019, p.3.

Duo system in July 2019 for users considered by UL to pose a 'high risk'.[24] (Users classified by UL as 'High-risk' users included senior managers, employees in Student Affairs (where a high volume of special category personal data is processed), the Academic Registry and UL's Data Protection Officer. At least one user whose login credentials were compromised by a breach the subject of this inquiry was included in this group, but other users generally were not so classified. [25])

74. During the Inquiry, UL informed the DPC that it planned to move its staff email system from the Exchange 2010 platform to Microsoft 365. This would significantly enhance the security of its email services, including by the availability of encryption, and would support MFA for all users. UL had noted the need to invest in encryption technology in its risk register in April 2018,[26] and included the need for MFA in its August 2019 risk registry entry, together with the requirement to migrate all staff to Microsoft 365.[27] UL confirmed that migration to Microsoft 365 and implementation of MFA was completed for staff in July 2020 and for students in April 2021.[28]

75. The DPC finds that an appropriate level of security in the circumstances included MFA. Accordingly, UL's failure to implement MFA at the time of the Breaches meant that it fell short of the standards required in the circumstances.

76. UL was obliged to implement technical measures that, in the context of the processing environment in question, provided appropriate confidentiality, integrity, availability and resilience of processing systems and services that reflect the risks posed. While UL had technical security measures in place at the time of the Breaches, the absence of domain-level authentication techniques, the failure to implement MFA for all users, and continued use of Exchange 2010 even after a more secure platform had been identified, means that the level of technical security measures implemented by UL during the temporal scope of the inquiry was not appropriate to the risk caused by the processing of personal data on its staff email system. Therefore, the DPC considers that technical security measures in place at the time of the Breaches did not meet the standards required by Article 5(1)(f) or Article 32(1) GDPR.

---

24 UL Submission in response to Commencement Notice, 23 July 2019, p.2 and UL to DPC, response providing further information, 20 November 2019, p.6.

25 UL Submission on Draft Decision, 7 November 2025, p. 38.

26 UL to DPC, response providing further information, 20 November 2019, p.48

27 UL to DPC, response providing further information, 20 November 2019, p.48.

28 UL Submission on Draft Decision, 7 November 2025, p. 5.

(ii) Organisational measures

1. Training and Awareness

77. UL stated that IT security training had been made available to all staff since September 2018.[29] However, this training was not mandatory for all staff during the temporal scope of the Inquiry. Training is a fundamental process which raises awareness and should be provided to staff to ensure that are aware of the implications of and risks to the rights and freedoms of data subjects. The DPC has previously published guidance which states

> No matter what technical or physical controls are placed on a system, the most important security measure is to ensure that staff are aware of their responsibilities.... Effective employee training about the risks of data compromise, their role in preventing it and how to respond in the event of problems can be a very effective line of defence. Many organisations set security policies and procedures but fail to implement them consistently. Running scenario based training sessions may assist in effective training.[30]

78. UL were required to ensure that all staff had the appropriate level of awareness and training to ensure that the data processed in its email system had state of the art protection. The DPC accepts that some degree of human error is unavoidable. However, an appropriate level of training to mitigate the risk caused by the processing is crucial to reduce the risk of human error. Training and awareness are essential to mitigate against personal data breaches caused by human error. All of the Breaches concerned staff email accounts. Personal data breaches concerning staff accounts may pose a higher risk to the rights and freedoms of data subjects in circumstances where some of those accounts may routinely contain payment card details, disciplinary cases concerning staff, passport and birth certificate details, and PPS numbers.

79. In its submission of 23 July 2019,[31] UL stated that it had implemented an extensive cyber-security training module and provided an excerpt of training logs for a number of staff members. [32] This log detailed the first iteration of UL's online IT Security Awareness Training, which went live in September 2018 and showed the training schedule for 13 users and 26 training modules. Of these 26 modules, only 14 had been completed by the 13 users, and some users had not completed any training whatsoever. At the time of

---

29 UL Submission in response to Commencement Notice, 23 July 2019, p.2.

30 DPC, 'Data Protection Security Guidance', February 2020, available at https://www.dataprotection.ie/en/organisations/know-your-obligations/data-security-guidance

31 UL Submission in response to Commencement Notice, 23 July 2019, p.12.

32 UL to DPC, response providing further information, 20 November 2019, p.156.

providing this record to the DPC, there were 12 modules yet to be completed, and 5 of the users had no record of completing any training modules.[33]

80. UL subsequently submitted a full training schedule which outlined training modules available to staff and detailed which unit or area receives the training.[34] The table below describes each training and awareness campaign, the target audience and the dates when the training was provided.

IT Security Awareness Training	Target audience	Dates
Online IT Security Training	All Staff	Ongoing (Drive in June & Oct 2019)
Departmental Face to Face	Graduate Entry Medical School	Feb-19
Face to Face	Executive Committee	Aug-19
Induction Leaflet	All New Staff	Six Times a Year
General IT Training including IT Security	All New Staff	28-Mar-19
Policies Summary	Union, Audit & Risk Committee	19-Sep-19
Technical GDPR Training	IT Department	08-Oct-17
Twitter & Instagram	UL Community	Ongoing
Email Notification	All Staff	Ongoing
Posters	UL Campus	Ongoing (Summer 2019)
Desk Top Popups	All Staff	Daily

81. In the same document, UL stated that any staff member who had fallen victim to a phishing incident was considered to be a 'High Risk User' and was required to undertake or retake Data Protection Training. Training was also provided to all IT Department staff on a mandatory basis.

82. UL submitted that in September 2018 it had 'rolled out and commenced both online and in-person data protection training in advance of the Governing Authority formally approving the Data Protection Policy.' [35]

83. UL also had training in place to educate staff on the dangers of phishing, and implemented alert pop-ups that would make users aware of phishing activity and inform them of how to avoid such attacks. These alerts were set to appear for users approximately twice a day and could be closed only by clicking a button on them.

---

33 UL Submission in response to Commencement Notice, 23 July 2019, p.24.

34 UL to DPC, response providing further information, 20 November 2019, Table 9.

35 UL Submissions on the Draft Inquiry Report, 26 November 2020, p.8, at point 37.

84. Having regard to the risk caused by the processing, the DPC finds that an appropriate level of security for the processing required mandatory cyber security training for all staff during the temporal scope of the Inquiry. As set out above, UL failed to implement such training during the temporal scope of the Inquiry. The DPC therefore finds that UL's failure to implement a robust cyber security training regime that was mandatory for all UL staff prior to the personal data breaches infringed Articles 5(1)(f) and 32(1).

2. *Other organisational measures*

85. UL established a GDPR project before the GDPR took effect in May 2018 to ensure that its legislative obligations would be met.[36] This project also prepared and reviewed policies that would allow UL to function appropriately while complying with the GDPR.

86. UL had a number of relevant policies which were in effect at the time of the Breaches. Some of these were in place before the occurrence of the first breach (BN-18-12-2) in November 2018. The Data Protection Policy[37] was a key policy, which outlined UL's commitment to protect the privacy rights of individuals in accordance with the applicable legislation. This policy was in existence in draft form at the time of the first breach, but was not formally approved until December 2018. The policy in effect before that was dated 26 June 2015, predating the introduction of the GDPR.[38] However, UL presented no evidence during the course of this Inquiry to show that it had taken necessary steps to implement some aspects of the newer policy – such as online and in-person training – prior to the occurrence of the first breach in November 2018.

87. Another key policy submitted by UL was its Records Management & Retention Policy.[39] This outlined how UL stores and manages personal data and other information. It also detailed for how long data should be retained and how it should be archived or disposed of. This policy was first implemented in January 2015.

88. The Records Management & Retention Policy was updated in December 2018, after the first breach (BN-18-12-2) occurred. The revised policy stated that emails should be retained for the 'current year or until they cease to be of administrative use'. Notwithstanding that revision, the policy did not specify appropriate methods of filing, or archiving of emails or attachments, or provide for means by which compliance would be monitored and assessed. [40]

---

36 UL Submission in response to Commencement Notice, 23 July 2019, p.1.
37 UL Submission in response to Commencement Notice, 23 July 2019, p.43.
38 UL to DPC, response providing further information, 20 November 2019, p.66.
39 UL Submission in response to Commencement Notice, 23 July 2019, p.52.
40 UL Submission in response to Commencement Notice, 23 July 2019, p.56.

89. Other policy documentation was provided to the DPC during the course of this inquiry. All policies and formal approval dates are set out in the table below. The DPC notes that six of these were first implemented, and one was revised, shortly after the Inquiry commenced on 8 July 2019.

