An Coimisiún um Chosaint Sonraí
Data Protection Commission

In the matter of the General Data Protection Regulation

Data Protection Commission Case Reference: IN-19-7-3

In the matter of the City of Dublin Education and Training Board

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

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

DECISION

Decision-Makers for the Data Protection Commission:

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

18 June 2025

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Protection Commission
6 Pembroke Row
Dublin 2, Ireland

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Contents

A. Introduction

1. The General Data Protection Regulation ('**GDPR**') is a regulation in European Union law on the protection of individuals with regard to the processing of their personal data. The date of application of the GDPR is 25 May 2018.[1]

2. The Data Protection Commission ('**the DPC**') was established on 25 May 2018, pursuant to the Data Protection Act 2018 ('**the 2018 Act**'), as Ireland's supervisory authority within the meaning of, and for the purposes specified in, the GDPR.[2]

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

    1. Everyone has the right to the protection of personal data concerning him or her.

    2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

    3. Compliance with these rules shall be subject to control by an independent authority.

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

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

6. This Decision is being provided to the City of Dublin Education and Training Board ('**CDETB**') pursuant to section 116(1)(b) of the 2018 Act, in order to give notice of the Decision, the reasons for it, and the decision in relation to the powers exercised pursuant to Article 58 of the GDPR.

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ('**General Data Protection Regulation**').

[2] SI 175/2018 Data Protection Act 2018 (Establishment Day) Order 2018.

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

B. Preliminary Matters

a) Data Controller

8. In commencing the Inquiry, the DPC considered that CDETB may be the controller, within the meaning of Article 4(7) GDPR, in respect of personal data that were the subject of the personal data breach notifications. In this regard, CDETB confirmed in its email notification of the personal data breach to the DPC on 19 November 2018[3] that it was the controller.

b) Factual Scope of the Inquiry

9. This inquiry concerns a data breach notified by CDETB to the DPC on 16 November 2018 and which related to a security incident that occurred on a web server under the control of CDETB. CDETB discovered malware on this web server and also noticed that the web server was storing the personal data of student grant applicants who had uploaded information connected to their grant applications through CDETB's website. CDETB had not intended that such data be retained on the server and promptly notified the DPC of a breach before taking mitigating measures to address the issue and prevent reoccurrence. This discovery of retained personal information combined with the detection of malicious malware on the web server, meant that the personal data of grant applicants were being put at risk.

10. CDETB identified that the personal data included data subject identity, PPSN, contact details, identification data, economic or financial data, location data, criminal convictions, offences or security measures, data revealing racial or ethnic origin and health data. Approximately 13,000 data subjects were impacted by the breach.

[3] CDETB to DPC Update Email re Breach on 19 November 2018.

C. Legal Framework for the Inquiry and the Decision

a) Legal Basis for the Inquiry

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

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

b) Legal Basis for the Decision

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

14. Having considered the information obtained in the Inquiry, the DPC is satisfied that the Inquiry has been correctly conducted and that fair procedures have been followed throughout. The DPC has had regard to the submissions that CDETB made in respect of this Decision before proceeding to make this final Decision under section 111 of the 2018 Act.

D. Factual Background and Materials Considered in the Inquiry

a) Notification and investigation

15. CDETB operates a website (https://www.susi.ie) on which third-level students can find information relating to their eligibility for a higher education grant. Student Universal Support Ireland (**'SUSI'**) was created in 2012 as a business unit of CDETB (then known as the City of Dublin Vocational Education Committee) following CDETB's designation as the single awarding authority for new grants under the Student Support Act 2011, replacing 66 previous grant-awarding bodies.[4] As a business unit of CDETB, SUSI is not a separate legal entity.

