In the matter of the General Data Protection Regulation

DPC Case Reference: IN-20-4-1

In the matter of The Teaching Council

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

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

DECISION

Decision-Maker for the Commission:

Helen Dixon
Commissioner for Data Protection

2 December 2021

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Protection Commission
2 Fitzwilliam Square South
Dublin 2, Ireland

Contents

1. Introduction

1.1 This document ("**the Decision**") is a Decision of the Data Protection Commission ("**the DPC**") in accordance with Section 111 of the Data Protection Act (**"the 2018 Act").** I make this Decision having considered the information obtained in the own volition inquiry (**"the Inquiry"**) conducted by a Case Officer of the DPC (**"the Case Officer")** pursuant to Section 110 of the 2018 Act. The Case Officer who conducted the Inquiry provided the Teaching Council (**"the Council"**) with the Draft Inquiry Report and the Final Inquiry Report. The Decision is being provided to the Council pursuant to Section 116(1)(a) of the 2018 Act in order to give the Council notice of the Decision and the reasons for it, and the corrective powers that I have decided to exercise.

1.2 This Decision contains corrective powers under Section 115 of the 2018 Act and Article 58(2) of the General Data Protection Regulation ("**the GDPR**") arising from the infringements which have been identified herein by the Decision Maker. The Council will be required to comply with these corrective powers, and it is open to this office to serve an enforcement notice on the Council in accordance with Section 133 of the 2018 Act.

2. Legal Framework for the Inquiry and the Decision

i. Legal Basis for the Inquiry

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

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

ii. Legal Basis for the Decision

2.3 The decision-making process for this Inquiry is provided for under Section 111 of the 2018 Act, and requires that the DPC must consider the information obtained during the Inquiry; to decide whether an infringement is occurring or has occurred; and if so, to decide on the proposed corrective powers, if any, to be exercised. As the sole member of the Commission, I perform this function in my role as the Decision-Maker in the DPC. In so doing, I am required to carry out an independent assessment of all the materials provided to me by the Case Officer as well as any other materials that the Council has furnished to me and any other materials that I consider relevant, in the course of the decision-making process.

2.4 The Final Inquiry Report was transmitted to me on 12 April 2021, together with the Case Officer's file, containing copies of all correspondence exchanged between the Case Officer and the Council; and copies of all submissions made by the Council, including the submissions made by the Council in respect of the Draft Inquiry Report. A full schedule of all documentation considered by me for the purpose of this Decision is appended hereto. I issued a letter to the Council on 13 April 2021 to notify it of the commencement of the decision-making process.

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

3. Factual Background

3.1 The Council is located at Block A Maynooth Business Campus, Maynooth, Co. Kildare. Its purpose is to be the professional standards body for the teaching profession and to promote and regulate professional standards in teaching. The Minister for Education and Skills commenced Section 30 of the Teaching Council Act, 2001 on 28 January 2014. Section 30 makes it a requirement for teachers to register with the Teaching Council in order to be paid a salary by the State.

3.2 The DPC received notification of a personal data breach from the Council on 9 March 2020. The breach notification (BN-20-03-399) indicated a potential contravention of the data protection legislation by the Council in its capacity as a data controller.

3.3 The breach notification stated that a phishing email had been received by two members of staff in the Council and was accessed by them. The notification claimed:

"*This caused a script to be activated that established an auto forwarding rule for all subsequent emails being sent to the two individuals to an external Gmail account*."

3.4 In total, 323 email messages were forwarded to the external Gmail account.

3.5 The Council commissioned Consultancy 1 to undertake a report into the occurrence of the breach, a copy of which was provided to the DPC on 17 June 2020. In that report it is stated that:

"Due to the same type of email redirection to Gmail and method of redirection used it is our opinion the same phishing campaign was used in both cases. It is the opinion of Consultancy 1 that both users were phished as part of a phishing campaign where users entered their passwords online.

"It should be noted that both users have stated that [they] did not enter their password. This would be expected as they would have perceived this to be normal activity and an advanced phishing campaign would capture details without the user being aware."

i. Chronology

3.6 On 17 February 2020 the IT section of the Council, consisting of internal IT staff and an external IT services provider, received an email alert in Office 365 with subject *Low-severity alert: Creation of forwarding/redirect rule* in relation to the account of staff user *nameduser1@teachingcouncil.ie.* In response to the receipt of this alert, the Council IT staff changed the password of the affected user, checked the Global forward rules in Office 365 and carried out anti-virus scans on the user's PC. The Council did not discover at that time that an auto forward rule had been created on the user's account, despite the subject of the alert clearly stating that a forwarding/redirect rule had been created.

3.7 When asked by the Case Officer to provide clarification as to why the auto forwarding rule had not been found when checked on 17 February 2020 the Council stated that :

"A number of steps were taken to investigate why a low severity alert was received including running Anti-Virus scans on the user's PC and checking the Global forward rules in the Exchange Administrator portal in Office 365. As no evidence of malware or virus was discovered on the user's desktop the IT personnel considered the alert to be a false alert. The Outlook client or user's OWA personal access was not checked on this date."

3.8 On 19 February 2020 the IT section of the Council received an email alert in Office 365, again to the account of user *nameduser1*, with subject *High severity alert: User restricted from sending email*, the content of which stated

"*User nameduser1@teachingcouncil.ie has been restricted from sending messages outside the organization due to potential compromised activity"*

3.9 On foot of this alert, Microsoft Office 365 automatically blocked emails being sent from the *nameduser1* account. The Council have stated in submissions that at that time it again changed the affected user's password as a precautionary measure.

3.10 The Council was requested to provide clarification on why the auto forwarding rule for the *nameduser1* account was not found when the second email alert was received on 19 February 2020. The Council stated that :

"*the Outlook client or user's OWA personal access was not checked on this date*"

and that :

"The measures taken at the time are regarded as good practice within the IT industry and an appropriate and reasonable measure in the circumstances."

3.11 On 4 March 2020 the IT section of the Council received a low severity email alert in Office 365 in relation to a second email account*, nameduser2@teachingcouncil.ie*, which stated

"MailRedirect. This alert is triggered when someone gets access to read your user's mail"

3.12 The Council indicated that the same process was undertaken by IT staff with this account as had been undertaken with the *nameduser1* account.

3.13 On 6 March 2020 a high severity alert was triggered in Office 365 for user *nameduser1*. In response, User Credentials were changed by onsite Council IT staff and Office 365 functionality was disabled for the users in question. At that time, the rules within the Outlook client side were explored, and a desktop review discovered a highlighted rule which forwarded emails to an external Gmail account- *phisher1@gmail.com*. When previous alerts had been received by the Council it had only checked the auto forward rules on the server side. 6 March 2020 was the first time the Council checked the auto forward rules on the client side. At this time, the IT Team reported the issue to the Council's Data Protection Officer (DPO). The Council have submitted that prior to this point in time the incident could only be categorised as a potential security alert which was not reportable to the DPO or the DPC. I do not agree with this submission, and address it in detail in Section 7 of this Decision.

3.14 The Council have stated that auto forwarding was discovered that day when:

"IT recalled the similar alerts for nameduser1 and felt that they were connected which meant that a virus or malware were no longer a rational explanation for the receipt of the previous alerts therefore the IT team explored the issue further. A member of the IT Team suggested to check the Outlook rule on the user's desktop. This had not been done

previously. This resulted in the discovery of the rule in nameduser2's Outlook client account which was immediately removed. This also prompted the checking of the account for nameduser1 due to the similarity in the alert, where a similar auto forward rule was discovered and straight away removed from that Outlook client account on 6 March."

3.15 It was later determined that an email forward had been in place for user *nameduser1* from 17 February, when the first alert connected to this account was received, until 6 March 2020, when it was discovered. Email forwarding was active for user *nameduser2* from 4 March 2020, when the first alert on this account was received, until 6 March 2020, when it was discovered.

3.16 The Council was unable to provide an exact number of affected data subjects in the breach notification, however it did identify that 323 emails were forwarded to the unauthorised external email address and that those emails contained, *inter alia*, the vetting status details of 9,735 teachers, including names, addresses, PPS numbers and vetting clearance status. These numbers are not representative of the volume or extent of any personal data held in the inbox, sent items or the content of any folders within the two user email accounts. The Council have stated, in submissions dated 3 September 2021, that there is no evidence to suggest that any other items were accessed.

3.17 As previously stated the Council have submitted that the DPO of the Council was informed of the security incident on 6 March 2020. However, the controller's obligation to notify the breach to the DPC on time is not an obligation solely for the DPO, but rather for the organisation at large.

3.18 The Council notified the DPC of the data breach on 9 March 2020.

3.19 On 2 April 2020, the DPC informed the Council of the commencement of an Inquiry under, and in accordance with, section 110(1) of the Act, by way of a Notice of Commencement of Inquiry (**"the Notice"**) by email[1].

3.20 The DPC made the decision to commence the Inquiry having regard to the circumstances of the personal data breach. The Notice contained details of the breach notified to the DPC which would be the subject of the Inquiry. The Notice set out the scope and legal basis of the Inquiry. The Notice informed the Council that it would examine whether or not the Council had discharged its obligations in connection with the subject matter of the breach and determine whether or not any provision(s) of the 2018 Act and/or the GDPR had been contravened by the Council. The Notice set out that the Inquiry would seek to establish the facts as they relate to the subject of the Inquiry.

3.21 The Notice contained fifteen questions seeking further information from the Council in relation to the circumstances of the breach and sought relevant documentation that informed the Council's responses. Included were questions in relation to the measures in

[1] The Council provided consent to receive electronic notices per Section 106 of the Data Protection Act 2018 by email on 1 April 2020

place at the time of the breach. In particular, the Council was asked to provide specific information that addressed what measures were in place to comply with Article 32 GDPR and by reference to the principle set down in Article 5(1)(f) GDPR in terms of:

1. An assessment of the risks of varying likelihood and severity associated with the forms of data processing at issue in the breaches

2. Appropriate technical and organisational measures to counter those risks

3. Capability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services

4. Processes for regular testing, assessment and evaluating the effectiveness of the technical and organisation measures for ensuring the security of the processing.

3.22 The letter sought a response from the Council by 23 April 2020.

3.23 On 2 April 2020, the Council acknowledged receipt of the Commencement Letter and indicated that it would revert to the DPC with a response to the questions by 23 April 2020 as requested.

3.24 On 23 April 2020, the Council provided its response to the DPC which included supporting documentation.

3.25 On 12 May 2020, after a review of the materials submitted to date, the Case Officer carrying out the inquiry sent an email to the Council seeking responses to a range of further technical questions in relation to the cause of the breach and a copy of the review report undertaken by Consultancy 2 in relation to the breach. The letter sought a response by 26 May 2020.

3.26 On 26 May 2020, the Council provided its response to these technical questions. The Consultancy 2 report was not provided as the Council stated that Consultancy 2 had been engaged:

"to assist with a review of the breach with the objectives being to provide recommendations around addressing risks identified as a result of the breach, conduct a policy review and create an action plan to implement these changes. They were not mandated to carry out a specific report into the breach itself."

3.27 The Council outlined that another entity, Consultancy 1, had been engaged to carry out a report into the breach but that this report was not yet available due to delays relating to COVID-19.

3.28 On 28 May 2020, the Case Officer issued a further letter to the Council seeking clarification on a technical point. The letter again sought a copy of the Consultancy 2 report and a copy of the Consultancy 1 report in draft format, if the completed report was still unavailable. The letter also requested the Council to instruct both Consultancy 2

and Consultancy 1 to retain any notes in relation to the work undertaken by them in relation to the breach. The letter sought a response by 10 June 2020.

3.29 On 10 June 2020, the Council sent an email requesting a one week extension to provide its response. This was acceded to. The email confirmed that the Council had instructed Consultancy 1 and Consultancy 2 to retain notes relating to the breach as requested.

3.30 On 17 June 2020, the Council provided its response and a copy of the report prepared by Consultancy 1. In relation to the other report by Consultancy 2 requested by the Case Officer on 12 and 28 May 2020, the Council stated

"Please note that a report of the phishing incident was not requested by the Teaching Council from Consultancy 2. Consultancy 2 provided assistance to the Teaching Council in putting in place the action plan (previously provided to the DPC) and compiling recommendations on general security awareness and O365 security settings."

3.31 The Consultancy 1 report identified unknown logins to the *nameduser2@teachingcouncil.ie* account on 3 and 4 March 2020 from IP addresses outside of Ireland. These IP addresses were located in the USA and Switzerland (but were likely being used as IP proxies by the attacker) and the logins were most probably made by the attacker as they coincide with when the forwarding rules for the *nameduser2* account were put in place.

3.32 The Consultancy 1 report (dated 17 June 2020) identified that the forwarding rule for the *nameduser1* account was put in place on 17 February 2020. The report could not confirm if an unknown login had taken place on 17 February 2020 to the account as the Office 365 logs did not go back that far. Under standard licensing, Office 365 logs are available for only 90 days. However, the Consultancy 1 report was of the opinion that had the logs been available, they would have shown that "*the same method of redirection was used*".