Policy Documentation	Date Approved
Data Protection Policy	26-Jun-15
Data Protection Compliance Regulation	26-Jun-15
Data Protection Policy	Dec-18
Records Management and Retention Policy	25 January 2013, Revised 18 July 2019
Code of Conduct for Employees	27-Sep-11
Risk Management Policy	Feb-16
IT Security Policy	22-Jul-19
Personal Device Policy	22-Jul-19
Password Policy	22-Jul-19
Email Policy	22-Jul-19
Data Encryption Policy	22-Jul-19
Acceptable Usage Policy	22-Jul-19

90. Following the first breach (BN-18-12-2) in November 2018, UL set up a Security Incident Response Team. This team was responsible for the initial containment of a breach and investigated the extent of each breach. [41]

91. UL maintained a risk register which detailed identified risks and proposed solutions or means of mitigating those risks.

92. UL indicated that, at the time of the first breach in November 2018, it had no controls in place to prevent users of the staff email system from automatically forwarding emails to external email addresses. Similarly, users could create rules that would cause received emails that matched defined criteria (e.g. containing specific phrases or originating from specified domains) to be automatically filed into a designated folder. This was a feature exploited by hackers in the Breaches. UL did not prohibit or discourage the use of such features on the staff email system.

93. The DPC finds that, having regard to the risk caused by UL's processing, appropriate organisational measures included controls with regard to email forwarding, a properly implemented data storage policy for employees, and policies relating to phishing or security incidents. While, as outlined above, UL had some organisational security

---

41 UL Submission following inspection 14 February 2020, p.11.

measures in place at the time of breach, its failure at the time of the initial breach to implement these measures meant that adequate organisational measures were not in place to ensure the ongoing security of personal data processed by UL. Therefore, the DPC finds that the organisational measures in place at the time of the initial breach did not meet the standards required by Article 5(1)(f) or Article 32(1) GDPR.

94. In its submission on the Draft Decision, UL accepted the DPC's provisional finding of infringements of Articles 5(1)(f) and 32(1) GDPR:

> The University of Limerick accepts the DPC's provisional findings in respect of Articles 5(1)(f) and 32(1) GDPR. We acknowledge that, at the time of the breaches (November 2018 to January 2020), the technical and organisational measures in place to secure our staff email system were not sufficient to mitigate the risks posed by increasingly sophisticated phishing attacks.[42]

95. UL submitted that the shortcomings admitted to should be understood in the context of several matters enumerated in its submission, and on improvements in UL's technical and organisational measures undertaken since the Breaches occurred. Those factors and improvements are considered separately in sections I and K of this Decision.

b) Issue 2: Article 30(1) GDPR

96. Article 30(1) GDPR requires controllers to maintain a record of processing activities, containing the following information:

> (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
>
> (b) the purposes of the processing;
>
> (c) a description of the categories of data subjects and of the categories of personal data;
>
> (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

---

42 UL Submission on Draft Decision, 7 November 2025, p. 4.

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

97. In correspondence on 19 November 2019[43] and 5 February 2020[44] UL provided its Record of Processing Activity ('**ROPA**'). This detailed categories of data that UL processed and the reasons why that data was retained. It also detailed the sources of data and the form in which it was maintained. The DPC noted however that UL's ROPA did not include all required information regarding the description of categories of data subjects and categories of personal data which was processed, and the technical and organisational measures in place, as required by Article 30(1) GDPR.[45] For example, the ROPA did not take account of the processing of personal data on UL email accounts, including those affected by the Breaches.[46] Further, it did not contain a description of UL's organisational and technical measures in place to protect the data that UL processed. (The DPC notes however that that information was included in UL's revised ROPA issued in May 2020.)

98. UL revised its ROPA and implemented that revised version on a pilot basis to two departments in January 2020 and on a University-wide basis across all departments in May 2020. UL informed the DPC on 26 November 2020 that, although some required information was not included in the ROPA, that information was documented elsewhere in UL's policies and procedures, which were implemented during the temporal scope of this Inquiry.[47] However, the DPC finds that UL's policies and procedures also did not adequately describe the processing of personal data on UL email accounts, and did not adequately describe UL's organisational and technical measures in place to protect the data that UL processed.

---

43 UL to DPC, response to queries, 19 November 2019, p.15.

44 UL to DPC, email containing Record of Processing Activity, 5 February 2020.

45 Final Inquiry Report, paragraph 138.

46 Final Inquiry Report, paragraph 138, p. 40.

47 UL Submission on Draft Inquiry Report, 26 November 2020, p. 7.

99. Therefore, the DPC finds that UL infringed Article 30 GDPR from 25 May 2018 to May 2020 by failing to maintain a ROPA that contained a description of UL's organisational and technical measures in place to protect the data that UL processed, and that adequately described the processing of personal data on UL email accounts, including those affected by the Breaches.[48]

100. In its submission on the Draft Decision, UL accepted 'that its initial ROPA, developed in 2018, did not fully meet the requirements of Article 30(1)'.[49] UL submitted that this reflected a number of mitigating factors, which are considered in sections I and K of this Decision.

c) Issue 3: Article 33(1) GDPR

101. As set out in paragraph 11 above, each of the Breaches constitutes a personal data breach as defined in Article 4(12) GDPR.

102. 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.

103. The obligation to notify the DPC applies to all personal data breaches unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. In each of the Breaches examined for this Inquiry, UL correctly recognised that such a risk had been posed.

104. Article 33(1) requires notifications to be made 'without undue delay.' This must be assessed by reference to when UL 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

---

48 Final Inquiry Report, paragraph 138, p. 40.

49 UL Submission on Draft Decision, 7 November 2025, p. 11.

notification to individuals is to provide specific information about steps they should take to protect themselves.

105. 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>[50]

106. 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.

107. Recital 87 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 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.

---

[50] Emphasis added.

108. 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.[51]

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

(i) The Breach Notifications

110. In all cases, UL notified the DPC of the relevant breaches. However, the notifications for BN-18-12-2, BN-19-6-96 and BN-19-8-135 occurred more than 72 hours after UL became aware of those breaches and thus, fall to be considered in the context of UL's obligation under Article 33(1) GDPR to notify the DPC without undue delay and, where feasible, within 72 hours.

111. **BN-18-12-2** concerned unauthorised access to an email account, which UL assessed as posing a high risk. UL stated that it became aware of the breach on 20 November 2018 but did not notify the DPC until 30 November 2018. By way of explanation, UL stated that the breach was reported to its Data Protection Officer on 28 November 2018 who, in turn, notified the DPC within 72 hours.

112. The DPC finds that UL failed to notify the DPC of this personal data breach without undue delay. Article 33(1) imposes the obligation to notify breaches on the controller – in this case, UL itself. An internal delay in notifying the data protection officer of a personal data breach does not excuse a resulting undue delay on the part of the controller in notifying the relevant supervisory authority. Similarly, the obligation is to notify the controller's supervisory authority – in this case, the DPC – not the controller's data protection officer.

---

51 EDPB Breach Notification Guidelines, p.6.

UL could and should have notified the DPC of this breach within 72 hours of discovering it on 20 November 2018. The DPC therefore finds that an undue delay occurred in notifying the DPC of this breach.

113. **BN-19-6-96** concerned unauthorised access to a UL staff email account following a phishing attack on 1 June 2019. The user in question had forwarding rules added to their email account. The breach notification in this case stated that the breach, which UL assessed to pose a medium risk, had come to UL's attention on 1 June 2019. However, the breach was not notified until 6 June 2019.

114. **BN-19-8-135** was notified on 8 August 2019. This breach involved a phishing email received by 1,430 UL staff members, which sought to acquire UL email login credentials through a fake UL webmail login page. Subsequent investigations revealed that one staff member's credentials were compromised, giving unauthorised access to that person's personal data, as well as that of third parties accessible through the mailbox. UL became aware of the attack and the risk of compromised credentials on 2 August 2019, but did not notify the DPC until 8 August 2019.

115. In submissions during the inquiry and in response to the Draft Decision, UL maintained that both BN-19-9-96 and BN-19-8-135 had been reported to the DPC without undue delay and within 72 hours of UL becoming aware of them, and therefore that no infringement of Article 33(1) had occurred in those cases. UL pointed out that both of these breaches were initially detected over bank holiday weekends by 'a contracted service provider [who] identified suspicious activity...and reset the relevant employee's password and disabled the mailbox.' The incidents were investigated by UL's IT Department ('ITD') on the following Tuesday. 'Once they established that a breach had taken place, ITD notified [the office of UL's data protection officer.] The DPO then notified the DPC without undue delay and within 72 hours.'[52]

116. UL cited in support of its position the EDPB's 'Guidelines 9/2022 on personal data breach notifications under GDPR':

> After first being informed of a potential breach by an individual, a media organisation, or another source, or when it has itself detected a security incident, 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'.[53]

---

52 UL Submission on Draft Decision, 7 November 2025, p. 13.

53 EDPB, 28 March 2023, Guidelines 9/2022 on personal data breach notifications under GDPR,

117. The DPC notes that this refers to cases where a controller is aware only that 'a security incident' has or may have occurred, but needs time to determine whether the incident comprises the components of a 'personal data breach' as defined in Article 4(12) GDPR and, if it does, whether it is likely to pose a risk to rights and freedoms of natural persons. For the reasons given below, the DPC does not accept that this is the case in either BN-19-9-6 or BN-19-8 135.