16. To apply for a grant, an applicant must create an online SUSI account or use their verified MyGovID account. At the time under consideration in this Decision, functions relating to submissions by grant applicants were primarily fulfilled through a separate public-facing front-end portal at https://grantsonline.ie. A link from https://susi.ie redirected users to the grantsonline.ie website, where an applicant could create a SUSI online account. Once an applicant had created a SUSI online account, they could fill in an application form for a grant on grantsonline.ie. Applicants were required to provide the following information when making an application through the grantsonline.ie website:

    - Personal details of the applicant;
    - Nationality and residency of the applicant;
    - Course details and previous education and other sources of financial support of the applicant;
    - Dependent children and relevant persons;
    - Income details of parent(s)/legal guardian(s), spouse, civil partner or cohabitant, as applicable)[5]

17. CDETB indicated to the DPC that the original intended purpose of the susi.ie website was simply to provide information on the grant application scheme. However, in April 2017, functionality was added to the susi.ie website to allow applicants, after making their application to SUSI on the grantsonline.ie website, to submit supplementary requests and data through online forms. Applicants were enabled to submit and provide information in respect of the following:

    - requests for internal review of a grant application (grant applicants)
    - requests for cancellation of a grant application (grant applicants)

---

4 S.I. 161/2012 Student Support Act (Appointment of Awarding Authority) Order 2012.

5 https://www.susi.ie/how-to-apply/your-new-application-form-guide-/ (retrieved 9 July 2024).

- requests to be enabled to make a late grant application (grant applicants and non-applicants)
- submitting a formal complaint to SUSI (grant applicants and non-applicants)
- reporting suspicious activity to SUSI (grant applicants and non-applicants)

18. On 16 November 2018, the DPC received a breach notification (BN-18-11-258)[6] from CDETB relating to a security incident on its www.susi.ie website. The notification said that CDETB had discovered on 14 November 2018 that its web server was retaining personal data in the form of contact forms and uploaded documents. Prior to that discovery, the data controller had assumed that personal data being submitted through its website were being emailed to the relevant SUSI team and were not being retained locally on its web server. CDETB stated that this discovery, combined with its detection of malicious malware contained on its web server in October 2018, now resulted in a realisation that the personal data of grant applicants were being put at risk.

19. In its breach notification, CDETB estimated that the malware had been inserted in January 2018 and stated that the retention of personal data on the server was detected by it on 14 November 2018. CDETB outlined that on 16 October 2018 it discovered 'malicious code on the SUSI website via a firewall security sweep'.[7]

20. In the notification form, CDETB identified that the following personal data relating to individuals were disclosed:

- Data subject identity (name, surname, birth date)
- PPSN (or other national identification number)
- Contact details
- Identification data (passports, licence data etc.)
- Economic or financial data
- Location data
- Criminal convictions, offences or security measures

In addition, the following special categories of data were disclosed:

- Data revealing racial or ethnic origin
- Health data

21. CDETB estimated that the number of affected individuals and data sets impacted by the breach was 8,000. The breach notification form indicated that the risk posed by the

[6] Breach Notification Form, 16 November 2018.

[7] Breach Notification Form, 16 November 2018, 3.

breach was assessed by CDETB to be low. On 19 November 2018, CDETB provided the DPC with an update by email.[8] This update comprised two reports:

(a) An undated report from exSite Communications (**'exSite'**) – CDETB's web development and support provider – which conducted an investigation of the SUSI website between 13 and 14 October 2018.[9]
(b) A Wordfence[10] 'Malware Removal Report' produced on the instructions of exSite and completed on 19 October 2018.[11]

22. In its report, exSite stated that it conducted an initial investigation of the SUSI website, scanning the website with Wordfence and the Revision Antivirus. The report stated that exSite identified suspicious files through its Revision Antivirus. (In its submissions on the DPC's draft inquiry report in this matter, CDETB stated that its personnel had identified those files during the deployment of a new firewall by SUSI on 16 October 2018, and that this prompted SUSI to have exSite conduct its investigation.)[12]

23. The exSite report stated that its support team removed the suspicious code within one hour of receiving an email from the SUSI IT team querying the presence of the code on 16 October 2018.

24. exSite performed an internal investigation of the security incident of 16 October 2018 and contacted Wordfence to conduct an external investigation. exSite stated that, as well as removing all malicious code from the website on 16 October 2018, it took the following actions:

- Changed all user and key administration (FTP, SSH and database) passwords
- Checked all file permissions – these were as they should be
- Deleted infected files – code on header.php and in /wp-admin/class-dependency.php and fake buddypress plugin with encrypted file
- Deleted exploitable file – Timthumb.php
- Added an improved scanning function to the server (Revision Antivirus)
- Added an improved firewall to the server (Fail2Ban)

---

8 Email CDETB to DPC, 19 November 2018.

9 exSite Report on SUSI Breach, undated (received by DES 16 October 2018 and by DPC 19 November 2018).