3.33 Following a careful examination of the Council's 17 June 2020 submissions, the Case Officer considered that certain aspects of the specific technical cause of the breach remained unclear. Therefore, a further letter seeking information and clarification issued by email to the Council on 21 July 2020, seeking a response by 31 July 2020.

3.34 On 31 July 2020, the Council provided its response.

3.35 On 2 October 2020, the Case Officer issued a draft Inquiry Report to the Council with a response date for any submissions thereon by 1 November 2020.

3.36 On 30 October 2020, the Council provided its submission on the content of the draft Inquiry Report. The submissions included a number of comments and observations by the Council. The submissions were considered by the Case Officer and the Final Report amended to include the comments and observations as appropriate.

3.37 In its submission, the Council sought clarity with regard to the remaining Inquiry process. This clarification was provided by letter on 26 November 2020.

3.38 On 13 April 2021, I wrote to the Council to notify it of the commencement of the decision-making stage of the Inquiry. In doing so, I consider the Inquiry Report, together with all other submissions and relevant information, and reach conclusions as to whether I identify infringements of data protection legislation. The Inquiry Report sets out the scope and legal basis for the Inquiry and the Case Officer's view as to whether the Council complied with its obligations under the GDPR and the 2018 Act in respect of the subject matter of the Inquiry. As set out in paragraphs 1.1 and 1.2, this document is my Decision on this matter.

3.39 The Final Inquiry Report was issued to the Council on 13 April 2021.

3.40 On 28 April 2021, the Council wrote to me disputing the findings of the Final Inquiry Report and requesting that the Council be permitted to provide legal submissions prior to the preparation of the draft decision, in particular in relation to Article 33(1).

3.41 On 29 April 2021, I wrote to the Council in response and stated that I would not be accepting any further submissions at that time, but that the Council would have a full opportunity to make submissions in response to the preliminary findings in due course and before they are finalised.

3.42 On 8 June 2021, I wrote to the Council seeking further information on, *inter alia*, the data-flow of information into the Council, how the information is processed and by what method it is accessed by staff of the Council, seeking a response by 15 June 2021.

3.43 On 15 June 2021, the Council sent an email requesting a three day extension to provide its response. This was acceded to, and the information provided on 18 June 2021.

3.44 The Draft Decision was issued to the Council on 15 July 2021.

3.45 Subsequent to the finalisation of the Draft Decision issued to the Teaching Council, the European Data Protection Board adopted a decision ("the EDPB Decision" [Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a)]) relating to IN 18-12-2, an inquiry conducted by the Commission into WhatsApp Ireland Limited's compliance with Articles 12, 13 and 14 GDPR. The EDPB Decision arose out of a dispute resolution procedure pursuant to Article 65 GDPR, and was adopted by the Commission on 2 September 2021.

3.46 Submissions on the Draft Decision were received from the Council on 3 September 2021.

3.47 On 8 September 2021, I wrote to the Council enclosing the Revised Draft Decision and requesting submissions on same, should the Council so wish.

3.48 On 13 September 2021, the Council sent an email requesting additional time to deliver submissions on the Revised Draft Decision. This was acceded to by email of response on 13 September 2021, granting an extension until 29 September 2021.

3.49 Submissions on the Revised Draft Decision were received from the Council on 29 September 2021.

4. Scope of the Inquiry

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

4.2 In this regard, the Notice expressly stated that the scope of the Inquiry would include Articles 5(1), 32(1) and 33 of the GDPR. The Notice stated that the Inquiry would focus on the areas of Security of Personal Data, and Data Breach Notification.

5. Issues for Determination

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

(i) Whether the Council complied with its obligations pursuant to Articles 5(1) and 32(1) of the GDPR with regard to the technical and organisational measures in place to ensure that there was adequate security over personal data held in manual or electronic form.

(ii) Whether the Council complied with its obligation pursuant to Article 33 of the GDPR in relation to the reporting of a personal data breach.

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

6.1 Article 5(1) of the GDPR provides for the principle of integrity and confidentiality and requires that personal data shall be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

6.2 Article 32(1) of the GDPR particularises the requirement in Article 5(1) to provide for security of processing:

"1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) the pseudonymisation and encryption of personal data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."

6.3 As provided for in Article 32 of the GDPR in considering the technical and organisational measures that a controller or processor must implement, regard must be had to a risk assessment concerning the rights and freedoms of natural persons, the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing.

6.4 The Council is the professional standards body for the teaching profession, which promotes and regulates professional standards in teaching. The primary role of the Council is the registration, re-registration and vetting of teachers in Ireland. The Council also provides a number of educational and personal supports to teachers. The Council's functions result in a limited scope of personal data being processed by the Council. However, the sensitivity of some of the personal data being processed as a result of the necessity to carry out Garda vetting, including the recording of convictions or potential prosecutions, heightens the risk to the rights and freedoms of data subjects, in this case the relevant teachers. It is important to note that the spreadsheets containing vetting status information, the subject matter of this incident, did not contain vetting disclosures or criminal conviction data. The registration process of teachers is done by way of a secure registration database with access controls which was not compromised by the phishing attack.

6.5 Teachers register with the Council for the first time by completing a paper application form and submitting it by post to the Council. Once received, the information contained on the form is entered into the Council's Registration Database, Database 1, by a member of the Council's registration team. All teachers must be Garda vetted before gaining access to the register as part of the initial registration process. All teachers must renew

their registration annually. The Council may seek a vetting disclosure as part of a teacher's registration renewal, and have recently made the decision to seek a vetting disclosure for registered teachers approximately every three years. However, registered teachers applying for re-vetting, may email the signed form and identification to the Council rather than submit it by post. The Council also acts as a conduit between employers and potential employers and the National Vetting Bureau ("**The NVB**") and facilitates applications for vetting disclosures being made. This is separate and distinct from vetting disclosures being sought for the purposes of the Council's own registration or renewal process.

6.6 As has been detailed in Section 3 of this decision, as part of the successful phishing campaign on two email accounts of Council staff, over 323 emails were forwarded to an external Gmail account, by a malicious actor. One of the emails identified as being forwarded to the Gmail account was a spreadsheet containing the vetting status details of almost 10,000 teachers. The Council was asked to provide information on this spreadsheet, including details as to whom and from whom this spreadsheet was being sent and for what purpose. The Council submitted that the spreadsheet was an excel spreadsheet which was generated as a report from Database 1 by an IT database administrator responsible for data compilation and the generation of reports. The Council further submitted that this report could not have been generated by any member of staff. The report was generated for the purposes of informing a list of teachers that they were required to be vetted prior to that year's registration renewal, as part of the Council seeking a vetting disclosure for registered teachers approximately every three years. The Council stated that the excel spreadsheet was generated using specific criteria from the Database1. The Council submitted that the data required to generate the list of teachers contained on Database 1 included the date of the teacher's last vetting, their registration renewal dates, their addresses, and unique identifiers such as PPS numbers and Teaching Council registration numbers. Once the report was generated in the form of the excel spreadsheet the staff member who had generated it emailed it to his colleague, a Council NVB Liaison Person.

6.7 The personal data recorded in the spreadsheet consisted of: Registration Number, Name, Vetting Clearance Date, Vetting Clearance Name, Vetting Clearance Reference, NVB Status Date, NVB Reference Number, Address, PPS Number, Join Month, Renewal Date and Status Code. Within the spreadsheet four categories existed and the Council have submitted that the spreadsheet could be filtered on this basis. The labels and details of the four categories of vetting status were provided to the DPC. To be clear, the term "*vetting status details*" (which is referred to throughout this Decision) denotes basic details regarding the vetting of a teacher, i.e., when (s)he has most recently been vetted, what label has been attached to them and certain internal/external reference numbers. It does not contain any vetting disclosures, information within them, or criminal conviction data. The Council submitted, in submissions dated 3 September 2021, that if the terms were named in this decision it may alert those responsible for the cyber-attack to the meaning of the terms, as the terms are unique to Council staff and as of now would only be understood by the registration and vetting team of the Council. I have therefore

chosen not to name the categories on that basis. The Council have submitted that, according to its analysis of the approximately 10,000 teachers listed on the spreadsheet only 13 teachers were recorded as "Label 1" and two were listed as "Label 2".

6.8 The DPC requested a response from the Council as to why a shared drive was not in use to access the required information, rather than an excel spreadsheet being generated by one staff member and sent to another via email. The Council did not provide an explanation as to why a shared drive was not in use at the time of the breach. In response to the query, the Council stated only that the Acceptable Usage Policy ('**AUP**') in place at the time of the breach contained a section on password usage, but only in respect of the circulation of external documents. The spreadsheet which was generated was therefore sent unencrypted and without password protection over an inadequately secured email system, which had allowed the creation of forwarding rules. The Council detailed a number of updates which have been made to the AUP since the breach, which will be discussed later in this Decision.

i. Assessing Risk

6.9 The processing of personal data by the Council, including the transfer of personal data by email, creates the risk that unauthorised third parties may gain access to the data. This may arise either because of an inadvertent misdirection of an email to the wrong recipient or it may occur, as in the present case, where the email user falls prey to a phishing attack. The technical and organisational measures implemented must be appropriate to this risk.

6.10 Recital 76 of the GDPR provides guidance as to how risk should be evaluated:

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

6.11 *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources and others*[2] provides further guidance on this risk assessment. In this case, the CJEU declared the Data Retention Directive[3] invalid. The Directive required electronic communication service providers to retain certain data for a period of time. The Court held that the directive did not ensure effective protection of the data retained against the risk of abuse and unlawful access in circumstances where it did not lay down specific rules in relation to (i) the vast quantity of data retained, (ii) the sensitive nature of the data, and (iii) the risk of unlawful access.

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

6.12 Risk is assessed objectively by reference to (i) the likelihood of the risk to the rights and freedoms of natural persons, and (ii) the severity of that risk. A risk assessment should consider, first, the likelihood of unauthorised access to the Council's email accounts, and, second, the severity of that risk in respect of the rights and freedoms of the data subjects. These objective assessments are made by reference to the nature, scope, context and purposes of the processing. In considering these factors, regard must also be had to the quantity of personal data processed and the sensitivity of that data. The Council have submitted that in 2016 a named external information security services provider conducted a Personal Data Security Assessment and reviewed a number of assets as part of a risk assessment.

6.13 Submissions made by the Council demonstrate that, at the time of the breach, a high quantity of personal data was being processed on the Council's email accounts and that transfers of personal data between staff members via email were taking place as part of ordinary workplace practices. This is most particularly illustrated in circumstances where the aforementioned vetting status details of almost 10,000 teachers were sent via email from one staff member to another. In this instance a staff member ran a report in Database 1 and sent it to a colleague by way of an excel spreadsheet, by email. This information was sent unencrypted, as the Council's AUP at the time of the breach stated that only data that was being sent externally had to be encrypted or password protected. Therefore the risk of the data being unlawfully accessed by way of misdirected email or phishing attack was at all times high. It is noted that the Council stored vetting information on Database 1 a secure oracle database which was not compromised as part of the phishing attack. Having drawn down a report from the database, it was put into an unencrypted excel spreadsheet and sent via an inadequately secured email system. If the data contained therein is going to be sent by inadequately secured means this negates the use of the secure Database 1.

6.14 Analysis of the 323 emails sent to the external Gmail account also identified the forwarding of an email containing the sensitive data of one named data subject, namely information on a criminal conviction and former drug use. This was an isolated disclosure of criminal conviction data as part of the phishing attack. The personal data of the data subject in question is by its very nature particularly sensitive with regard to their fundamental rights and freedoms. I am also cognisant of the risk of fraud and identity theft to the almost 10,000 data subjects whose personal data, including PPS numbers, was contained in the spreadsheet. The nature of the personal data processed through the Council's email accounts varies on the scale of sensitivity. It is noted that the majority of emails sent to the malicious Gmail account were low-risk and did not contain personal data or special category data.

6.15 Exacerbating the Council's transfer of personal data via email is the fact that the email system in use by the Council at the time of the breach was not appropriately secured. Auto forwarding rules to external addresses on the user side had not been restricted, which permitted the setting up of the auto forward rule by the phisher. In the submission in response to the draft Inquiry Report, dated 30 October 2020, the Council stated:

"*Furthermore, it is not standard practice for general IT managers to disable the auto-forward rule. Of course, this may have been something that an IT security expert would have been aware of however the standard that the Teaching Council should in our submission, be held to is the reasonable standards test, and not that of a security expert. The Teaching Council submits that its levels of security is similar to other comparable bodies…"*

The DPC does not agree with the submissions of the Teaching Council. The GDPR obliges data controllers to implement organisational and technical measures commensurate with the risks inherent in the personal data processing operations in which that specific controller is engaged. Each organisation has a different risk profile in terms of their personal data processing operations and it is incorrect to assert here that the DPC is holding the Teaching Council to an unreasonable standard in expecting it to implement measures to prevent personal data loss.