118. The DPC accepts that controllers must investigate breaches thoroughly upon becoming aware of them, and that weekends and holidays may limit the ability to establish all relevant facts. However, the obligation to notify arises once the controller is aware, or should be aware, that a breach exists and is likely to pose a risk to the rights and freedoms of natural persons. Article 33(4) GDPR accommodates investigations by allowing controllers to submit missing information as it becomes available after the notification. In these cases, the existence of a breach and the risks they posed was known – or should have been known – to UL from the start.

119. In correspondence on 26 November 2020, UL stated that the delay in notifying BN-19-9-6 was due to the fact that the breach occurred during a bank holiday weekend.[54] That is not a valid explanation, as the breach was known to pose a risk – and so to be notifiable – from the time of its discovery, and the period of 72 hours provided for in Article 33(1) GDPR does not include any exception for Sundays, Saturdays or public holidays.[55]

120. In the case of BN-19-8-135, UL pointed out that the breach was identified on Friday 2 August 2019 and brought to the attention of UL's DPO on Tuesday 6 August.

> Once the DPO became aware, it assessed the breach to determine the likely risks arising to the impacted data subjects and, having determined that a risk was likely to arise, notified the DPC of the incident on 8 August 2019, within the 72-hour timeframe and, therefore, in accordance with Article 33(1) of the GDPR.[56]

121. The DPC considers that a phishing email specifically designed to compromise UL email logins that was able to circumvent UL's security measures and be received by 1,430 staff members gave ample indication of a personal data breach, and of a risk to the rights and freedoms of persons. This breach was therefore notifiable within no more than 72 hours of its nature becoming known on 2 August 2019. Regarding the time taken to investigate, and for UL's data protection officer to 'determine the likely risks', the DPC rejects UL's explanation for the same reasons set out above, because an internal delay in notifying

---

54 UL Submissions on the Draft Inquiry Report, 26 November 2020, p.5, under section BN 19-6-96.

55 Regulation (EEC/Euratom) 1182/71, Article 3(2) and (3).

56 UL Submissions on the Draft Inquiry Report, 26 November 2020, p.5, under section BN 19-8-135.

the data protection officer does not excuse a resulting undue delay on the part of the controller in notifying its supervisory authority.

122. For these reasons, the DPC does not accept UL's submission that these breaches were notified within the period specified in Article 33(1) GDPR. In both cases, it was established at an early stage that the registered user's email account had been compromised, allowing unauthorised persons access to emails in Inboxes, and potentially to contacts identifiable from within those accounts. In the case of BN-19-9-6, the attacker was able to create forwarding rules for emails received. The components of the definition of 'personal data breach' in Article 4(12) GDPR were therefore readily apparent at an early stage, as was the risk posed by the breaches. The DPC therefore finds that UL infringed Article 33(1) GDPR in relation to BN-19-96 and BN-19-8-135 by failing to notify those breaches without undue delay and within 72 hours of becoming aware of them.

d) Issue 4: Article 34 GDPR

123. Article 34(1) GDPR provides:

> When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay

124. Recital 86 GDPR explains that the purpose of requiring controllers to communicate data breaches to data subjects assessed to be at high risk is 'to allow [the data subject] to take the necessary precautions.' Data subjects are often better placed than the controller to take precautionary steps such as notifying their bank or medical practice, scrutinising emails purporting to be from contacts with extra care, or changing passwords on other sites that they use. Time is of the essence in doing this, which is why Article 34(1) GDPR requires controllers to communicate the breach to data subjects at high risk 'without undue delay'. The requirement is a logical immediate consequence of the controller's assessment that the risk posed by a breach is high. It is not a measure to be deferred pending detailed examination of the causes and effects of a breach.

125. In three of the six data breach notifications that fall within the scope of this inquiry, UL informed the DPC that data subjects would be informed of the breach pursuant to Article 34(1) GDPR. These breaches were BN-18-12-2, BN-19-4-3 and BN-19-4-348.

126. In **BN-18-12-2**, UL assessed the risk posed by the breach to be high and acted promptly to communicate the breach to 261 individuals, 115 GP practices and 3 companies, based on information identifying them (or persons working in them) being accessible in the

email account accessed by hackers.[57] All notifications were completed by 11 February 2019, less than 2 months after the breach was discovered on 19 November 2018. The DPC finds that UL assessed the risk correctly and fulfilled its responsibilities under Article 34(1) GDPR in this case.

127. In **BN-19-4-3**, UL assessed the risk posed by the breach to be high when it notified the DPC on 27 March 2019. However, it did not notify data subjects until 5/6 September 2019, after a detailed review by an external specialist which identified 76 persons considered to be at high risk. The interval of nearly six months between UL's assessment of a high risk breach and the eventual notification of the affected data subjects did not give data subjects the information they needed, or allow them to act promptly, to protect their rights and freedoms. While thorough investigation of data breaches is essential, it should not be at the expense of data subjects' ability to take necessary precautions.

128. UL could and should have taken steps to notify affected data subjects as soon as it assessed that the breach placed them at high risk. Even if the early stage of investigations prevented a precise understanding of the cause and effects of the breach, UL could and should have been able to give a general notification of potential harms, and so enable data subjects to begin taking necessary precautions. The DPC therefore finds that UL contravened Article 34(1) GDPR by not communicating this breach to data subjects without undue delay.

129. In **BN-19-4-348**, UL's breach notification on 16 April 2019 rated the risk as high. UL commissioned an external security company to investigate the contents of an email account used by a staff member whose login credentials had been compromised as a result of a phishing attack. UL informed the DPC on 25 July 2019 that the review had established that the personal data in the email account (both of the user and of third parties) related to a total of 24 persons but did not include special category personal data or other sensitive information such as bank details. Based on this, UL revised its initial risk assessment to medium and did not communicate the breach to data subjects.

130. In its submission on 26 November 2020, UL explained that its initial rating of the risk as high had been done 'provisionally' and 'to err on the side of caution in terms of having to notify data subjects.'[58] The DPC notes that, while UL's breach notification on 16 April 2019 made clear that the circumstances of the breach and the categories of personal data affected were still under investigation, it did not mention either of these qualifications to its risk rating. UL maintained that its choice not to communicate the

---

57 UL email to DPC, 11 February 2019, Annex 1. Among those contacted, 115 were GP practices where data in the compromised email accounts identified a total of 127 individual persons.

58 UL Submissions on the Draft Inquiry Report, 26 November 2020, p.6.

breach to data subjects was justified by the security company's finding that no special category or sensitive personal data was made accessible by the breach.[59]

131. The DPC does not accept that a controller can retroactively justify a decision not to follow the clearly stated requirements of Article 34(1) GDPR by revising the risk rating more than three months later. In circumstances where UL assessed the risk to be high, the obligation to communicate the personal data breach was triggered, and UL was obliged to make that communication without undue delay. UL ought to have communicated the breach to data subjects before the reduced risk assessment on 25 July 2019, and its failure to do so constituted an undue delay. As stated above, the purpose of Article 34(1) is to enable data subjects to take appropriate precautions when the controller has assessed that a breach has placed their rights and freedoms at high risk. Risk is contingent in nature: it looks to what might happen in the future, rather than looking back to what resulted. Controllers must therefore approach that assessment with particular care and in full awareness of the consequences that flow from it. To allow a retroactive review to cancel out the responsibility to communicate a breach to data subjects assessed to be at high risk without undue delay would render initial risk assessments of breaches, and the protections afforded by Article 34(1), which are fundamentally directed towards contingent risk, essentially nugatory.

132. The DPC accepts that UL's initial assessment of a high risk was made in good faith and in circumstances where it was not yet fully aware of the types of personal data made accessible by the breach. However, the GDPR's overarching purpose is the protection of fundamental rights and freedoms of natural persons, particularly the protection of their personal data.[60] On discovering the breach, UL, as controller, determined that the facts immediately available to it indicated a high risk to data subjects and it was obliged to act without undue delay.

133. UL wished to err on the side of caution in terms of notifying data subjects, but should have favoured the interests of those data subjects, and enabled them to act to protect their rights and freedoms. Taking into account the circumstances of the breach, particularly in relation to the relatively small number of potentially exposed data subjects, the DPC is of the view that UL should have informed the data subjects sooner and without disproportionate effort. The DPC therefore finds that UL infringed Article 34(1) in this case by not communicating the breach without undue delay to data subjects assessed to be at high risk.

---

[59] UL Submissions on the Draft Inquiry Report, 26 November 2020, p.6.