6.16 At the time of the breach the Council was using a free version of Microsoft Office 365 A1 License which does not permit the rollout of certain recommended functionality in Office 365 which would provide additional security measures and assist to promptly identify security and data breaches. In particular, the Council did not have Advanced Threat Protection ('ATP') enabled in Office 365 due to licensing issues, which provides tools to identify and mitigate against malicious threats posed by email messages and URL links. The Council have stated, in submissions dated 3 September 2021 that "*even with ATP, phishing emails can get through*". However, despite the fact phishing emails may still get through if ATP is in place, there is still a requirement to implement it. The Council have also submitted, in the same submissions, that the vulnerability was exposed by human error, i.e., "*falling for a phishing attack.*" The DPC's position is that the GDPR requires implementation of technical and organisational measures that as far as practicable account for human error. The A1 license is a free version of Microsoft 365 provided to students and educators at eligible institutions. The Council have submitted in the same submissions that the A1 licence does contain threat management tools as standard. Specifically, default alerts for the creation of forwarding/redirect rules; and user restrictions on sending emails. The Council have also submitted that it spends significant budget on Microsoft server licensing.

ii. Security Measures Implemented by the Council

6.17 The Council made submissions throughout the Inquiry detailing the technical and organisational measures implemented at the time of the personal data breaches to provide for the security of its email service. The Council also made submissions on the steps that it has taken since the personal data breaches to enhance security. This Decision considers the level of security implemented at the time of the breach. Therefore, the measures implemented since the breach are not relevant to determining whether an infringement of

Articles 5(1) or 32(1) occurred at the time of the breach. However, Part 8 of this Decision details how these measures are relevant to the issue of corrective powers.

6.18 The DPC asked the Council a range of questions as to the security measures which were in place at the time of the breach, specifically the Council was asked to provide information as to what measures were in place to comply with Article 32 GDPR and Article 5(1).

6.19 The Council was asked to provide details as to the risk assessment that was in place at the time of the breach, the appropriate technical and organisational measures in place to counter those risks, the capability of the Council to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services and the processes in place for the regular testing, assessment and evaluation of the effectiveness of the technical and organisation measures for ensuring the security of processing.

6.20 The Council, in submissions dated 3 September 2021, have submitted that a Personal Data Security Assessment was carried out in 2016 by an external information security services provider. As part of this risk assessment the Council stated the following assets were reviewed:

(a) Oracle DB for Teachers registration (i.e. the registration database)
(b) Exchange Server
(c) Network drive shares, various files and folders
(d) Information stored in ETB
(e) Back Up Tapes in Iron Mountain
(f) Physical filing cabinets
(g) Committee and Panel Consideration files
(h) External hard drives
(i) Mobile devices
(j) APIs
(k) Offsite storage of files
(l) Department of Education, paymaster files
(m) Revenue servers
(n) SharePoint
(o) Printers

6.21 In response to the other details sought the Council stated:

"The measures in place at the time of the breach were as follows:

- *The Teaching Council was using Microsoft Office 365 and Outlook in order to have a solution which provides a number of security settings and tools to provide security measures.*
- *The Teaching Council engaged a third-party ICT Managed Service provider to provide additional expertise and monitoring for their in-house ICT team. This ensures that the*

Teaching Council has resources to ensure the delivery of the required measures. Consultancy 1 is ISO27001 certified and holds Certified Ethical Hacker accreditation.

- *The Teaching Council engages independent third parties to provide security assessments and tests on a regular basis. For example, an ICT security review was carried out in 2019 which focused on Level 2 Wireless and Infrastructure Penetration Test and was conducted by an external third party.*
- *The Teaching Council has a detailed Acceptable Usage Policy (which includes a section on password protection) and Information Security Policy in place.*
- *Staff are sent notifications to alert them to potential phishing scams.*
- *The Teaching Council has a detailed Record of Processing Activities (Article 30 Record) in place which includes details of the personal data processing [sic] which may undergo processing by the Teaching Council. A copy of the relevant extract from the Article 30 Record was provided to your offices on 27 March 2020.*
- *The Teaching Council has a documented data retention policy in place, a copy of which has already been provided to your offices.*
- *A Data Protection Officer (DPO) was in place and has been in place for a number of years.*
- *The Teaching Council is part of the secure e-Gov network.*
- *All servers are patched with the latest security patches on a monthly and quarterly basis.*
- *All servers are patched, monitored and scanned using the latest recommended Anti-Virus from ICT Managed Services.*
- *Cisco Firewalls in Maynooth and Revenue Data Centre (where the Teaching Council's servers are hosted) has Firepower restrictions enabled.*
- *Symantec Anti-Virus server installed that manages all internal desktops and push out latest patches.*
- *Email filtering was enabled on the Microsoft Office 365 security platform to block or quarantine potential spam emails.*
- *User list enabled to inform users on secondary blocked email if needed.*
- *Standard Office 365 alerts.*
- *In-built Spam, Malware and Phishing email filtering.*
- *OWA, Active Sync and Mobile Sync disabled for staff that do not need it. New Mobile Sync using Outlook are quarantined and only allowed by an administrator*
- *Web filtering enabled on the Firewall on the Teaching Council network.*
- *Strict administrator access to prevent any software installations or downloads on users' desktops.*
- *USB and storage devices are disabled in the Teaching Council.*
- *Role based access for email and network shares is in place.*
- *System Access Request form for requesting/ removing access to email requiring authorisation from management in the department/ area.*
- *GDPR training provided to staff."*

6.22 The Council outlined the measures it had in place at the time of the breach to prevent or detect malicious or abnormal access to the Council's email system:

- *Exchange Online Protection enabled (Same protection we used for on-premise Exchange before Office365)*
- *Inbound and Outbound Spam, Malware, connection filter, quarantine enabled.*
- *Office365 alerts enabled for suspicious activity*
- *Security and Compliance Centre enabled*
- *Blocked email and domain lists enabled*
- *Staff notification for quarantine emails*
- *Exchange rule enabled*
- *Symantec Anti-Virus on all desktops*
- *OWA and Mobile sync not enabled for all staff*

6.23 However, in spite of the measures as detailed by the Council above, the breach still occurred. The Council stated in submissions that following the breach it had engaged the services of a cyber-security company to carry out a security review of the incident, which resulted in a number of recommendations.

6.24 It is of serious concern that the Council had a practice of transferring unencrypted personal data between staff members via email, and that the AUP in place at the time of the breach contained a section on password usage, but only in respect of external documents. The Council, in submissions dated 3 September 2021, has stated it is unclear to it how I have reached the conclusion that the Council had a 'practice' of transferring personal data in this way. Where the Council has given no alternative method for the transfer of this type of information, where it has not said that this particular transfer of information was done on the date in question in this way as an isolated event, and furthermore where the Council has not in fact in its submissions refuted my conclusion that it had a practice of transferring personal data between staff in this way, I have reached a conclusion that the Council had a practice of doing so.

6.25 It is of note that the Microsoft Office 365 A1 License in use by the Council at the time of the breach does not permit the rollout of certain recommended functionality in Office 365 which would provide additional security measures and assist prompt identification of security and data breaches. In particular, the Council did not have Advanced Threat Protection ('ATP') enabled in Office 365 due to licensing issues, which provides tools to identify and mitigate against malicious threats posed by email messages and URL links. The Council, in submissions dated 3 September 2021, have submitted while the A1 license in use did not have ATP that "*even with ATP, phishing emails can get through*". As stated above, although phishing emails may be received even when ATP is in place, this does not mean that there is not a requirement to implement it as part of an adequately secured email system. The A1 license is a free version of Microsoft 365 provided to students and educators at eligible institutions. The Council, in the same submissions, have stated that:

"*The Draft Decision gives the unfair impression that the Teaching Council purposefully put in place a licence that was free in order to reduce IT spend. This is not the case. The A1 licence*

is a license that educational bodies qualify for at no additional cost. As an education body, the Teaching Council qualified for the A1 licence."

6.26 However, the free licensed version of Microsoft 365 (A1) being utilised by the Council did not provide a level of security appropriate to the risk associated with the type of personal data it processes in its role as a professional standards body. Furthermore, at the time of the breach, users in the Council had system privileges sufficient to allow them to set forwarding rules to external email addresses, which is how the breach occurred. In its submission on 17 June 2020 the Council stated that "*Outlook did not advise user of the forward that was in place*." The restriction of such privileges is a key element in reducing the risk that arises from a successful phishing attack. The Council also stated that one user's machine was running Outlook 2013 as part of the Microsoft Office 2013 suite, and that the recommendation was that the Council would update all users to the latest 2016 version.

iii. The Appropriate Level of Security

6.27 As per the provisions of Article 5(1)(f) and Article 32(1) of the GDPR, I have considered whether data being processed by the Council at the time of the breach is being processed in a manner that ensures appropriate security of that data, including protection against unauthorised processing and against accidental loss, destruction or damage using appropriate technical or organisational measures. I have also considered the nature, scope, context and purposes of the processing; the cost of implementation; and the state of the art. Furthermore, I have considered the risk to the rights and freedoms of the data subjects. I find that the Council failed to implement appropriate organisational and technical measures to provide security to the personal data being processed.

6.28 With reference to the Council's use of unencrypted, non-password protected, excel spreadsheets to download and transfer personal data I find that the Council has failed to comply with the pseudonymisation and encryption of personal data mitigation safeguards of Article 32(1)(a) of the GDPR. I find that the Council failed to ensure the ongoing confidentiality, integrity and resilience of its processing systems and services in accordance with Article 32(1)(b) in circumstances where the Council did not have an adequately secure email system, in which auto forwarding rules should have been restricted which would have prevented the successful hacker forwarding personal data to the external Gmail account. The Council have stated, in submissions dated 3 September 2021, that they do not accept the provisional finding made in the Draft Decision that the Council did not have a secure email system in place, however my finding based on the facts in this matter, stands. I find that the Council failed to regularly assess and evaluate the effectiveness of technical and organisational measures for ensuring the security of the processing of personal data, in accordance with Article 32(1)(d).The Council have stated, in submissions dated 3 September, that a DPIA was conducted by a named security services provider in 2016. However, this is not evidence of a regular review of processes and it is noted that this was conducted four years prior to the data breach the subject of this decision. Such assessment and evaluation should have identified the serious risk of unauthorised disclosure of, or access to, personal data being downloaded to an unencrypted excel spreadsheet and sent by email between staff

members. Further, I find that data processed by the Council was not done in a manner which ensured the appropriate security of the data in accordance with Article 5(1)(f) of the GDPR, in circumstances where emails containing personal data, including sensitive data, were sent to the external Gmail account. I find that wheresoever possible the Council should not send sensitive personal data via email.

6.29 I have considered the nature, scope, context and purposes of the processing of personal data by the Council, in accordance with Article 32(1) of the GDPR. I note that the data being processed is limited in scope and is being processed for the purposes of registering and establishing the vetting status of teachers in the State. I note that as part of the vetting status process it is necessary for the Council to process sensitive data concerning data subjects, and that this is unavoidable given the nature of the work teachers are employed to carry out in working with children. However, I am also cognisant of the risk to the rights and freedoms of data subjects should this information be accidentally or unlawfully disclosed. I find that the risk of sensitive data being unlawfully disclosed is high given the organisational and technical measures in place at the time of the breach.

6.30 The Council have stated, in submissions dated 3 September 2021, that:

"*…the scope of the Inquiry appears to have been broadened, either intentionally or inadvertently, to include the Teaching Council's entire end-to-end registration and vetting process*.

The subject matter of the Inquiry is the disclosure of emails as a result of a phishing attack via Microsoft Office 365."

This is incorrect. The Inquiry report stated, as outlined in the Commencement Letter dated 2 April 2020, that the following areas would be considered as part of the scope of the Inquiry, at 1:

"*Security of personal data – An examination of the Council's compliance with Articles 5(1) and 32(1) of the GDPR with regard to the technical and organisational measures in place to ensure that there is adequate security over personal data held in manual or electronic form*."

6.31 I have considered the state of the art and the costs of implementation in accordance with Article 32(1). I note the Council's submissions on the security measures in place by the Council at the time of the breach, however I find that the Council has failed in its obligation to ensure appropriate organisational and technical measures where the state of the art is significantly more advanced than the systems in use by the Council at the time of the breach. I acknowledge that perfect security is not the standard set by the GDPR and that, in considering whether there has been an infringement, I must avoid reasoning purely with the benefit of hindsight. Rather, controllers are required to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. I note that the Council are a professional standards body and that newly qualified teachers cost of registration is €90 per year, while the cost of annual registration renewal is €65. I find that

the costs of implementation of the below findings are not unduly onerous and were appropriate in the circumstances at the time of the personal data breach, especially where the risk to the rights and freedoms of data subjects is high where sensitive personal data is being processed by the Council.