134. In its submission on the Draft Decision, UL acknowledged that it had not met the requirements of Article 34(1):

> UL accepts the DPC's provisional findings in respect of Article 34(1) GDPR. We acknowledge that the communication of the two breaches to affected data subjects was either delayed (BN-19-43) or not carried out (BN-19-4-348), and that this fell short of the standard required under the GDPR.

135. UL submitted that this must be understood in the light of several factors, which are examined in sections I and K of this Decision.

H. Findings Regarding Articles 5(1)(f) and 32(1), 30(1), 33(1) and 34(1)

136. For the reasons set out above in Section F, the DPC finds that UL

- infringed Articles 5(1)(f) and 32(1) GDPR by failing to ensure appropriate security of the personal data related to its email accounts, and 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.

- infringed Article 30(1) GDPR by failing to document a general description of organisational and technical measures within a designated Record of Processing Activity, during the period from 25 May 2018 to May 2020.

- infringed Article 33(1) GDPR by its failure to notify the DPC without undue delay after becoming aware of breaches BN-18-12-2, BN-19-6-96 and BN-19-8-135.

- infringed Article 34(1) by failing without undue delay to notify 24 data subjects affected by breach BN-19-4-348, and 76 data subjects affected by breach BN-19-4-3, of those breaches, which UL had assessed to pose a high risk to the rights and freedoms of natural persons.

I. Decision on Corrective Powers

137. The DPC has set out above, pursuant to section 111(1)(a) of the 2018 Act, its decision to the effect that UL has infringed Articles 5(1)(f) and 32(1) GDPR, Article 30(1) GDPR, Article 33(1) GDPR and Article 34(1) GDPR.

138. Section 111(2) of the 2018 Act provides that, 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 one or more 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.

139. 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...

140. 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. A reprimand to UL pursuant to Article 58(2)(b) GDPR in respect of its infringements of Articles 5(1)(f) and 32(1) GDPR, Article 30(1) GDPR, Article 33(1) GDPR and Article 34(1) GDPR; and

b. Administrative fines for the infringements of Articles 5(1)(f) and 32(1) GDPR, Article 30(1) GDPR, Article 33(1) GDPR and Article 34(1) GDPR.

141. The DPC notes that, since the breaches, UL has taken very significant steps to remediate the deficiencies in its processing of personal data identified in this inquiry. These measures include the following:

- Improved email security and management to reduce phishing risks and improve management of incidents that occur,
- Enhanced identity and access management measures including encryption of devices, use of MFA for all staff, student and guest email accounts, improved management of email accounts of persons leaving the organisation, and enhanced MFA and geographical restrictions for privileged accounts,
- Use of cloud solutions for email and file storage, to improve management and control of email and file storage,
- Improved network management and security measures, including new firewall clusters, enhanced segmentation and use of MFA for network access by both staff and students,

- Improved anti-malware software, policies and procedures;
- Improved backup and recovery technology and procedures,
- Establishment of a dedicated Security Incident Response Team,
- Mandatory training for staff on IT security, phishing awareness, breach response and secure data handling,
- Review and revision of policies covering subjects including data protection, IT security, acceptable usage, email management passwords, encryption and records management,
- Integration of data protection risks in UL's enterprise risk framework,
- Revised governance structures to ensure that data protection and IT security issues are recognised and overseen at appropriate levels in UL's administration.
- Enforcement of the requirement to perform data protection impact assessments where high-risk processing is proposed.

142. Based on the details of those improvements provided by UL in its submissions, the DPC has decided that it is not necessary or proportionate for it to issue an order for UL to bring its current processing into compliance with the GDPR. The DPC's acknowledgement of those improvements does not however relieve UL 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.

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

J. Reprimand

144. 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

145. The DPC issues to UL a reprimand in respect of its infringements of Articles 5(1)(f) and 32(1), Article 30(1), Article 33(1) GDPR and Article 34(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 formally recognise the serious nature of the infringements and to dissuade such non-compliance. The reprimand will contribute to ensuring that UL 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. Administrative fine

146. 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

147. The purpose of administrative fines is to strengthen the enforcement of the rules of the GDPR.[61] Fines sanction non-compliance and seek to re-establish compliance with the GDPR.

148. 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'),[62] and the Article 29 Working Party's Guidelines on the application and setting of administrative fines ('the A29WP Fining Guidelines'),[63] which have been endorsed by the EDPB.

149. 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 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)

---

61 GDPR, Recital 148.

62 EDPB, 'Guidelines 04/2022 on the calculation of administrative fines under the GDPR', version 2.1, adopted on 24 May 2023.

63 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.

that apply in this case. In particular, Article 83(1) GDPR requires fines to be effective, proportionate and dissuasive. These principles will inform the calculation of any fine that is imposed in this Decision.

a) Whether to impose an administrative fine

150. 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...

151. 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;

152. Article 83(2)(a) requires consideration of the identified criteria 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 as meaning all of the processing operations that UL carries out on personal data regarding the delivery of UL's email systems.

153. Considering next the meaning of 'infringement', it is clear from Articles 83(3)-(5), that 'infringement' means an infringement of a provision of the GDPR. Above, UL was found to have infringed Articles 5(1)(f) and 32(1), Article 30(1), Article 33(1) and Article 34(1) GDPR. Thus, **'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) as meaning the infringements of those Articles. While each is an individual 'infringement' of the relevant provision, they all concern 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, unless otherwise indicated, assess all of these infringements simultaneously by reference to the collective term **'infringements'**.

154. 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

155. 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.

156. 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.'[64]

157. 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.[65]

158. The nature of the processing relating to the infringements identified herein is UL's processing of personal data via its email systems.

159. 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.[66]

160. 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.

---

64 EDPB Fining Guidelines, paragraph 53.b.i.
65 EDPB Fining Guidelines, paragraph 53.b.i.
66 EDPB Fining Guidelines, paragraph 53.b.ii.

The data processed included data subject identity, PPSN, contact details, economic or financial data and health data.

161. 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).[67]

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

163. 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.[68]

164. Five hundred and twenty one data subjects were identified as being potentially affected by the access to the compromised accounts:

Breach	No. of Email Recipients	No. of Disclosed Credentials	No. of Data Subjects who had Personal Data Present

[67] EDPB Fining Guidelines, paragraph 53.b.iii.

[68] EDPB Fining Guidelines, paragraph 53.b.iv.

BN-18-12-2	1	1	379
BN-19-4-3	1	1	76
BN-19-4-348	369	1	24
BN-19-6-96	360	1	22
BN-19-8-135	1430	3	20
BN-20-1-282	723	2	0
Total	**2884**	**9**	**521**

165. 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.[69]

166. The Breaches resulted in 521 data subjects being identified as potentially affected by the access to the compromised accounts. 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, and to the difficulties and inconvenience caused by having to take protective steps in consequence of the Breaches. The personal data affected by the Breaches was likely to have included data subject identity, PPSN, contact details, economic or financial data, and health 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.[70]

167. The infringement of Article 30(1) identified in this Decision arises from UL's failure to ensure that full details of its processing and of its measures to protect personal data were

---

69 EDPB Fining Guidelines, paragraph 53.b.v.

70 Recital 75 GDPR.

recorded in a way that allowed prompt demonstration of compliance with the data protection law. The ROPA did not take due account of UL's processing of personal data on its email systems. While – as is made clear by Recital 82 – the primary purpose of the record of processing activity under Article 30 GDPR is to demonstrate compliance, the process of creating and maintaining it assists controllers in monitoring and assessing risk in their processing operations. UL's failure to maintain a full record of its processing activities is therefore likely to have contributed at least in part to the failures of security identified in relation to Articles 5(1)(f) and 32(1) GDPR, and the damage resulting from them as analysed in paragraph 166 above.

168. Regarding the infringements of Article 33(1) GDPR identified, Recital 87 makes clear that an important purpose of that Article is to enable the supervisory authority to intervene in accordance with its tasks and powers. This can include its powers to act to prevent further risks or harms to natural persons arising from a breach. Any undue delay in notifying a breach can therefore extend the duration or increase the level of the risks posed to affected data subjects. In BN-18-12-2, UL assessed the risk posed by the breach to be high and was aware that a large amount of personal data was exposed by the breach. However, UL did not notify the DPC of the breach until 10 days after it became aware of it. In BN-19-6-96 and BN-19-8-135 the notifications were not made until 5 and 6 days respectively after UL became aware of them. The consequence of these failures was that the affected data subjects were effectively deprived of a legislatively mandated additional layer of protection in the context of a personal data breach, whereby a supervisory authority can consider using its powers to protect the rights and freedoms of data subjects.