6.32 On the basis of the above findings I find that an appropriate level of security includes the following technical and organisational measures in the circumstances. I find that where the Council have a centralised Teaching Council Registration Database- Database 1, that staff members receive training to generate reports from this database to remove any possibility of excel spreadsheets being emailed between staff members. Where this is not possible I find that the Council's procedures and policies must provide that, if such spreadsheets are to be generated, that they would be password protected and stored on a shared drive, with limited access rights. I find that the Council's procedures and policies must provide that the Council should not, except in exceptional and unavoidable circumstances, transfer personal data by way of email between staff members. In such unavoidable circumstances I find that this personal data should be encrypted and password protected both for internal and external document sharing. I find that the Council should review its risk assessment on an annual basis as to its processing of personal data. I note that additional security measures may be required for the processing of sensitive personal data. The manner in which sensitive personal data was transferred by email between staff members, including in one specific instance a small number of emails which detailed the criminal convictions of one data subject, does not meet the appropriate level of security and I find that an appropriate level of security requires that such personal data must be protected by password protected email archiving or other secure filing systems.

6.33 Having regard to the likelihood and severity of the risk of unauthorised access to the Council's email accounts by way of the technical and organisational measures in place at the time of the breach, I find that an appropriate level of security includes the implementation of 2FA (two factor authentication) in Office 365 for all users. This will require the Council to change from the A1 license in use at the time of the breach. I also find that all Legacy Authentication protocols in Office 365 should be disabled for all users.

6.34 I find that the Council should implement Advanced Threat Protection (ATP) in Office 365. This will also require a change in licensing for the Council. I find that the Council should mandate annual data protection and cyber security training for all staff. This measure should assist users in identifying emails from malicious actors and require them to report any such emails to IT staff. This is in circumstances where the Consultancy 1 Report, commissioned by the Council, opined that both users were phished as part of a phishing campaign where users entered their passwords online and stated:

"It should be noted that both users have stated that [they] did not enter their password. This would be expected as they would have perceived this to be normal activity and an advanced phishing campaign would capture details without the user being aware"

I note the Council's submissions, dated 3 September 2021, state ATP has been implemented for all staff and that all staff have attended mandatory data protection and cyber training which was conducted in 2020 and will be renewed in 2021 and annually going forward.

6.35 I have considered the security measures that the Council implemented at the time of the breach; the nature, scope, context and purposes of that processing; the cost of implementation; and the state of the art. I acknowledge the security measures in place in the Council at the time of the breach and have taken account of these factors in Section 8 of this Decision. However, I find that the Council failed to implement appropriate organisational and technical measures to ensure the security of personal data

6.36 I have had regard to the cost of implementing organisational and technical measures for the purposes of ensuring the appropriate level of security of personal data. I find that implementing such measures, for example by paying Office 365 license fees appropriate to the level of a professional standards body such as the Council, would not impose a disproportionate cost on Council with regard to its obligation to implement a level of security appropriate to the risk presented. However, it should be noted that implementing such specific guidance does not relieve the Council of its obligation to continually evaluate the measures that are necessary to ensure a level of security that is appropriate to the level of risk presented by being in possession of over 100,000 data subjects' personal data.

iv. Finding

6.37 I find that the Council infringed Article 5(1) and Article 32(1) of the GDPR between 25 May 2018, when the GDPR came into application, and the dates of the personal data breaches, by failing to process personal data in a manner that ensured the appropriate security of the personal data using appropriate technical and organisational measures.

7. Issue 2: Article 33(1)

i. The Obligation to Notify Without Delay

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

'In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural

persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.'

7.2 Under Article 4(12), a personal data breach

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

7.3 Article 33(1) requires that notifications must occur without undue delay. The Article 29 Working Party (now the EDPB) addressed the meaning of the term 'undue delay' in the context of the requirement to communicate a breach to affected individuals in its '*Guidelines on Personal Data Breach Notification under Regulation 2016'*. The Guidelines outline that:

"*The GDPR states that communication of a breach to individuals should be made "without undue delay," which means as soon as possible. The main objective of notification to individuals is to provide specific information about steps they should take to protect themselves."*[4]

7.4 The Article 29 Working Party Guidelines on Personal Data Breach Notification under Regulation 2016/679[5] 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>*."[6]
(Emphasis added)

7.5 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

[4] Page 20
[5] Article 29 Working Party, Guidelines on Personal Data breach notification under Regulation 2016/679, Adopted 6 February 2018.
[6] Breach Notification Guidelines, page 11

incident to determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required."[7]

7.6 The Guidelines further state:

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". However, it is expected that the Initial investigation should begin as soon as possible and establish with a reasonable degree of certainty whether a breach has taken place; a more detailed investigation can then follow.[8]

7.7 The importance of being able to identify a breach, assess the risk to individuals and notify it promptly is emphasised in Recital 85, which provides that:

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons…"[9]

In this respect, the issue of 'awareness', and its role in terms of defining the timeframe within which notification is required to take place, must be understood in the context of the broader obligation on a controller to ensure that it has appropriate measures in place to facilitate such 'awareness'.

7.8 Recital 87 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*."

7.9 The Breach Notification Guidelines state that:

[7] Ibid at 11.
[8] Ibid, page 11
[9] The Article 29 Working Party (now the EDPB) addressed the meaning of the term 'undue delay' in the context of the requirement to communicate a breach to affected individuals in its 'Guidelines on Personal Data Breach Notification under Regulation 2016/679 (Adopted on 3 October 2017; As last Revised and Adopted on 6 February 2018)'. In this regard, the Guidelines outline on page 20 that "*The GDPR states that communication of a breach to individuals should be made "without undue delay," which means as soon as possible. The main objective of notification to individuals is to provide specific information about steps they should take to protect themselves."*

"*…the 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."*[10]

7.10 In considering whether the Council complied with its obligation to notify a personal data breach under Article 33(1), therefore, I have considered the objectives underlying this obligation and the broader context in which this obligation arises. At this point, I note that, in its submissions in relation to the Draft Decision dated 3 September 2021, the Council raised objections to the interpretative approach which was outlined in the Draft Decision with regard to the meaning and effect of Article 33(1). I consider the Council's position on this issue below.

7.11 In order to ensure that controller responsibility for the processing of personal data is applied more effectively, the principle of *accountability* was specifically incorporated, as a central principle, into the GDPR. While the principle of accountability was expressly enunciated in the text of the GDPR, the principle was already established in EU data protection law prior to the application of the GDPR.

7.12 In this regard, the Article 29 Working Party in its *Opinion on the principle of accountability*[11] outlined that the purpose of including an accountability principle, within a legislative framework, would be to "*…reaffirm and strengthen the responsibility of controllers towards the processing of personal data…"* and further stated that such a provision would focus on two elements, being "*the need for a controller to take appropriate and effective measures to implement data protection principles"* and *the need to demonstrate upon request that appropriate and effective measures have been taken*…"[12]

7.13 In terms of what is meant by the principle of 'accountability', the Article 29 Working Party also stated that "*In general terms…its emphasis is on showing how responsibility is exercised and making this verifiable. Responsibility and accountability are two sides of the same coin and both essential elements of good governance."*[13] In a similar vein, the European Data Protection Supervisor (EDPS), in its guidelines on accountability, states

[10] Breach Notification Guidelines, page 6
[11] Article 29 Data Protection Working Party 'Opinion 3/2010 on the principle of accountability', Page 8
[12] Ibid, pages 8 and 9
[13] Ibid, page 7

that "[*a*]*ccountability means that the controller is in charge of ensuring compliance and being able to demonstrate compliance*."[14]

7.14 In the GDPR, the issue of controller accountability is specifically addressed in Article 5(2) and Recital 74. Recital 74, in this regard, provides that:

"*The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures*."[15]

Article 5(2) then places overall responsibility for compliance with the accountability principle on the controller, stating, in this regard, that the controller shall be responsible for compliance with the data protection principles set out in Article 5(1), and in addition, that the controller shall be able to demonstrate such compliance.

7.15 Article 25 ('*Data Protection by Design and by Default*') then imposes an obligation on a controller to ensure that it has *appropriate* technical and organizational measures in place that are designed to implement the data protection principles in Article 5. The EDPB has considered the meaning of the term '*appropriate*' in the context of Article 25 of the GDPR in its *Guidelines on Article 25 Data Protection by Design and by Default.* In this regard, the EDPB has stated that, in order to be 'appropriate', the technical and organizational measures applied by a controller must be:

"*…suited to achieve the intended purpose, i.e. they must implement the data protection principles effectively. The requirement to appropriateness is thus closely related to the requirement of effectiveness."*[16]

"*…suited to achieve the intended purpose, i.e. they must implement the data protection principles effectively. The requirement to appropriateness is thus closely related to the requirement of effectiveness."*[17]

ii. The Breach Notification

7.16 The Council notified the DPC of the data breach on 9 March 2020. In breach notification BN-20-03-399 the Council advised that:

[14] EDPS, 'Accountability on the Ground: Guidance on Documenting Processing Operations for EU Institutions, Bodies and Agencies (v 1.3 July 2019) Section 3
[15] Recital 74 GDPR
[16] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (13 Nov 2019), page 6
[17] Ibid, page 6

"A phishing email was received by two members of staff in the Council and was accessed. This caused a script to be activated that established an auto forwarding rule for all subsequent emails being sent to the two individuals to an external Gmail account. In total, 323 email messages were forwarded to the external Gmail account and these were issued from one user from 17 February 2020 to 6 March 2020 and from the other user from 4 March 2020 to 6 March 2020."

The IT team in the Council first received notification of a security alert on 17 February 2020 when an email alert was received to the account of *nameduser1.* It now falls for me as decision maker to determine whether the time between the first security alert received by the Council on 17 February 2020, until the notification of data breach to the DPC on 9 March 2020, constitutes compliance with Article 33(1) and was a period during which the Council ought to have been aware of a personal data breach.

7.17 The first security alert received by the Council on 17 February 2020 had the subject:

"*Low-severity alert: Creation of forwarding/redirect rule*"

the content of which stated:

"MailRedirect. This alert is triggered when someone gets access to read your user's email".

The Council have submitted that the steps it undertook to investigate this alert were:

"*A number of steps were taken to investigate why a low severity alert was received including running Anti-Virus scans on the user's PC and checking the Global forward rules in the Exchange Administrator portal in Office 365. As no evidence of malware or virus was discovered on the user's desktop the IT personnel considered the alert to be a false alert. The Outlook client or user's OWA personal access was not checked on this date."*

7.18 It is of note that despite the explicit subject line and contents of the security alert received, the Council did not examine at that time the Outlook clients or user's OWA personal access to examine whether a rule or redirect had been put in place, nor did it examine the "Exchange Admin Center" for user created inbox rules. It is also of note that having taken "*a number of steps*" to investigate the security alert and finding no cause for it, the IT team simply concluded it was a false alarm, without any further investigation to support this view. In this way, the Council did not implement all appropriate technological protection and organisational measures to establish immediately if a breach had taken place to ensure that it was "*aware*" of any breaches in a timely manner as per the Working Party Guidelines. The failure to investigate whether a redirect or forwarding rule had been created continued in circumstances where the second security alert received on 19 February 2020 indicated "*potential compromised activity*", and the third security alert stated that "*This alert is triggered whenever someone gets access to read your user's email.*" It is of serious concern that despite receiving three different

alerts indicating a security alert, that only when the fourth security alert was received did:

"*A member of the IT Team suggested to check the Outlook rule on the user's desktop. This had not been done previously*."

7.19 The above action resulted in the discovery of the rule on the second account for which security alerts had been received, the *nameduser2* account. This then:

"…prompted the checking of the account for nameduser1 due to the similarity in the alert, where a similar auto forward rule was discovered and straight away removed from that Outlook client account on 6 March."

7.20 On 6 March 2020, when the auto-forward had been discovered, IT staff spoke to Named User 1 and:

"*The user confirmed to IT on 6 March that she had not set up the auto-forward rule and she did not recognise the Gmail account. She also informed IT that she clicked on a potential spam link and attachment a few days earlier without realising. When the IT personnel were informed of this on 6 March, it became apparent to them that this triggered the auto-forward on her Outlook Client."*

7.21 It of note that Named User 1 had not been questioned when she received the first security alert to her email account. It is my view Named User 1 should have been asked if she had received any spam mail, suspicious mail, or mail from an account she did not recognise, and whether she had clicked on any attachments as a result. That the above memory was triggered in the staff member only after the discovery of the auto forwarding rule appears to demonstrate that at no time was she questioned about the security alert. This has not been disputed by the Council, in submissions dated 3 September 2021, in response to the Draft Decision.

7.22 The Council have submitted repeatedly, in submissions dated 3 September 2021, that the DPO was informed of the security alerts and data breach only on 6 March 2020. Article 33 requires a controller to notify the supervisory authority when aware of the breach. When the DPO became aware of the breach is immaterial. What is in issue is that the Council ought to have been aware of the data breach if it had used all appropriate technological and organisational measures to establish the cause of the initial, second and third security alerts as it was obliged to do.

7.23 It is noted that when the first security alert was received the Council undertook significant, although incomplete, steps to identify the cause of the alert on that date. Council IT staff changed the password for the account, checked the global email forwarding rules and conducted an antivirus scan on the user's PC. It is my view that these actions demonstrate that the Council ought to have been aware of a potential serious security breach but chose not to investigate the alert any further and incorrectly

concluded it was a false alarm. I also find that the Council was aware that personal data was being processed on its email accounts, or ought to have been aware in accordance with its responsibilities as a controller pursuant to Article 32(1). Further, the Council ought to have been aware that the version of software it was deploying permitted auto-forwarding rules to external accounts to be set by users on their email accounts. I therefore find that the Council ought to have been aware that the security breach could lead to the accidental or unlawful destruction, loss or disclosure of personal data, as per Article 4(12) of the GDPR. Therefore, it is my view that the Council ought to have been aware of a security breach for the purposes of Article 33 GDPR when it received the first security alert, on 17 February 2020. The Council has stated, in submissions dated 3 September 2021, that "*the obligation under Article 33(1) is to report a data breach and not a potential breach or a potential security incident*." This is correct, however, as above the Council were under an obligation to ensure that it was "*aware*" of any breaches in a timely manner. It is of note that the Council in its submissions state that it had sufficient security systems in place to be in compliance with the GDPR. However these security systems are of no protection to personal data and the rights and freedoms of data subjects if, when such alert is received, the Council do not adequately investigate and identify the exact cause of the alert.

7.24 The Council have submitted that it only became aware of the data breach when a member of the IT staff suggested to check the Outlook rule on the user's desktop, on 6 March 2020. The DPC cannot conceive of a situation where a data controller, despite being aware of an explicit security breach on an email system which processes unencrypted and un-password protected personal data in accordance with the Council's AUP, and having failed in its duty to adequately identify in within a reasonable period of time the cause of the data breach despite the security alerts explicitly stating that a forwarding rule had been created, would be permitted to rely on such failure to avoid being found in breach of Article 33(1) of the GDPR as to when it became "*aware"* of a personal data breach.

7.25 It is my view that the Council upon receipt of a high security alert for the same account, on 19 February 2020, the subject of which stated:

"*High-severity alert: User restricted from sending email*"

and the content of which stated:

"*User nameduser1@teachingcouncil.ie has been restricted from sending messages outside the organization due to potential compromised activity*"

again ought to have been aware of a personal data breach in circumstances where a repeated, specific, security alert was received on the same email account which processed personal data, including personal data contained in the user's Inbox, Sent Items, and the emails they continued to send warning of compromised activity. Again the

Council undertook extensive antivirus scans but failed to undertake all appropriate and reasonable measures by checking the forwarding rules on the account.

7.26 In submissions, dated 31 July 2020, the Council state that:

"We feel it is important to conclude by saying that appropriate and reasonable measures were taken in the investigations of 17 and 19 February and 4 March. It is only on 6 March 2020 that the auto forward rule was discovered and the obligation to consider whether a report to the DPC was required was triggered."

7.27 In submissions, dated 3 September 2021, the Council state that:

"*It is clear that Article 33(1) imposes a duty on a data controller that has actually become aware of a breach. It follows that the duty does not fall on a data controller that is unaware of the breach, even if it could be said that it should have been aware of it."*

7.28 The Council, in the same submissions, also state:

"*…the Teaching Council checked its systems once it received the automated alerts and concluded (incorrectly) that there had been no "intrusion into its network" and consequently no security incident. If the finding in the Draft Decision is correct then it would seem to follow that any data controller who incorrectly concludes that there has not been a security incident leading to a data breach and therefore does not make a notification will, in principle, have contravened Article 33(1)."*

7.29 The Council, again in the same submissions, state:

"*It is accepted that, in hindsight, had the Teaching Council checked the outlook rule on the user's desktop the security incident would have been uncovered*."

7.30 The acknowledged failure to check the outlook rule on the user's desktop is a failure of the Council's duty to implement all appropriate technological protection and organisational measures to establish the cause of the alert and a failure of the Council's obligation to ensure that it was "*aware*" of any breaches in a timely manner.

7.31 The Council, again in submissions dated 3 September 2021, submit that the DPC "*seeks to quite pointedly elide (sic) the concepts of a security alert, security breach and personal data breach*". In response , I note once again Article 4(12) which states that:

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

This is precisely what occurred in this case. The Council submit that:

"*It was only on foot of further steps taken on 6 March 2020 that it was determined with a reasonable degree of certainty that a security incident had occurred*."

7.32 The purpose of the GDPR is to ensure the protection of the fundamental privacy rights of Data Subjects and in that way Article 33(1) should be interpreted in a broader context. The Council have submitted that:

"*…the purpose of Article 33(1) is essentially procedural insofar as it imposes an obligation to report a specific category of breach (i.e. personal data breaches) in a timely fashion*."

7.33 This is not a correct interpretation of Article 33(1), which as stated earlier in this section, is not a stand-alone provision, but rather must be read and interpreted in conjunction with the GDPR as a whole and with the fundamental privacy rights of Data Subjects at the forefront.

7.34 In submissions, dated 3 September 2021, the Council submit:

"*In effect the Draft Decision regards a data controller that is unambiguously unaware of a personal data breach as being obliged to report same in accordance with Article 33(1) by reason of the fact that its lack of awareness is, of itself, culpable. Such an interpretation is incapable of achieving any useful purpose as it is wholly irrational to assume that punishing those who do not report personal data breaches of which they are unaware is likely to be of any utility."*

7.35 The Council also submit that:

"*…there was no process failure in this case. As confirmed by the DPC, the IT team carried out significant steps to investigate the alerts. On foot of those steps the potential security incident was deemed to be a false alert. As soon as the security incident was confirmed on 6 March 2020, the IT Team immediately notified the DPO. It is the date that the IT Team were put on notice of the auto forward of the incident and notified the DPO which is the relevant date for the purpose of determining the date of awareness."*

7.36 This is an incorrect interpretation of the Draft Decision and is contrary to the evidence at hand. The DPC is not attempting to fix data controllers, who *could not* have been aware of a security or data breach, with a date of knowledge of when a breach occurred where they could not have known that it had occurred. What the DPC is doing is obliging data controllers to undertake all appropriate and technological measures to investigate security incidents when notified of them and to notify the DPC within 72 hours of when they ought to have been aware of a data breach.

7.37 The Council did failed to appropriately investigate, failed to follow all appropriate steps and ignored the specifics of an alert when received. This was in circumstances where the first alert the IT team of the Council received was an email alert in Office 365 with the subject *Low-severity alert: Creation of forwarding/redirect rule,* and where there was a

clear process failure to investigate both the user and the server side to establish if forwarding rules had been put in place. This process failure and lack of sufficient investigation continued two days after the first alert on 19 February 2021 when the Council received the second alert and again did not undertake sufficient investigation to establish the cause of the alert, and again when the Council received the third alert on 4 March 2020.

7.38 What falls for my consideration, in respect of Article 33(1) of the GDPR is whether the Council complied with the obligation to:

'…not later than 72 hours after having become aware of the breach, notify the personal data breach to the supervisory authority…"

7.39 I find that the Council failed in its obligation to notify the DPC of the breach within the prescribed time period of when it ought to have been aware that a data breach had occurred. Controllers are not under an obligation to notify the DPC if the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. However, I am satisfied, on the basis of the above, that the personal data breach concerned in BN-20-03-399 did result in such a risk and find therefore that the Council was obliged to notify the DPC within 72 hours of when it ought to have been aware of the data breach. I find that the Council's submission that it:

"*did not know whether the security incident was reportable i.e. whether it was likely to result in a high risk to the rights and freedoms of individuals*"

does not justify not notifying the DPC of the personal data breach. The Council ought to have notified the DPC of each personal data breach as it occurred, and if it were not possible to provide the DPC with all information as to the details of the breach at that time, provide it at a later date. The Council, in submissions dated 3 September 2021, state that controllers are only obliged to report a data breach, and not a potential breach. While I agree with this contention, what is at issue in this matter is that the Council ought to have been aware of the breach if they had sufficient organisational and technical measures in place and if the IT team took all reasonable and appropriate steps to identify the cause of the repeated security alerts, rather than concluding, on three separate occasions, that the alerts being received were false alerts. I find that the Council ought to have reported the personal data breaches of 17 February 2020 and 4 March 2020, being the dates on which the auto-forward rules were set up, within 72 hours of each occurring. As set out above, the alternative, textual and formalistic approach to the interpretation of Article 33(1) being advanced by the Council would lead to absurd results, create perverse incentives, and contradict the clear aims of the EU Legislator when the GDPR is considered as a whole.

7.40 In breach notification BN-20-03-399, the Council assessed the risk of the breaches for affected individuals as a medium risk. At the time of the notification, the Council was

aware that 323 email messages had been forwarded to the external Gmail account. The Council stated that research was being undertaken to identify all affected data subjects at that time and that the number of affected records and affected individuals was unknown. The Council also stated that at that time it was unknown whether any of the emails sent to the external Gmail account contained any special categories of personal data. It is now known that a small number of emails related to special categories of data, namely the criminal convictions of one data subject.

7.41 It is appropriate to have regard to whether the personal data has come into the possession of individuals whose intentions are unknown or possibly malicious. In this regard, these breaches occurred due to phishing and resulted in suspicious logins to the affected email accounts from various locations globally. The personal data transmitted to the external Gmail account is unrecoverable. In the circumstances, I am satisfied that the personal data breaches resulted in damage and a risk to the rights and freedoms of data subjects, including, but not limited to, the ongoing risk of fraud and/or identity theft utilising the personal data maliciously obtained.

7.42 It is noted that the Council has submitted that to date no cases of fraud or identity theft have been reported to it and that on this basis it states that "*no evidence of any damage exists*". The Council also submits that I "*ha(ve) no jurisdiction to make a determination that damage was caused."* In this respect I would advise the Council to have due regard to Recital 85 which states:

"*A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data*…"

The loss of control of personal data has affected 9,735 data subjects in this matter, whose personal data was sent to a malicious email account as a result of the successful phishing attack the subject of this Decision.

7.43 The Council notified the DPC of the data breach on 9 March 2020. However, two separate personal data breaches occurred, both of which are connected to the successful phishing attempt by the malicious actor. These breaches took place on 17 February 2020 and 4 March 2020, the dates on which the auto-forward rules were set up on each of the affected user accounts. The Council provided the DPC with a spreadsheet detailing the emails which were forwarded to the malicious email account. This spreadsheet details that from the date of the first security alert, 17 February 2020, personal data was forwarded from a Council email account to the malicious email account. Therefore, the Council notified the DPC of the first breach three weeks after a personal data breach ought to have been detected and the second breach five days after it had been detected. The Council, in submissions dated 3 September 2021, have stated:

"*The Teaching Council also submits that it is incorrect to say that four separate breaches occurred. Four potential security alerts were received, the last of which was confirmed and identified as a security incident.*"

The DPC considers this is an inaccurate and incorrect interpretation of what occurred in this matter. The analysis of the emails sent to the malicious account provided by the Council to the DPC at the Inquiry stage of this process, detail that personal data was sent to the malicious account from the date of the first data breach, 17 February 2020 when the first auto-forward rule was set up Notably, the email containing the most sensitive personal data to be sent to the malicious account, containing the criminal convictions of one named data subject, was sent to the malicious account on 19 February 2020.

7.44 I find that all appropriate technological protection and organisational measures had not been implemented to establish within a reasonable period of time whether a personal data breach had taken place. The Council states that it failed to check for auto-forwarding rules on the client side of Office 365, when it received alerts on 17 February 2020, 19 February 2020 and 4 March 2020 and only investigated whether an auto-forward had been put in place on the server side. I note that the first email alert, received on 17 February 2020, was explicit in notifying the Council of the creation of a forwarding/redirect rule and find that the Council was remiss in failing to adequately investigate and identify the creation of an auto-forward on the user's side of Office 365.

iii. Finding

7.45 I find that the Council infringed Article 33(1) of the GDPR by failing to notify the DPC of the personal data breach(es) when it ought to have been aware of them.

8. Decision on Corrective Powers

8.1 I have set out above, pursuant to Section 111(1)(a) of the 2018 Act, my decision to the effect that the Council has infringed Articles 5(1), 32(1) and 33(1) of the GDPR. Under Section 111(2) of the 2018 Act, I must now make a decision as to whether corrective powers should be exercised in respect of the Council and, if so, the corrective powers to be exercised. The remaining question for determination in this Decision is whether or not those findings merit the exercise of any of the corrective powers set out in Article 58(2) and, if so, which one(s).

8.2 Recital 129, which acts as an aid to the interpretation of Article 58, provides that:

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

8.3 In the circumstances of the within inquiry and the findings of infringements, I find that the exercise of one or more corrective powers is appropriate, necessary and proportionate for the purpose of ensuring compliance with the GDPR.

8.4 Having considered the infringements identified in this Decision, I have decided to exercise corrective powers in accordance with Section 115 of the 2018 Act and Article 58(2) of the GDPR. I set out below the corrective powers that are appropriate to address the infringements in the particular circumstances, and the reasons for that decision, having considered all of the corrective powers set out in Article 58(2).