169. In relation to the infringement of Article 34(1) GDPR identified, the DPC considers that the delay in communicating the breach (or, in the case of BN-19-4-348, the failure to do so) created additional and unnecessary risk for the affected data subjects by depriving them of the opportunity to act promptly to assess for themselves risks that UL had determined to be high, and to take such steps as they might have thought appropriate to protect their rights and freedoms. The DPC notes however that UL's forensic review of the data affected by BN-19-4-348 established that the risk posed was, with the benefit of hindsight, medium rather than high, and that no special category or otherwise sensitive personal data was affected.

The nature of the infringements

170. 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:

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.[71]

171. In line with the text of the GDPR, 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.[72]

172. The nature of the infringements identified regarding Articles 5(1)(f) and 32(1) GDPR comprises a failure of UL to fulfil 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 damage to them that personal data breaches can cause, including unavailability or destruction of essential personal data, or unauthorised access, alteration or disclosure of it. Therefore, compliance with Articles 5(1)(f) and 32(1) is central to the protection of the rights and freedoms of natural persons under the GDPR.

173. The nature of UL's infringement of Article 30(1) identified herein comprises its failure to fully document a general description of the technical and organisational security measures referred to in Article 32(1). The objective of Article 30(1) is to enable controllers to demonstrate their compliance with their obligations and responsibilities under the GDPR.[73] A clear record of how, when and why processing takes place will also help ensure that data subjects who exercise their transparency rights can access relevant information regarding the controller's processing activities. It can also help controllers and supervisory authorities to identify gaps or deficiencies in technical and organisational measures to secure processing and ensure compliance with other data protection requirements.

174. The nature of the infringements of Article 33(1) identified herein comprises a failure by UL to notify the DPC of personal data breaches within the appropriate time after UL, as

---

71 EDPB Fining Guidelines, paragraph 53.a.

72 Article 83(2)(a) GDPR.

73 Recital 82 GDPR.

the controller, became or should have become aware of them. These infringements must be assessed in light of the fact that they are also usually capped at the lower threshold under Article 83(4). The purpose of Article 33(1) is to ensure prompt notification of data breaches to supervisory authorities. This enables the supervisory authority to assess the circumstances of the data breach, including the risks to natural persons. It 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 breach,[74] for example by ordering a controller to communicate a personal data breach to affected data subjects under Article 34(4) or 58(2)(e) GDPR.

175. The nature of the infringements of Article 34(1) GDPR identified herein comprises UL's failure to communicate to data subjects without undue delay information about personal data breaches which UL had assessed to pose a high risk. The purpose of Article 34(1) is to enable data subjects to take prompt action to protect their rights and freedoms, and to mitigate risks posed to them by the breach. Failure to communicate a breach as required by Article 34(1) may prevent data subjects becoming aware of the breach even though the controller has assessed that it poses a high risk to them.

The gravity of the infringements

176. 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.[75]

177. The gravity of the infringements of Articles 5(1)(f) and 32(1) GDPR is high. A large number of data subjects (521) had personal data present in the compromised UL email accounts and so were placed at risk by the Breaches. Some of that data was special category personal data as it included health records; some was financial data and passport details, which are also highly sensitive. The Breaches placed data subjects at a clear risk of identity theft or fraud, as bank details, payment card details, and identity documents were also affected by the Breaches. The DPC recognises that, since the temporal scope of the inquiry, UL has made substantial improvements to its technical and organisational measures to secure processing, including improved training and awareness programmes, moving to the more secure Microsoft 365 platform, the introduction of multi-factor authentication for all staff and student users and more comprehensive and appropriate policy documentation. However, UL's compliance with these Articles must be assessed as at the time of the Breaches. As detailed above in this Decision, UL failed to implement

---

74 Recital 85 GDPR.

75 Article 83(2)(a) GDPR.

appropriate security measures to secure its processing and protect the rights and freedoms of data subjects. These failures resulted in a series of data breaches that posed serious risks to rights and freedoms. For these reasons, the DPC considers the gravity of UL's infringements of these Articles to be high.

178. The gravity of the infringement of Article 30(1) is low. Article 30(1) states clearly what is required in a ROPA, and as a controller with considerable technological and compliance resources, UL should have been aware of its obligation under the GDPR to arrange for an appropriate record to be created and maintained. However, UL failed to document a general description of the technical and organisational security measures that were in place at the time of the Breaches. On this basis, the DPC finds the gravity of the infringement of Article 30(1) to be low.

179. The gravity of the infringement of Article 33(1) is medium. In each of the three cases in which breach notifications were made more than 72 hours after UL became aware of them, the delays were of moderate duration, and appropriate notifications with all required information were sent to the DPC within 72 hours of their being brought to the attention of UL's data protection officer.

180. The gravity of the infringement of Article 34(1) is high. UL failed to notify affected data subjects of personal data breaches that UL itself had assessed to pose high risks. The DPC takes account of the fact that, in breach BN-19-4-3, UL conducted an internal investigation which concluded that 76 data subjects were at high risk and so required notification. However, that notification did not occur until nearly six months after UL first became aware of the breach and stated to the DPC that it posed a high risk. In BN-19-4-348, UL initially assessed the risk posed by the breach to be high. However, following an investigation of more than three months' duration, UL reassessed the risk and reduced it to medium. Based on that revised assessment, UL did not contact the relevant data subjects. The DPC notes that UL regarded its initial high risk assessment as erring on the side of caution. However, UL's failure to notify the affected data subjects shows that the same caution did not apply to the rights and freedoms of the affected data subjects.

The duration of the infringement

181. 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.[76]

182. 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.[77]

183. 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.[78]

184. Regarding the duration of the infringements of Articles 5(1)(f) and 32(1) GDPR, this Decision considers UL's security measures as in effect from 19 November 2018 until 17 January 2020, the date of the breach BN-20-1-82. The DPC therefore finds that the duration of UL's infringements of Articles 5(1)(f) and 32(1) GDPR was 1 year, 1 month and 29 days.

185. Regarding the duration of the infringement of Article 30(1) GDPR, UL's records of processing activity did not contain a general description of the technical and organisational security measure in place, until the revised edition was rolled out to two departments on a pilot basis in January 2020, and to all departments in May 2020.[79] Creating and maintaining a record of processing activity became a requirement when the GDPR took effect on 25 May 2018, but was not fulfilled by UL until May 2020. The DPC therefore finds that the duration of this infringement was 2 years.

186. Regarding the duration of the infringements of Article 33(1), for the reasons set out in section G.c) above, none of the information or submissions received by the DPC during the course of this inquiry indicate any sufficient reason why breach notifications could not have been submitted to the DPC within the 72-hour period referred to in Article 33(1) GDPR. UL notified the DPC of BN-18-12-2 ten days after becoming aware of it, of BN 19-6-96 five days after, and BN-19-8-135 six days after. Allowing for the 72-hour period

---

76 EDPB Fining Guidelines section 53.c.

77 A29WP Fining Guidelines, p.11.

78 Article 83(2)(a) GDPR.

79 UL Submissions on the Draft Inquiry Report, 26 November 2020, p.7.

provided for in Article 33(1) GDPR, the DPC therefore finds that the duration of UL's infringement of Article 33(1) was seven days in the case of BN-18-12-2, two days for BN-19-6-96, and three days for BN-19-8-135.

187. Regarding the duration of the infringements of Article 34(1), in BN-19-4-3 the DPC recognises that UL notified data subjects of the breach and the risks to their rights and freedoms approximately six months after UL became aware of the breach and assessed the risk it posed as high. In the case of BN-19-4-348, UL initially assessed the risk as high but did not inform the data subjects and undertook an internal investigation. After approximately three months, this resulted in the risk assessment being downgraded from high to medium. UL had ample opportunity during those periods of six and three months to identify and notify data subjects, but did not do so. The DPC finds that the duration of UL's infringements of Article 34(1), were six months in the case of BN-19-4-3, and three months in the case of BN-19-4-348.

Assessment of Article 83(2)(a)

188. In relation to Articles 5(1)(f) and 32(1) GDPR, the identified deficiencies in security measures for UL's processing of personal data via its email and IT systems allowed unauthorised third parties to gain access to personal data for which UL was responsible. They led to a loss of control over personal data, and had the potential to lead to further risks to the rights and freedoms of data subjects.

189. Having regard to Article 30(1), UL was required to maintain a designated Record of Processing Activities that detailed prescribed information about its processing. Failure to do this is a contravention of the GDPR, increases risks to the rights and freedoms of data subjects, and impedes the controller's ability to demonstrate compliance with its obligations under GDPR. Information required to be included in the Record of Processing Activity was accessible and could have been, but was not, included.

190. With regard to the infringements of Article 33(1), the personal data breaches BN-18-12-2, BN-19-6-96 and BN-19-8-135 all resulted in risk to the rights and freedoms of natural persons and should have been notified to the DPC within 72 hours of UL becoming aware of them. 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.