8.5 In summary the powers I have decided to exercise are:

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

A. Order to Bring Processing into Compliance

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

8.7 This order is made to ensure that full effect is given to the Council's obligation to implement appropriate technical and organisational measures. In deciding that an order is appropriate to achieve this end, I have had particular regard to significant number of data subjects who were affected by this personal data breach. I have also had regard to the manner in which unauthorised access was achieved by way of two successful phishing attempts. I consider that additional technical and organisational measures are essential to protect the rights and freedoms of data subjects. The Council must perform the necessary risk assessment to inform the measures that it must implement. However, as outlined at Part 6 of this Decision above, I find that those measures should include:

a) An updated Data Protection Impact Assessment of the end-to-end personal data processing the Council undertakes in the context of teacher registration including an assessment of manual/postal processing and systems-based processing;

b) The implementation of 2FA (two factor authentication) in Office 365. This will require the Council to change from the A1 license in use at the time of the breach;

c) Legacy Authentication protocols in Office 365 should be disabled for all users;

d) A policy of encryption and password protection on all data spreadsheets containing personal data in their possession, for both for internal and external document sharing;

e) Where it is necessary for the Council to retain and store information pertaining to vetting status details, such personal data must be protected by password protected email archiving or other secure filing systems;

f) The implementation of Advanced Threat Protection (ATP) in Office 365;

g) Mandatory annual data protection and cyber security training for all staff.

8.8 I am cognisant of the submissions of the Council that since the personal data breach it has engaged Consultancy 2 to provide assistance in identifying necessary improvements on general security awareness and Outlook 365 security settings. The Consultancy 2 Report, provided to the DPC on 17 June 2020, made a number of recommendations which the Council indicated that it will implement to improve IT security and to reduce the likelihood of the reoccurrence of a similar breach. I note in submissions dated 3 September 2021 that the Council has submitted that since the breach occurred it has implemented all but one of these corrective measures at its own initiative and intends to implement the last measure in the near future.

8.9 However, my decision to impose this order is on the basis of the technical and organisational measures which were in place at the time of the breach. As stated in Part 6 of this Decision, I find that the technical and organisational measures in place did not ensure a level of security appropriate to the risk. My order is therefore made to ensure that full effect is given to the Council's obligations to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. In deciding that an order is appropriate to achieve this end, I have had particular regard to the importance of ensuring that the vetting details of over 100,000 data subjects who are registered as teachers with the Council are adequately protected, although it is again noted that the registration database and vetting online system in use by the Council were not compromised and were not the subject of the Inquiry Report or this Decision.

8.10 I propose to specify a deadline of 2 June 2022 for the Council to bring its processing into compliance with Articles 5(1) & 32(1) of the GDPR. I will require the Council to submit a report to the DPC outlining the steps it has taken on or before this date.

B. Reprimand

8.11 I am issuing the Council with a reprimand in respect of its infringements of Articles 5(1), 32(1), and 33(1) of the GDPR. Article 58(2)(b) provides that a supervisory authority shall have the power to "*issue reprimands to a controller or processor where processing operations have infringed provisions of this Regulation*." I note that the Council, in submissions dated 3 September 2021, submits that it does not believe a reprimand is necessary or proportionate where, amongst other arguments, it states that the DPC in the Draft Decision "*misunderstood the scope of the Inquiry*" and that the Council having provided no evidence to the DPC of a Risk Assessment ever being carried out, despite repeated requests for same, were now submitting that an "*organisation wide DPIA was carried out previously in the form of the (named security services provider) Assessment in 2016 together with other security reviews over the years*". The Council also submitted that "*significant measures that were in place at the time of the incident, as outlined in…the Draft Decision, which you appear to have given little weight to."* The foregoing reasoning and rationale behind my findings in this matter demonstrate that the DPC has taken all due account of the matters aforesaid. However, I consider that a reprimand is appropriate, necessary and proportionate in view of ensuring compliance with the infringed Articles, as the reprimand will act to formally recognise the serious nature of all of the infringements. Further, the reprimand emphasises the requirement for the Council to take all relevant steps to ensure future compliance with the infringed Articles.

8.12 Recital 148 of the GDPR provides:

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

8.13 It is clear from the GDPR that a reprimand does not have to be issued in isolation to the exercise of any other corrective power. Furthermore, in accordance with Recital 129, each measure that I have decided to impose by way of the exercise of a corrective power for the infringements I have found must be appropriate, necessary and proportionate in view of ensuring compliance with the GDPR. In this respect, I consider it appropriate, necessary and proportionate to impose a reprimand in addition to the order in Part 8(A) of this Decision and the administrative fine detailed below in order to give full effect to the obligations in Articles 5(1), 32(1), and 33(1) and to formally recognise the seriousness of the infringements found in this Decision.

C. Administrative Fine

8.14 In addition to the corrective powers under Article 58(2)(b) & (d), I have also decided that the Council's infringements of Articles 5(1) & 32(1), and 33(1) of the GDPR warrant the imposition of an administrative fine. The reason for that decision, and the method for calculating that fine, are set out below.

i. Whether Each Infringement Warrants an Administrative Fine

8.15 Article 58(2)(i) permits the DPC to consider the imposition of an administrative fine, pursuant to Article 83, in addition to, or instead of, the other measures outlined in Article 58(2), depending on the circumstances of each individual case. This is also reflected in Section 115 of the Data Protection Act, 2018, which permits the DPC to impose an administrative fine on its own or in combination with any other corrective power specified in Article 58(2).

8.16 Article 83(1), in turn, identifies that the administration of fines *"shall in each individual case be effective, proportionate and dissuasive"*. In this context, when deciding whether or not to impose administrative fines and the amount of any such fines, I must give due regard to the criteria set out in Article 83(2) GDPR, which provide that:

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

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

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

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

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

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

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

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

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

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

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

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

8.17 The decision as to whether to impose an administrative fine (and if so, the amount of the fine) is a cumulative decision which is taken having had regard to each of the factors as set out in Article 83(2)(a) to (k). Therefore, I will now proceed to consider each of these criteria in turn in respect of the Council's infringements of Article 5(1) and Articles 32(1), and Article 33(1) respectively:

a) The nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

8.18 I find that the nature of the Council's infringements of 5(1) and Article 32(1) comprise a failure to comply with its obligation to implement an appropriate level of security in respect of its processing operations. This infringement must be assessed in light of the fact that infringements of Article 32 are usually capped at the lower threshold under Article 83(4), suggesting that infringements of Article 32, depending on the circumstances, may be less serious in nature than infringements that evoke the higher threshold under Article 83(5). The Council, in submissions dated 3 September 2021, have stated that they believe this finding should only be made in respect of Microsoft Office 365. As above, I would reiterate the scope of the Inquiry as set out in the Commencement Letter on 2 April 2020 stated that point 1 of the Inquiry was

"*An examination of the Council's compliance with Articles 5(1) and 32(1) of the GDPR with regard to the technical and organisational measures in place to ensure that there is adequate security over personal data held in manual or electronic form*."

And was therefore at no time limited to the Council's use of Microsoft Office 365.

8.19 The nature of the failure to implement appropriate technical and organisational measures must also be assessed in light of the sensitivity of the personal data processed. The Council has State-wide responsibility for, and are in possession of, the sensitive personal data contained in the registration details of over 100,000 data subjects. It is

again noted that at no time was the registration database or online vetting system in use by the Council compromised by the phishing attack the subject matter of this Decision. The personal data contained in the spreadsheets sent between employees of the Council contained the names, addresses and PPS numbers of the data subjects. A small number of emails contained details of the criminal convictions of one data subject. It is noted that the Council has been in breach of the GDPR in failing to implement appropriate and technical measures to ensure a level of security appropriate to the risk since the coming into application of the GDPR on 25 May 2018. The sensitivity and the large number of data subjects significantly elevates the seriousness of the nature of the infringement of Article 32(1).

8.20 9,735 data subjects were affected by the personal data breach. Sensitive personal data was sent to the malicious account and is unrecoverable. As a result, each data subject has significantly lost control over their personal data. It is not possible to identify how many individuals the data has been disclosed to. As such, I find that the Council's non-compliance with this obligation has had serious consequences in that it has resulted in damage and a risk to the rights and freedoms of the data subjects. The data subjects in question continue to be at risk of fraud and identity theft, although it is noted that the Council submit that no cases of fraud or identity theft have been reported to them. I consider that the likely level of damage suffered by the data subjects as a result of the breach is moderate to serious and that their rights and freedoms have been seriously infringed.

8.21 The nature of the finding of an infringement of Article 33(1) comprises a failure to notify the DPC of a personal data breach within the time period it ought to have been aware of it. The infringement must be assessed in light of the fact that it is also usually capped at the lower threshold under Article 83(4). However, the nature of this infringement must also be assessed in light of the purpose of Article 33(1), which is to ensure prompt notification of data breaches to supervisory authorities. This enables a supervisory authority to assess the circumstances of the data breach, including the risks to data subjects. It can then decide whether the interests of data subjects must be safeguarded to the extent possible, by mitigating the risks to them arising from a data breach[18], for example ordering a controller to communicate a personal data breach to affected data subjects under Article 58(2)(e) of the GDPR. The personal data breach concerned the personal data of a very significant number of data subjects and I have found that there was a breach of the GDPR in notifying the DPC of the personal data breach at the required time. In those circumstances, and in light of the importance of the notification process in protecting the rights and freedoms of data subjects, the finding of an infringement of Article 33(1) is serious in nature.

8.22 I find that the gravity of the infringements of Articles 5(1) & 32(1) are moderate to serious in circumstances where they directly resulted in the loss of control of personal data of a

[18] Recital 85 GDPR.

very high number of data subjects. There was a significant quantity of sensitive data included in the personal data breaches, including a small number of emails containing the identification and criminal convictions of one named data subject. I find that the gravity of the infringement must be assessed in light of the aggravating factor of the future potential misuse of the data subjects' personal data where the data has not been recovered. I find that the gravity of these infringements is serious in circumstances where the data subjects are at ongoing risk as a result of the infringement.

8.23 I find that the gravity of the infringement of Article 33(1) is serious in circumstances where it resulted in a failure on the part of the Council to mitigate the personal data breach. The Council notified the DPC of the personal data breach(es) on 9 March 2020, three weeks after receiving the initial low severity alert the subject line of which was "*Creation of forwarding rule/redirect rule*" and the content of which states that "*This alert is triggered when someone gets access to read you user's email*" on 17 February 2020. I note that it was not until a further **three** high and low severity alerts had been received by the Council that it identified the issue, despite the initial alert on 17 February 2020 explicitly identifying the cause of the breach. It is my finding that the appropriate technological and organisational measures should have been implemented within a reasonable period of time to establish the cause of the personal data breach. I find that had the Council appropriately investigated the cause of the first breach, and discovered the auto forward rule, it would have mitigated loss of further personal data after that date.

8.24 Regarding the duration of the infringements of Articles 5(1) & 32(1), there is no indication that the Council ever used a Microsoft Office programme other than the free licensed version of the Microsoft 365 A1 license, in use at the time of the breach, which did not provide a level of security appropriate to the risk associated with the type of personal data it processes in its role as a professional standards body. In those circumstances, I find that the infringements of Articles 5(1) & 32(1) commenced at the coming into application of the GDPR on 25 May 2018, and was ongoing at the time of the personal data breach. Therefore, the duration of the infringement, for the purposes of this, is over 22 months in length.

8.25 Regarding the duration of the infringement of Article 33(1), as outlined above, it is my finding that there are no circumstances concerning this breach that justify a failure to notify the DPC within 72 hours when the Council ought to have become aware of it. Therefore, the first infringement commenced on 20 February 2020, 72 hours after the Council ought to have become aware of it. The infringement ceased when the Council notified the DPC on 9 March 2020. Therefore, the duration of this infringement is two weeks and four days weeks in length. I find the duration of this infringement is at the moderate to high end of the scale of culpability in the circumstances. The second infringement commenced on 7 March 2020, 72 hours after the Council ought to have become aware that the second auto-forward rule had been established. The infringement ceased when the Council notified the DPC on 9 March 2020. Therefore, the duration of

this infringement is 48 hours in length. I find that the duration of this infringement is at the low to moderate end of the scale of culpability in the circumstances.

8.26 In submissions, dated 3 September 2021, in response to the above the Council submit that:

"…the vast majority of the 323 emails concerned were on the lower scale of sensitivity, which is acknowledged… (in) the Draft Decision.

It is also important to note that no actual damage has been suffered by any of the data subjects. The cyber-attack occurred well over a year ago and there have been no reported cases of fraud or identity theft and indeed no adverse consequences for the data subjects."

And that*:*

"…*it is important to emphasise that the security incident in question was as a result of a cyber-attack and human error****."***

b) the intentional or negligent character of the infringement

8.27 I find that the Council's infringements were unintentional, but that they were negligent in character, within the meaning of Article 83(2)(b). The Article 29 Working Party Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679 provide that:

"In general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law."[19]

8.28 I find that the Council was negligent within the meaning of Article 83(2)(b) and breached the duty of care required of it by omitting to adequately implement the appropriate technical and organisational measures required of it by Articles 5(1) and 32(1) to a level of security appropriate to the risk of its processing operations. However, I am satisfied that the Council did not intend to cause this infringement. I find that the Council was also negligent in the extent of its infringement of Article 33(1) where it ought to have been aware of the data breach(es) if it had used all appropriate technological protection and organisational measures to establish the cause of the initial, second and third security alerts as it was obliged to do.

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

8.29 The Council, in submissions dated 3 September 2021 written in response to the Draft Decision, have stated that:

"*We do not accept that the infringement was negligent. A finding that the infringement was negligent does not accurately represent the human error nature of the incident nor does it fairly represent the bona fides of the Teaching Council*."

8.30 The Council have also made submissions in response to this finding in respect of their efforts "*to ensure that privacy is embedded into the Teaching Council's processing activities*", including the Council's spend on security and IT, which I have had due regard for. The Council have also submitted, in the same submissions, that:

"*A breach of the law can of course take place without it being described as "negligent" which is arguably inflammatory language. If the DPC is minded to find that there has been an infringement, which is not accepted, the nature of that infringement should be described as unintentional*."

8.31 In response I would remind the Council that it is the GDPR which prescribes the word 'negligent' and that it is in no way inflammatory. As above, I have made a finding that the infringement was unintentional, but was negligent, i.e., a failure to take proper care that the Council had adequately implemented the appropriate technical and organisational measures required of it by Articles 5(1) and32(1) to a level of security appropriate to the risk of its processing operations.

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

8.32 The Council attempted to mitigate the damage and risk to the rights and freedoms suffered by the data subjects as a result of the personal data breach. On 26 March 2020, it wrote to the 9,735 data subjects apologising for and providing information regarding the breach. However, it is noted that the sensitive personal data of the data subjects in unrecoverable. It is noted that had the Council carried out proper investigations into the first security alert, the three following alerts and the loss of personal data which ensued would not have occurred. This potentially would have mitigated the damage suffered by the data subjects. It is also noted that all of the Council's mitigating action was taken after the two week and four day delay in discovering and reporting the first breach. I note that the Council has submitted that the decision to notify data subjects could only be taken once the Data Breach Risk Assessment was complete, and that this required an on-site forensic assessment of each of the 323 emails sent to the external email account. I note also the Council's submission that its offices closed on 12 March 2020 amidst the onset of the Covid-19 pandemic, and that significant logistical and administrative support was required in order to prepare the notifications.

8.33 The Council have submitted, in submissions dated 3 September 2021, that:

"*…the statement that the purported delay reduced the capacity to mitigate damage suffered by the data subjects is unfounded. There is no evidence to suggest that any damage has been suffered by the data subjects or that damage was a result of any delay on the part of the Teaching Council to notify data subjects*."

In this respect, I would remind the Council that the loss of control of personal data constitutes damage to the effected data subjects. The Council has also detailed the steps it took to mitigate "*any potential damage*" including contacting external legal advisors to conduct a Data Breach Risk Assessment. I note also that the Council has submitted that its Privacy Policy, AUP and Data Loss/Personal Data Breach Procedure record the requirement to notify a data breach within 72 hours. I have considered each of these factors in mitigation when deciding on the eventual fine.

d) The degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 5(1) & and 32(1)

8.34 As outlined above, I find that the Council infringed Articles 5(1) & 32(1) of the GDPR by failing to implement appropriate and organisational measures designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects. I consider that the Council 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 infringements of Articles 5(1) & 32(1) against the Council, this factor cannot be considered aggravating in respect of that infringement.

8.35 Regarding the infringement of Article 33(1), I note that the Council has a DPO in place who notified the DPC of the personal data breach. The Council have submitted that the Privacy Policy in place at the time of the data breach states the requirement to notify the DPC of a data breach within 72 hours.

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

8.36 There are no previous infringements by the Council.

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

8.37 The Council cooperated fully with the DPC to remedy the infringements and to mitigate their adverse effects. In its breach notifications and incident reports, the Council illustrated the steps that it had taken, and was in the course of taking, to remedy the infringements and the possible adverse effects. Furthermore, the Council's submissions during the Inquiry detailed the measures that the Council has implemented, and is in the course of implementing, to provide an appropriate level of security in respect of its data processing. The Council commissioned a report by Consultancy 1 to investigate the cause of the personal data breaches. The Council also engaged Consultancy 2 to:

"…assist with a review of the breach with the objectives being to provide recommendations around addressing risks identified as a result of the breach, conduct a policy review and create an action plan to implement these changes."

8.38 In submissions the Council outlined a number of security measures which were not in place at the time of the breach, but have been put in place subsequent to the breach, or are under consideration for implementation. These measures include the upgrade of the Office 365 license to provide the Council with the ability to enable additional security features, the enabling of a data loss protection plan on Outlook 365, the roll out of two factor authentication and the initiation of a plan for phishing campaigns.

8.39 The Council have submitted that a data breach response plan is in place which sets out the mandatory reporting requirements, and that Council staff are provided with training on reporting data breaches immediately. The Council have further submitted that a Cyber Security Runbook is in place and that security emails are sent to staff on a monthly basis to remind them of common threats and encourage reporting of any security or data breach incidents. The Council have submitted that at the time of the breach, the requirement to notify data breaches was set out in the Council's Privacy Policy and AUP.

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

8.40 The categories of personal data affected by the infringements include sensitive personal data. While the data subjects' vetting status information is not special category personal data within the meaning of Article 9 of the GDPR, this category of personal data is, nonetheless, highly sensitive in the circumstances. As previously stated in Part 6 of this Decision, the criminal convictions of one named data subject were contained in an email which was auto-forwarded to the external Gmail account. As outlined above, the mishandling and/or misuse of this type of personal data by the malicious actor who created the auto forwarding rule may seriously infringe the rights and freedoms of data subjects above and beyond the already serious loss of control that has been occasioned. Therefore, I find that this data is highly sensitive. The finding of an infringement of Article

33(1) is aggravated because the higher risk to the rights and freedoms of data subjects makes prompt notification to the DPC even more imperative.

h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

8.41 The infringements became known to the DPC because the Council notified the DPC of the personal data breach. The Inquiry was conducted to examine whether or not the Council had discharged its obligations in connection with the subject matter of the personal data breach and determine whether or not any provision(s) of the 2018 Act and/or the GDPR had been contravened by the Council in that context.

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

"The controller has an obligation according to the Regulation to notify the supervisory authority about personal data breaches. Where the controller merely fulfils this obligation, compliance with the obligation cannot be interpreted as an attenuating/ mitigating factor."[20]

8.43 The Council's compliance with its obligation to notify personal data breaches under Article 33(1) cannot be considered mitigating in respect of the Article 32(1) infringement. Conversely, the breach of Article 33(1) in notifying the DPC of the breach is not aggravating in circumstances where that infringement is the subject of consideration for this corrective power.

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

8.44 Corrective powers have not previously been ordered against the Council with regard to the subject-matter of this Revised Draft Decision.

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

8.45 There are currently no fully approved national certification schemes or mechanisms in line with Article 42 of the GDPR.

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

k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

8.46 The Council has submitted, in submissions dated 3 September 2021, that "*No financial benefit was gained from the purported infringement by the Teaching Council.*" This is accepted.

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

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

"The assessment of what is effective, proportional and dissuasive in each case will have to also reflect the objective pursued by the corrective measure chosen, that is either to re-establish compliance with the rules, or to punish unlawful behaviour (or both)."[21]

8.49 Regarding the infringements of Articles 5(1) & 32(1) and 33(1), I find that an administrative fine is necessary in respect of the infringements, in order to provide an effective, proportionate and dissuasive response in the particular circumstances of the case.

8.50 In making this decision, I have had regard to the order and reprimand proposed in this Decision. Those corrective powers are of utility in re-establishing compliance and in providing an effective and dissuasive response. However, I find that those measures alone are not sufficient. Article 32(1) places a continuous obligation on controllers to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Therefore, the order and reprimand alone cannot guarantee future compliance. In finding that an administrative fine is necessary to provide an effective, proportionate and dissuasive response, I have had regard to the serious nature and gravity of the infringement, the negligent character of the infringement, and the sensitivity of the personal data the subject of the personal data breach. It is clear that the Council's infringement of Articles 5(1) & 32(1) and 33(1) posed a significant threat to the rights and freedoms of data subjects.

8.51 The Council has submitted, in submissions dated 3 September 2021, that a number of factors "*should be taken into account in mitigation and the fine reduced accordingly*." The

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

Council has cited a number of decisions of the DPC wherein fines were reduced, taking into account the level of cooperation of the data controller in remedying the infringement and mitigating the possible adverse effects of the infringement. The Council has submitted that

"*We note that the Draft Decision does not indicate whether any such reductions will be applied in the present case to reflect the applicable mitigation. We submit that this is manifestly unfair as the whole purpose of furnishing the Teaching Council with the draft decision is to enable it to make submission in relation to, inter alia, the level of fine or sanction actually imposed. In that regard we must insist on being provided with a further opportunity to review another version of the Draft Decision which actually sets out your proposed approach to any reduction of the fine in light of the applicable mitigation. Otherwise the Teaching Council is essentially being deprived of any meaningful opportunity to make submissions in relation to the level of the actual fine imposed."*

8.52 I note the Council's submissions and its request to be provided with an opportunity to review a further version of the Draft Decision which sets out any reduction of the fine in light of applicable mitigation. I have given the applicable mitigation as submitted by the Council due consideration and have reduced the final fine having done so. I will therefore not be providing the Council with a further Draft Decision. The Council has further submitted that the proposed fine set out in the Draft Decision "*should be reduced to reflect the level of expenditure already incurred*…" and detail the Council's expenditure on consultancy fees, "*IT security risk assessments carried out over the last number of years and general expenditure on IT*" and the "*The significant level of expenditure that the Teaching Council will incur into the future in respect of IT services*." This submission of the Council fails to acknowledge that data security is an obligation for all data controllers, and therefore incurs necessary costs, which will not be taken into account by the DPC by way of mitigation.

8.53 The Council, in submissions dated 3 September 2021, has submitted that should I confirm the findings made in the draft decision in respect of Articles 5(1) and 32 that "*no corrective (action) should be taken or that the administrative fine should be reduced taking into account the factors addressed in…these submissions.*" The Council then sets out its reasons for this submissions. The Council submit that:

"*…we submit that the imposition of an administrative fine is not necessary or proportionate. A fine has the effect of providing a dissuasive response, as referred to in paragraph 8.43 of the Draft Decision. The Teaching Council is fully aware of the significance of the cyber-attack and consequent data breach. This is clear from the significant efforts which have been made to further improve the Teaching Council's security levels since this incident occurred. In this regard, the corrective actions included in the Draft Decision have already been given effect to prior to their inclusion in the Draft Decision. Therefore, it is difficult to see why an administrative fine would be required "with a view to re-establishing compliance…"*

8.54 I have considered the submissions and reaffirm my finding that an administrative fine is effective, proportionate and dissuasive with a view to establishing full compliance. I have had regard to all of the corrective powers available to me as set out in Article 58(2) of the GDPR. For the reasons set out above, and having particular regard to the matters discussed under Article 83(2)(a) – (j) cumulatively, I consider it appropriate to impose an administrative fine in respect of the infringement of Articles 5(1) & 32(1) and 33(1) of the GDPR in addition to the order and reprimand imposed at parts 7(A) & (B) of this Decision.

ii. The Permitted Range

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

8.56 Article 83(4) of the GDPR provides that infringements of the obligations of controllers pursuant to, amongst others, Article 5 shall:

> *"…in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher…"*

8.57 The income of the Council in 2018 was €6,927,015 as reported in the Council's financial statements for 2018, these being the most recently available financial statements available as per its annual report. I note that the Council have submitted in their submissions dated 3 September 2021 that due to expenditure in 2018 the Council had a deficit of €398,000 in that year.

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

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

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

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

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

8.59 Firstly, in order for this cap to apply, the controller or processor in questions must be a public authority or public body. "Public body" is defined in Section 2 of the 2018 Act as

"…a company (within the meaning of the Act of 2014 or a former enactment relating to companies within the meaning of section 5 of that Act) a majority of the shares in which are held by or on behalf of a Minister of the Government."

8.60 The Council was enacted on 17 April 2006. Therefore I am satisfied that the Council is a public body for the purposes of the 2018 Act.

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

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

8.62 I am satisfied that the Council is not an "*undertaking*" for the purposes of Section 141(4) of the 2018 Act. I therefore find that the permitted range for the proposed administrative fines in this case must be calculated by reference to the cap in Section 141(4) of the 2018 Act. Therefore, the permitted range in respect of each fine is €0-€1,000,000.

iii. Calculating the Administrative Fines

8.63 In the absence of specific EU-level guidelines on the calculation of fines in this context, I am not bound to apply any particular methodology[22]. In practical terms, this means that I am not bound to use a base figure or fixed financial starting point for the assessment of the proposed fine. I, therefore, ultimately intend to identify the amount of the administrative fine to be imposed on the Council on a general basis (as in the judgments cited in the footnotes above) and by reference to the factors to which I am required to have due regard in accordance with Article 83(2) and which I have already applied to the circumstances of this case in detail above. In doing so, I must also ensure that, in accordance with the obligation on supervisory authorities under Article 83(1), the administrative fine imposed in this case is effective, proportionate and dissuasive.