191. Article 34(1) requires UL to communicate a breach without undue delay to any concerned data subjects where the breach poses a high risk. It is understandable that controllers need to investigate breaches to fully determine their causes and effects. However, it is at least as important to ensure that the affected data subjects can act to protect and mitigate risks to their rights and freedoms. Article 34(1) therefore obliges controllers to

notify them without undue delay. The infringements found herein affected data subjects who were assessed by UL itself to be at high risk. The DPC acknowledges that, in BN-19-4-348, a subsequent review found that the risk to data subjects was medium rather than high, and that no special category or otherwise sensitive personal data was affected.

192. Taking account of all the factors outlined in this section, the DPC assesses these infringements to be of a serious nature.

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

193. 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.[80]

194. 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'.[81] 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.

195. In this case, the DPC finds that UL's infringement of Articles 5(1)(f) and 32(1) GDPR were negligent in character. This infringement arose from UL's 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. To classify this infringement as intentional, the DPC would have to be satisfied that UL (i) wilfully omitted to implement appropriate technical and organisational measures and (ii) knew at the time

---

[80] A29WP Fining Guidelines, p. 11.

[81] EDPB Fining Guidelines, paragraph 56.

that the measures that it implemented were not sufficient to meet the standards required by Articles 5(1)(f) and 32(1) GDPR.

196. While UL's attempts during the temporal scope of the inquiry 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 UL knew either that the measures implemented were not sufficient at the time, nor the extent of the shortfall in those technical and organisational measures. The DPC is reinforced in this view by the promptness, quality and extent of the actions taken by UL to remediate deficiencies in technical and organisational measures identified during the inquiry.

197. UL ought to have been aware that it was falling short of the duty owed under Article 5(1)(f) and 32(1). For example, UL ought to have been aware that its failure to implement MFA for all email accounts and its inadequately robust MailMarshal configuration greatly and inappropriately increased the risk of a cyber attack. Similarly, UL should have been aware that some essential security policies and procedures were inadequate or non-existent at various times during the temporal scope. The infringement was negligent because UL ought to have been aware that it was falling short of the standards required by Articles 5(1)(f) and 32(1) GDPR.

198. UL is required under Article 30(1) GDPR to maintain a sufficient record of processing activity. The DPC received an incomplete record of processing activity from UL. This lacked required information on the controller's organisational and technical measures specific to the categories of data subjects and categories of personal data being processed. UL informed the DPC that this information was documented elsewhere, but UL should have been aware of its obligation to document this information in compliance with Article 30(1) GDPR. To find that this infringement was intentional in nature, the DPC would have to be satisfied that the evidence indicated that UL was aware of the need to include the missing information but had deliberately chosen to omit it. The DPC has seen nothing in the information and materials provided to it during the Inquiry to suggest that this is the case. On this basis, the DPC finds that UL's infringement of Article 30(1) was negligent in character.

199. The DPC finds that UL's infringements of Article 33(1) were negligent in character. Nothing in the information or materials provided to the DPC indicate or suggest that UL intentionally chose to delay notification of breaches beyond the time provided for in Article 33(1). The reasons given by UL for the delays in notifying those breaches in question all reflect either unawareness, or an erroneous interpretation, of the clearly phrased requirements of Article 33(1) GDPR.

200. Similarly, the DPC finds that UL's infringements of Article 34(1) GDPR were negligent in character. The DPC recognises that each breach requires a certain degree of internal investigation to establish and address its causes and consequences. However, in a

situation where the controller itself has assessed a breach to pose a high risk to rights and freedoms, such investigations must not be at the expense of data subjects' rights to be informed and to take timely steps to protect their rights and interests. UL should have, but evidently did not, appreciate this. The DPC accepts that UL did not deliberately choose to conceal or withhold information about breaches from affected data subjects, and that the infringement of Article 34(1) identified herein arose from a misunderstanding of its responsibilities under that Article. The DPC therefore finds the infringement was negligent in character.

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

201. 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.[82]

202. UL put in place significant remedial measures both during and after the temporal scope of the inquiry. However, it is not always possible to correct a lack of control retrospectively, and these actions did not significantly mitigate the risk to the confidentiality of personal data that had already been compromised.

203. Between April 2019 and November 2025, UL made substantial technical and organisational changes as a result of the Breaches.[83] These included the acceleration of its plan to migrate all staff to the more secure Microsoft 365 platform, the implementation of MFA for staff and student users, updates to UL's training and awareness programmes and revisions of and additions to UL's policies and procedures relevant to data protection concerns. In respect of BN-19-4-3 and BN-19-4-348, UL commissioned external experts to investigate the Breaches and recommend appropriate responses. UL also established a Security Incident Response Team (SIRT) to assess the risks posed by breaches. Having regard to these actions for the purpose of Article 83(2)(c) GDPR, the DPC takes the view that they provide limited mitigation of the infringements identified herein.

---

82 A29WP Fining Guidelines, pp. 12-13.

83 UL Submission on Draft Decision, 7 November 2025, pages 5 – 10.

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;

204. The key question in relation to this provision is whether UL '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 it by the Regulation.[84]

205. As outlined above, UL infringed Articles 5(1)(f) and 32(1) GDPR by failing to implement appropriate technical and organisational measures regarding its processing of personal data on its email service during the temporal scope of this inquiry. The DPC considers that UL 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 infringement of Article 32(1), this factor cannot be considered aggravating in respect of those infringements.

206. UL submitted that the infringements identified in this Decision must be understood in the context of the recent introduction of the GDPR, 'when many public sector organisations were still adapting to the new regulatory framework'.[85] UL submitted that its technical and organisational measures, 'while ultimately found to be insufficient, were consistent with sectoral norms and reflected a reasonable effort to comply with the GDPR.' [86]

207. The DPC does not accept that the introduction of the GDPR approximately 6 months before the first of the Breaches provides any grounds for mitigation of the infringements found in this Decision. The GDPR was enacted two years before it entered into force, and UL had considerable technical, organisational and financial resources to properly assess its requirements and plan for compliance with it. Moreover, the standards of security required on the introduction of the GDPR were not significantly different from those applying before then. The DPC does not accept that 'sectoral norms' applying during the temporal scope of the inquiry would accommodate or excuse the infringements identified in this Decision.

208. In relation to the infringements of Articles 5(1)(f) and 32(1) GDPR, UL pointed out that it 'had already identified several of the relevant risks, and had initiated plans to address them' including migration to Microsoft 365, adoption of MFA and use of encryption. UL also cited the rapidly evolving threat landscape faced by higher educational institutions

---

84 EDPB Fining Guidelines, paragraph 77.

85 UL Submission on Draft Decision, 7 November 2025, page 5.

86 UL Submission on Draft Decision, 7 November 2025, page 29.

globally, and the promptness and thoroughness of its actions to contain and remediate the Breaches.

209. The DPC accepts that UL recognised at an early date the risks posed by the Breaches and the steps required to address them. However, the DPC notes that steps such as the introduction of MFA for all users was not completed until April 2021. Regarding the evolving threats faced by universities such as UL, the DPC reiterates that UL had adequate time and resources to plan for compliance with GDPR. Further, the threats facing UL were not significantly different from other large Irish universities, which did not demonstrate a similar history of serious personal data breaches.

210. Notwithstanding the reservations expressed above, the DPC acknowledges that UL has fully accepted its responsibility for the infringements of Articles 5(1)(f and 32(1) identified herein:

> The University of Limerick accepts the DPC's provisional findings in respect of Articles 5(1)(f) and 32(1) GDPR. We acknowledge that, at the time of the breaches (November 2018 to January 2020), the technical and organisational measures in place to secure our staff email system were not sufficient to mitigate the risks posed by increasingly sophisticated phishing attacks.[87]

211. During the course of this Inquiry, UL advised the DPC that, prior to the introduction of the GDPR in May 2018, an internal GDPR taskforce was put in place to oversee the implementation of the GDPR and ensure that UL would be in compliance.[88] As described in the analysis of the infringements above, this taskforce failed to identify its requirements to document a general description of the technical and organisational security measures within the record of processing activity, which resulted in UL failing to fully comply with its obligations in respect of Article 30(1).

212. UL also cited the recent entry into effect of the GDPR as relevant to the infringement of Article 30 GDPR identified herein. [89] For the reasons given in paragraph 207 above, the DPC does not accept this as a ground for mitigation. While, as UL noted in its submission on the Draft Decision, the EDPB had observed that bodies such as universities had had difficulty complying with Article 30 GDPR in the early days of its application, that is not an excuse for non-compliance.

---

87 UL Submission on Draft Decision, 7 November 2025, page 4.
88 UL Submission on Draft Decision, 7 November 2025, page 3.
89 UL Submission on Draft Decision, 7 November 2025, page 11.