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

8.64 In deciding on the fine, and in determining the quantum of the fine, I have, as set out above, had due regard to all of the factors set out in Articles 83(2)(a) to (k) as applicable. I am also obliged pursuant to Article 83(1) to ensure that the imposition of the fine in the circumstances of this case is effective, proportionate and dissuasive. In considering the application of the principles of effectiveness, proportionality and dissuasiveness of the administrative fine, I consider that a fine cannot be effective if it does not have significance relative to the revenue of the data controller. Moreover, the principle of proportionality cannot be adhered to if the infringement is considered in the abstract, regardless of the impact on the controller. This is compounded by the fact that future infringements need to be deterred. In this regard, I consider that a fine cannot be dissuasive if it will not be of any financial significance.

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

8.65 As outlined above, the permitted range is €0 - €1,000,000. In locating the fine on the permitted range, I have had regard to the nature, gravity and duration of the infringement as assessed in accordance with Article 83(2)(a) above. I have also had regard to the aggravating factors, specifically the negligent, within the meaning of Article 83(2)(b), character of the infringement and the sensitive categories of personal data affected by the infringement as assessed in accordance with Article 83(2)(b)&(g) above. I have considered the mitigating factors in the Council's favour, notably those detailed in respect of Article 83(2)(e), 2(f) and 2(2)(i) and have had regard to the Council's submissions in that respect. Having regard to all of these factors, I consider that the figure of **€40,000** is appropriate in the circumstances of this case.

The infringement of Article 33(1) of the GDPR

8.66 As outlined above, the permitted range is €0 - €1,000,000. In locating the fine on the permitted range, I have had regard to the nature, gravity and duration of the infringement as assessed in accordance with Article 83(2)(a) above. I have also had regard to the aggravating factors, specifically the finding of the negligent character of the infringement within the meaning of Article 83(2)(b) and the degree of responsibility of the Council taking into account its lack of measures to ensure that personal data breaches ought to be discovered within a reasonable period of time, in accordance with Article 83(2)(b) & (d) above. Again, I have considered the mitigating factors in the Council's favour and have had regard to the Council's submissions in that respect. Having regard to all of these factors, I consider that the figure of **€20,000** is appropriate in the circumstances of this case.

8.67 The cumulative fine is therefore **€60,000.**

8.68 I consider that the above range meets the requirements of effectiveness, proportionality and dissuasiveness of the administrative fine. In order for any fine to be effective, it must

reflect the circumstances of the individual case. The circumstances of this infringement concerns the failure to process personal data in a manner that ensured the appropriate security of the personal data using appropriate technical and organisational measures, and the failure to notify the DPC of the personal data breach without undue delay when the Council ought to have been aware of the data breach. It is noted that the personal data forwarded to the Gmail account was unrecoverable and that those data subjects whose data was affected may be further affected by this breach in the future. I consider that these circumstances require a significant fine in order for it to be effective. In order for a fine to be dissuasive, it must dissuade the controller from repeating the conduct concerned. I am satisfied that the fine would be dissuasive to the Council. As regards the requirement for any fine to be proportionate, this requires me to adjust the quantum of any proposed fine to the minimum amount necessary to achieve the objectives pursued by the GDPR. I am satisfied that the range of the fine proposed does not exceed what is necessary to enforce compliance with the GDPR, taking into account the impact of the infringements on the data subject rights enshrined in the GDPR. Accordingly, I am satisfied that the fine would be effective, proportionate and dissuasive, taking into account all of the circumstances of the Inquiry.

iv. The Article 83(3) Limitation

8.69 Article 83(3) of the GDPR provides that:

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

8.70 In the recent binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR decision by the EDPB[23] it states:

> *319. Article 83(3) GDPR reads that if "a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement."*
>
> *320. First of all, it has to be noted that Article 83(3) GDPR is limited in its application and will not apply to every single case in which multiple infringements are found to have occurred, but only to those cases where multiple infringements have arisen from "the same or linked processing operations".*

[23] Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR

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

8.71 The Board also state that:

"324. With regard to the meaning of Article 83(3) GDPR the EDPB… notes that in the event of several infringements, several amounts can be determined. However, the total amount cannot exceed a maximum limit prescribed, in the abstract, by the GDPR. More specifically, the wording "amount specified for the gravest infringement" refers to the legal maximums of fines under Articles 83(4), (5) and (6) GDPR. The EDPB notes that the Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679[24] state that the "occurrence of several different infringements committed together in any particular single case means that the supervisory authority is able to apply the administrative fines at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement". The guidelines include an example of an infringement of Article 8 and Article 12 GDPR and refer to the possibility for the SA to apply the corrective measure within the limit set out for the gravest infringement, i.e. in the example the limits of Article 83(5) GDPR.

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

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

8.72 I note the Council's submissions, dated 29 September 2021, which state that:

"You state in your letter of 8 September 2021 that it is necessary for you to follow the EDPB's interpretation of Article 83(3) of the GDPR in future inquiries. You say that this is

[24] Guidelines on Administrative Fines, p. 10.

because the issue is a matter of general interpretation, and is not specific to the facts of the case in which it arose. We respectfully disagree. As is clear from the wording of Article 65(1), the decision of the EDPB is binding only as it relates to the "individual cases" referred to it under Article 65. Nothing in Article 65, Article 60(1) or Article 63 requires the Data Protection Commission to adopt an interpretation of the GDPR of another supervisory authority or indeed the EDPB. The doctrine of stare decisis does not apply and it is open to the Data Protection Commission to adopt a different interpretation of Article 83(3).)."

8.73 The Council have also submitted that in relation to the fine in this matter that:

"*It would appear that the Commissioner is adopting an extreme and simplistic approach to the decision of the EDPB, and is taking the view that it requires that multiple fines be accumulated on a simple arithmetic basis. This approach is neither apparent from the EBPD decision, nor is it in accordance with (i) the totality principle or (ii) the obligation to impose a proportionate fine.*

Such an approach flies in the face of well-established principles concerning the imposition of penalties for multiple transgressions and, indeed, the terms of the EDPB ruling itself."

And have submitted that the totality of the penalty must be considered. I have had all due regard to the totality of the penalty, and the financial circumstances of the Council, when deciding of the amount of the fine in this case.

8.74 In the same submissions the Council have stated "*The Revised Draft Decision also fails to consider whether, taken as a whole, the total of the proposed fines in respect of the two infringements are effective, proportionate and dissuasive*." As I have set out above I have had all due regard to these factors when calculating the fine to be imposed.

8.75 As set out above, the infringements of Articles 5(1)(f), 32(1) and 33(1) were all negligent in nature. Furthermore, these infringements all concern the same or linked processing operations. This Decision makes findings of infringements of Articles 5(1) and 32(1) and both relate to the same processing operations regarding the Council's security of technical and organisational measures on the processing of personal data. Article 32(1) elaborates on the requirement for appropriate security in Article 5(1)(f).

8.76 Regarding the Council's infringement of Article 33(1), the finding in Article 33(1) arises from the Council's obligation to notify a breach to the DPC without delay. The underlying personal data breach concerning that infringement relates to unauthorised access to two Council staff user's email accounts. Therefore, the underlying personal data breach relates to the Council's security of technical and organisational measures of personal data, including its storage of personal data. Therefore, it involves the same processing operations that are subject to findings of infringements of Articles 5(1) and 32(1) in this

Decision. It follows that this infringement of Article 33(1) relates to the same or linked processing operations as the infringements of Articles 5(1) & 32(1) and 33(1).

8.77 Applying Article 83(3), in circumstances where these infringements were all negligent and all related to the same or linked processing operations, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement. Applying the EDPB's interpretation of Article 83(3) in 1/2021, this means that Article 83(3) does not provide for concurrency in fining, but, rather, identifies only the applicable fining cap. It is the duty of the DPC to have regard to the EDPB's decision arising from the DPC's obligations under Article 60 et al, to ensure cooperation and the consistent application of the GDPR.

8.78 As outlined above, Section 141(4) of the 2018 provides the applicable fining cap in this case as €1,000,000. Therefore, applying Article 83(3), the total amount of the fines imposed for the infringements of Articles 5(1)(f) & 32(1) and 33(1) must not exceed €1,000,000. The total cumulative fine in this case is €60,000. Therefore, these fines do not exceed the applicable cap.

v. The Amount of the Administrative Fine

8.79 I find that it is appropriate to impose administrative fines, pursuant to Articles 58(2)(i) and 83, addressed to the Council in the cumulative amount of €60,000. For the avoidance of doubt the fines reflect the infringements that were found to have occurred, as follows:

i. In respect of the finding of an infringement of Article 5(1) and 32(1) of the GDPR, a fine of €40,000
ii. In respect of the finding of an infringement of Article 33(1) of the GDPR, a fine of €20,000

8.80 The final step is to consider whether the figures arrived at are *"effective, proportionate and dissuasive"* in the circumstances in accordance with Article 83(1) of the GDPR. I consider that the figures of €40,000 and €20,000, for a total of €60,000 meet these requirements. In order for any fines to be effective, they must reflect the circumstances of the individual case. As outlined above, the infringements of Articles 5(1) and 32(1) and Article 33(1) are serious. The personal data breaches affected a high number of data subjects and the Council's failure to implement an appropriate level of security put the personal data of an even larger number of data subjects at risk. The potential consequences of the infringements are severe in circumstances where the Council processed sensitive personal data, and transmitted it by email in unencrypted spreadsheets. In order for a fine to be dissuasive, it must dissuade both the controller/processor concerned as well as other controllers/processors carrying out similar processing operations from repeating the conduct concerned. I am satisfied that

the amount of the proposed fines would be dissuasive to both the Council and to similar controllers.

8.81 As regards the requirement for any fines to be proportionate, this requires me to adjust the quantum of any fine to the minimum amount necessary to achieve the objectives pursued by the GDPR. I am satisfied that the amount of the fines does not exceed what is necessary to enforce compliance with the GDPR, taking into account the impact of the infringements on the data subject rights enshrined in the GDPR. The figures of €40,000 and €20,000 for a cumulative total of €60,000 amount to 6% of the cap available. Accordingly, I am satisfied that the amount of the fines is effective, proportionate and dissuasive, taking into account all of the circumstances of the Inquiry.

9. Right of Appeal

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

_____

Helen Dixon
Commissioner for Data Protection

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

The Case Officer delivered the Final Inquiry Report to me on 12 April 2021. I also had regard to all of the correspondence, submissions, and documentation gathered during the Inquiry and the decision-making stage, including:

(i) The DPC's Final Inquiry Report, Inquiry Reference IN-20-4-1;
(ii) Documentation concerning the breach notification BN-20-03-399, including the breach notification form and updates, the emails between the Council and DPC;
(iii) Letter dated 2 April 2020 notifying the Council of the Commencement of an Inquiry;
(iv) The Council's letter of response to the DPC on 23 April 2020 on queries raised in the Notification of Commencement Letter;
(v) The Council's Draft Action Plan, in excel format, received on 23 April 2020;
(vi) The Council's ICT Contracts;
(vii) The Solicitor 1 Risk Assessment, dated 20 March 2020;
(viii) The Email and Risk Categorisation excel spreadsheet, received on 23 April 2020;
(ix) The email sent by the DPC to the Council on 12 May 2020 requiring further information on certain technical areas;
(x) The Council's response to the DPC's technical questions received on 12 May 2020;
(xi) The email sent by the DPC to the Council, on 28 May 2020, requiring further information on the previously provided answers to technical questions;
(xii) The submissions of the Council, on 17 June 2020, in response to the request for further information on previously provided answers to technical questions;
(xiii) The Consultancy 1 Consulting Review, dated 17 June 2020;
(xiv) The letter sent by DPC to the Council on 21 July 2020 requesting further information;
(xv) The response to the letter of the DPC by the Council, received on 31 July 2020;
(xvi) Email alert screenshots provided to the DPC, on 31 July 2020;
(xvii) The submissions of the Council in response to the Draft Inquiry Response, on 30 October 2020;
(xviii) The Council's Glossary of Technical Terms;
(xix) The letter from the DPC to the Council, on 26 November 2020, in response to a request regarding the next steps of the Inquiry;
(xx) The letter from the Council to the DPC on 28 April 2021 requesting to make submissions before the issuing of the Draft Decision.
(xxi) The letter from the DPC to the Council, on 8 June 2021 requesting further information;
(xxii) The letter from the Council to the DPC, on 18 June 2021 providing the requested additional information;
(xxiii) The submissions of the Council in response to the Draft Decision, on 3 September 2021;
(xxiv) The letter from the DPC to the Council, on 8 September 2021, explaining why a Revised Draft Decision was being sent to the Council together with the Revised Draft Decision;

(xxv) The letter from the Council on 13 September 2021 requesting additional time to respond to the Revised Draft Decision;

(xxvi) The letter from the DPC to the Council on 13 September 2021 granting additional time to deliver submissions on the Revised Draft Decision until 29 September 2021;

(xxvii) The submissions of the Council in response to the Revised Draft Decision, received on 29 September 2021.