213. The DPC acknowledges UL's acceptance that its ROPA developed in 2018 did not fully meet the requirements of Article 30(1) GDPR.[90]In relation to the infringements of Article 33(1) identified herein, UL is obliged, as a controller, to comply with the GDPR to ensure that the rights and freedoms of data subjects are protected. In relation to BN-18-12-2, the DPC acknowledges that UL has accepted that it failed to comply with the requirements of that provision.[91] However, UL did not accept that it failed to notify BN-19-6-96 and BN-19-8-135 within the required time. For the reasons set out in paragraphs 115 to 122, the DPC has determined that UL failed without good reason to notify the DPC within 72 hours of becoming aware of those breaches. The DPC therefore finds that UL is entirely responsible for those infringements.

214. Regarding Article 34(1) GDPR, in BN-19-4-3 and BN-19-4-348 UL failed to meet its obligation as a controller to notify data subjects without undue delay of the high risk to their rights and freedoms that UL itself had assessed to be posed. The DPC acknowledges UL's acceptance of responsibility for these infringements:

> UL accepts the DPC's provisional findings in respect of Article 34(1) GDPR. We acknowledge that the communication of the two breaches to affected data subjects was either delayed (BN-19-43) or not carried out (BN-19-4-348), and that this fell short of the standard required under the GDPR.[92]

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

215. In line with the EDPB Fining Guidelines, prior infringements are those already established before the draft decision (in the sense of Article 60 GDPR) is issued.[93] According to the A29WP Fining Guidelines, '[t]his criterion is meant to assess the track record of the entity committing the infringement.'[94]

216. In this case, UL has not been found to have committed any relevant previous infringements of the GDPR.

---

90 UL Submission on Draft Decision, 7 November 2025, pages 11 and 12.
91 UL Submission on Draft Decision, 7 November 2025, page 14.
92 UL Submission on Draft Decision, 7 November 2025, page 16.
93 EDPB Fining Guidelines, paragraph 82.
94 A29WP Fining Guidelines, p.14.

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;

217. The extent to which UL has cooperated with the inquiry is relevant to consider under this heading.[95] UL cooperated fully with the DPC to remedy the infringements and to mitigate their adverse effects. In its breach notifications and incident reports, UL informed the DPC of the steps that it had taken, and was in the course of taking, to remedy the infringements and the possible adverse effects. UL cooperated fully with the DPC throughout the Inquiry, including on the day of the inspection, in seeking to remedy the infringements. UL's submissions during the Inquiry also detailed the measures that it implemented, and is in the course of implementing, to provide an appropriate level of security in respect of its email service. UL further updated the DPC on these measures in its submissions on the Draft Inquiry Report, including the establishment of a Security Incident Response Team (SIRT) to assess risks posed by breaches.

218. The DPC acknowledges UL's cooperation with the DPC during the course of the Inquiry. However, the DPC notes that UL was, in any event, under a duty, in light of Article 31 GDPR, to cooperate in this manner on request with the supervisory authority in the performance of its tasks.

219. The DPC recognises UL's actions to identify and remedy deficiencies in its processing identified during the course of this Inquiry. These have been separately taken into account for the purpose of mitigation under Article 83(2)(c) above and Article 83(2)(k) below.

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

220. 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 encrypted or whether the processing involves data whose dissemination would cause immediate damage or distress to the individual.[96]

221. The DPC considers that the categories of personal data affected by the infringements found in this Decision included special category personal data in the form of health data. As outlined above in this Decision, the personal data affected also included payment card

---

95 A29WP Fining Guidelines, p.14.

96 A29WP Fining Guidelines, p.14.

details, bank details, health data, home addresses, passport details and PPS numbers. Some of this personal data is by its very nature particularly sensitive with regard to the fundamental rights and freedoms of data subjects by reason of its sensitivity or its ability to be misused for purposes such as fraud and identity theft. The DPC finds that the sensitivity of these categories of personal data aggravates the infringements found in this Decision because unauthorised access to them can cause serious damage and distress to data subjects. In particular, the loss of control of these categories of personal data creates a significant risk of 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;

222. 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.'[97]

223. 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.[98]

224. UL'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), 30(1), 32(1) and 34(1). Similarly, UL's undue delay in notifying the DPC of breaches is not aggravating in circumstances where that infringement is the subject of consideration for this corrective power.

---

97 A29WP Fining Guidelines, p.15.

98 A29WP Fining Guidelines, p.15.

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;

225. 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'.[99]

226. Corrective powers have not previously been ordered against UL 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;

227. 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.

228. The EDPB Fining Guidelines state:

> Article 83(2)(k) GDPR gives the supervisory authority room to take into account any other aggravating or mitigating factors applicable to the circumstances of the case. In the individual case there may be many elements involved, which cannot all be codified or listed and which will have to be taken into account in order to ensure that the sanction applied is effective, proportionate and dissuasive in each individual case.
>
> Article 83(2)(k) GDPR refers to examples of 'any other aggravating or mitigating factor applicable to the circumstances of the case,'... It is considered that this provision is of fundamental importance for adjusting the amount of the fine to the specific case. In this sense, it is considered that it should be interpreted as an instance of the principle of fairness and justice applied to the individual case.[100]

---

99 A29WP Fining Guidelines, p.15.

100 EDPB Fining Guidelines, para 108.

229. In this case, save only in relation to BN-19-9-6 and BN-19-8-135, UL has expressly accepted each of the DPC's provisional findings of infringement as set out in the Draft Decision, and has acknowledged full responsibility for those infringements. As detailed in paragraph 141 above, UL informed the DPC that, in the period since the first of the Breaches, it has implemented substantive technical and organisational measures in order to reduce the likelihood of similar breaches occurring in future.

230. The DPC notes the interpretation of Article 83(2)(k) in the EDPB Fining Guidelines quoted in paragraph 230 above, which suggests that a wide range of factors may be considered by supervisory authorities as potentially mitigating or aggravating under this heading, with the overriding consideration being the principle of fairness and justice as applied to the circumstances of the case at hand.

231. Similarly, the DPC notes that the A29WP Fining Guidelines state:

> Regulatory experience from SAs under the 95/46/EC Directive has previously shown that it can be appropriate to show some degree of flexibility to those data controllers/processors who have admitted to their infringement and taken responsibility to correct or limit the impact of their actions.[101]

232. Although that statement in the A29WP Fining Guidelines is set out as part of its consideration of Article 83(2)(c), the DPC considers it appropriate to consider as part of its assessment of Article 83(2)(k) also, as UL has admitted to the majority of the infringements identified in this Decision, and taken responsibility to limit the risk of similar incidents occurring in future.

233. Taking all the above into account, the DPC considers that UL's actions in

- admitting to the majority of the infringements provisionally found in the Draft Decision and in
- proactively taking steps, without having been specifically directed to do so by the DPC, to limit the risk of similar incidents occurring in future

is commendable and, in the circumstances, constitutes a mitigating factor.

---

101 A29WP Fining Guidelines, 13.

b) Decision on whether to impose administrative fines

234. 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.'[102]

235. Taking into account the assessment of the criteria at (a) to (k) above, the DPC proposes to impose administrative fines in respect of the infringements of Articles 5(1)(f), 32(1), 33(1) and 34(1) GDPR. The infringements of Articles 5(1)(f) and 32(1), and 34(1) GDPR 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 of serious weight, which indicates that a fine should be imposed. When considering Articles 83(2)(b) and (g), the DPC found that UL was negligent with respect to those infringements and that the infringements affected personal data that, 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 identity theft. These are aggravating factors of moderate weight indicating that a fine should be imposed.

236. The DPC considers that the measures adopted by UL 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. Similarly, the DPC considers that the factors assessed in relation to Article 83(2)(k) are mitigating but do not negate the need to impose an administrative fine. The DPC considers that the factors assessed in relation to Articles 83(2)(e), (f), (h), (i) and (j) are neither mitigating nor aggravating.

237. 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

---

102 EDPB, Binding Decision 1/2023.

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.

238. While the reprimand will assist in dissuading UL and other entities from similar future non-compliance, in light of the seriousness of the infringements, 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 UL and other controllers or processors carrying out similar processing operations. The reasons for this finding include:

- The infringements of Articles 5(1)(f), 32(1) and 34(1) GDPR are 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 34(1) GDPR, the DPC considers that UL'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.
- The infringements of Article 33(1) were moderate in nature and gravity as set out pursuant to Article 83(2)(a) GDPR. The obligation to report breaches promptly is an important measure to ensure accountability of controllers and to enable supervisory authorities to act to protect the rights and freedoms of data subjects. This was not an isolated incident, as there were repeated delays in reporting over the temporal scope of this inquiry. Notwithstanding the moderate nature of the infringements found in this case, non-compliance with this important requirement must be dissuaded, and an administrative fine is the appropriate way to do so in this case.
- The infringement of Article 30(1) was minor in nature and gravity as set out pursuant to Article 83(2)(a) GDPR. However, it formed part of a larger pattern of non-compliance by UL with its obligations under GDPR including, as found in relation to Article 32(1) GDPR, absent or inadequate technical and organisational measures to ensure the security of processing. Taking account of all factors previously mentioned, an administrative fine is the appropriate means of dissuading non-compliance with this requirement.

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

240. Having regard to the nature, gravity and duration of the infringements, the DPC also considers that administrative fines are proportionate for ensuring compliance. UL's infringements of Articles 5(1)(f) and 32(1) GDPR were a primary cause of the data breaches examined in this inquiry. In light of this damage, the DPC considers that administrative fines are proportionate in response to UL's infringements of Articles 5(1)(f) and 32(1), 30(1), 33(1) and 34(1) GDPR with a view to ensuring future compliance. The DPC considers that the administrative fines imposed in this Decision do not exceed what is necessary to enforce compliance in respect of the infringements identified in it.

241. The DPC considers that the negligent character of UL's infringements of Articles 5(1)(f) & 32(1), 30(1), 33(1) and 34(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 UL directs sufficient attention to its obligations under those Articles in the future.

242. The DPC considers that administrative fines would help to ensure that UL 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.

243. The DPC has had regard to the lack of previous relevant infringements by UL, which is a slightly mitigating factor. The DPC has also had regard to the actions taken by UL as a result of the breach. In light of the negligent character of the infringements and of UL'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.

c) Decision on the amount of the administrative fine

244. Above, it was determined that it was necessary to impose administrative fines. This section calculates the amount of those fines, 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

245. 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.

246. As outlined previously, the infringements identified herein all relate to the processing concerned, i.e. via UL's email system.

247. 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.

> 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.

248. The impact of this interpretation is that administrative fines are imposed cumulatively, as opposed to imposing only the 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.

249. In this case, infringements of Articles 5(1)(f) & 32(1), 30(1), 33(1) and 34(1) GDPR were identified. The gravest infringements are that of Article 5(1)(f), as it involves an infringement of a core principle of the GDPR. As stated in paragraph 264 below, section 141(4) of the 2018 Act, which sets a cap of €1,000,000 for administrative fines, applies in this case. Accordingly, €1,000,000 is the cumulative cap for the fines imposed in this Decision.

(ii) Categorisation of the infringements

250. 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.[103]

251. 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) GDPR 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), 30(1), 33(1) and 34(1) GDPR.

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

252. 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 as a whole.[104] These factors were assessed in paragraphs 170 to 195 and 220 to 221 above. The guidelines also state:

> 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.[105]

253. Having regard to these factors as a whole, the infringements are of a medium level of seriousness. Under Article 83(2)(a) the infringements of Articles 5(1)(f) and 32(1), and of Article 34(1) GDPR 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). UL were also negligent to a medium degree with respect to the infringements, as assessed under Article 83(2)(b). The infringement of Article 33(1) GDPR was found to be of a moderate nature and gravity, while that of Article 30(1) was minor in nature and gravity. Therefore, balancing these factors, the DPC considers that the infringements were of medium seriousness.

---

103 EDPB Fining Guidelines, paragraph 50.
104 EDPB Fining Guidelines, paragraph 51.
105 EDPB Fining Guidelines, paragraph 59.

(iv) Imposing an effective, dissuasive and proportionate fine

254. Article 83(1) GDPR requires a fine to be effective, proportionate and dissuasive in each individual case. As the guidelines also say that this does not 'dismiss a supervisory authority from the responsibility to carry out a review of the effectiveness, dissuasiveness and proportionality at the end of the calculation.'[106] Article 83(1) will be considered again at the end of this calculation.

(v) Aggravating and mitigating circumstances

255. 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 UL had not adopted measures to mitigate the damage to data subjects. However, UL made a number of substantial technical and organisational changes as a result of these data breach. This is considered to be a mitigating factor of low weight.

256. In relation to Article 83(2)(d), UL had a high degree of responsibility for the infringements. UL 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, this factor cannot be considered aggravating in respect of that infringement. Therefore, the DPC considers that this factor is neither aggravating nor mitigating in the circumstances.

257. In relation to Article 83(2)(e), it was noted that UL did not have any previous relevant infringements. This factor is considered to be neither mitigating nor aggravating.

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

259. In relation to Article 83(2)(h), it was noted that the manner in which the infringements became known to the DPC was by means of breach notifications submitted by UL. The DPC considers that this factor is neither aggravating nor mitigating in the circumstances.

---

106 EDPB Fining Guidelines, paragraph 64.

260. In relation to Article 83(2)(i), it was noted that UL has not been the subject of previous orders by the DPC with regard to the same subject matter.[107] This factor is considered to be neither mitigating nor aggravating.

261. 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. This factor is neither mitigating nor aggravating.

262. In relation to Article 83(2)(k), it was noted that UL accepted responsibility for all infringements except in relation to BN-19-9-6 and BN-19-8-135. UL also took steps to remediate and undertook technical and organisational measures to limit the risk of similar infringements occurring in future. The DPC considers this a mitigating factor of medium weight.

263. 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 proposes administrative fines as follows:

- In respect of UL's infringement of Article 5(1)f and 32(1) GDPR, an administrative fine of €45,000,
- In respect of UL's infringement of Article 30(1), an administrative fine of €3,000,
- In respect of UL's infringements of Article 33(1) GDPR, an administrative fine of €35,000,
- In respect of UL's infringement of Article 34(1), an administrative fine of €15,000.

These fines, totalling €98,000, are substantially lower than the total maximum fine of €161,000 proposed in the Draft Decision. The final fines reflect the mitigation occasioned by UL accepting the provisional findings of infringements in the Draft Decision, except, as noted previously, in respect of Article 33(1) regarding BN-19-9-6 and BN-19-8-135. UL's acceptance acknowledged full responsibility for infringements, recognised their seriousness and highlighted the significant

---

[107] 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.'

improvements in its technical and organisational measures as indicating its commitment to compliance protecting data protection rights.

d) The relevant legal maximum for administrative fines

264. The DPC notes that UL 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 UL acts as an undertaking for the purpose of the processing concerned.

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

(i) Effectiveness

265. 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 health 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 imposed ensures sufficiently effective fines, and no further adjustment is required.

(ii) Dissuasiveness

266. 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 administrative fines imposed in this Decision are dissuasive for both. The DPC considers the monetary value of the fines to be sufficient to have such a deterrent effect.

267. The infringements of Articles 5(1)(f) and 32(1), and of Article 34(1) GDPR are 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 those infringements, the DPC considers that UL'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.

268. While the infringements of Articles 30(1) and 33(1) GDPR identified in this Decision are less serious than those of Articles 5(1)(f) and 32(1) and Article 34(1) GDPR, the DPC views them as forming part of a pattern of non-compliance or inadequate compliance with important provisions of the GDPR. Controllers must be dissuaded from adopting such an approach to the rights and freedoms of individuals. For that reason, the DPC considers the administrative fines to be appropriate and necessary.

269. The DPC considers that the negligent character of UL's infringements of Articles 5(1)(f) & 32(1), 30(1), 33(1) and 34(1) GDPR carries weight when considering the amount of those fines. This negligence suggests that the administrative fines are necessary to ensure that UL directs sufficient attention to its data protection obligations in the future.

270. The DPC considers that the amounts of the administrative fines would help to ensure that UL 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.

271. The DPC has had regard to the lack of previous relevant infringements by UL, which is a slightly mitigating factor. It has also had regard to the actions taken by UL as a result of the breach. In light of the negligent character of the infringements, and UL'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.

(iii) Proportionality

272. 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 UL'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.

273. 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. UL's infringements of Articles 5(1)(f) and 32(1) GDPR were a primary cause of the data breaches. In light of this, the DPC considers that the administrative fines are a proportionate response to UL's infringement of Articles 5(1)(f) & 32(1), 30(1), 33(1) and 34(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

274. In summary, the corrective powers that the DPC proposes to exercise are:

- a Reprimand to UL pursuant to Article 58(2)(b) GDPR regarding the infringements identified in this Decision; and
- administrative fines, as follows:

(i) In respect of UL's infringement of Article 5(1)f and 32(1) GDPR, an administrative fine of €45,000,

(ii) In respect of UL's infringement of Article 30(1), an administrative fine of €3,000,

(iii) In respect of UL's infringements of Article 33(1) GDPR, an administrative fine of €35,000,

(iv) In respect of UL's infringements of Article 34(1), an administrative fine of €15,000.

M. Right of Appeal

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

This Decision is addressed to:
University of Limerick
Limerick, V94 T9PX,
Ireland

Decision-Makers for the Data Protection Commission:

Dr. Des Hogan
Commissioner for Data Protection
Chairperson

Dale Sunderland
Commissioner for Data Protection

Niamh Sweeney
Commissioner for Data Protection