10 https://www.wordfence.com a third-party plugin used to check and scan a WordPress site's core files, themes and plugins for malware, bad URLs, backdoors, search engine optimisation spam, malicious redirects and code injections.

11 Wordfence Report, 19 October 2018.

12 CDETB submission on Draft Inquiry Report, 12 November 2020, 3.

25. The Wordfence 'Malware Removal Report' included a full scan of the SUSI website and specified that the malicious file found in the fake Buddypress plugin was a WSO Web Shell.[13] Wordfence went on to state that this:

> allows hackers to read or write files and databases, and generally do anything that a web application is allowed to do on the server. Hackers usually just use it to maintain access in case the exploit they used gets patched. They may have used it to read your files and database; unfortunately there is no way to tell.[14]

26. The Wordfence report determined that the version of TimThumb.php was probably not the attack vector. The report also determined that the class-dependency file and malicious code in header.php was only for manipulating search engine optimisation. However, subsequently the updated Ward Solution report of 23 January 2019[15] provided supplementary additional findings identifying that the header.php was modified on 27 April 2018 when JavaScript was injected into it.[16] The Ward Solutions report determined that when activated, the malicious JavaScript within the header.php file would try to access a site called boxtubex.com establishing a connection between the domain susi.ie and the domain boxtubex.com. The Ward Solutions updated report stated that its sources of intelligence on online threats indicated that boxtubex.com had been:

- associated with serving phishing campaigns;[17]
- identified in malicious campaigns to disseminate malware; and
- used between April 2018 and September 2018 as a Keitaro TDS (Traffic Distribution System) used in infection chains for Sundown and RIG exploit kits.

This analysis pointed to boxtubex.com being used as part of

> an attack against SUSI's website users during this period, which had the aim of infecting the users' machines with malware.[18]

---

[13] Web Shells are malicious scripts updated to web servers to gain persistent access and enable remote administration of an already-compromised server. WSO stands for web shell by Orb. This form of web shell is a PHP script. Attackers often employ WSO to view host server information, but it also includes a file manager, a remote shell, a password brute-force tool, and an SQL browser. https://plextrac.com/what-are-web-shells/

[14] Wordfence Report, 5.

[15] Incident Response Investigation Report from Ward Solutions (received by DPC 31 January 2019).

[16] On 21 November 2018, CDETB contacted Ward Solutions for assistance and commissioned this report.

[17] Phishing - Refers to the process of deceiving recipients into sharing sensitive information with an unknown third party.

[18] Incident Response Investigation Report from Ward Solutions, 20 (received by DPC 31 January 2019).

27. The Wordfence report outlined that, as the website access logs were retained only for any preceding two weeks, Wordfence had been unable to identify how the security breach had occurred. However, in its opinion the most likely explanation was that SUSI's WordPress administrator account had been compromised, enabling a hacker to install malicious code after gaining access to the WordPress administrator panel.

28. The exSite report expanded on this by outlining that a user account with an email address name@susi.ie was added to the WordPress user list on 12 January 2018. exSite stated:

> This account appears as a subscriber account at present but due to the coincidence of the date the account was added, we must conclude that this was the admin account that was compromised and subsequently downgraded to subscriber. We have no record of creating this account. Probably another admin created the account for [name redacted]. In our opinion there are a couple of ways this could of [sic] occurred, including the email address being compromised.[19]

29. The Wordfence report recommended implementing several plugins on SUSI's website and reviewing applicable security resources.

30. On 21 November 2018, CDETB contacted Ward Solutions for assistance in responding to the DPC's queries and to determine if sensitive documents stored on the SUSI website had been accessed by any unauthorised party by using the WSO Shell found on the webserver.

31. On 27 November 2018, the DPC emailed CDETB a questionnaire[20] to assist the DPC in reviewing the breach.

32. On 30 November 2018, the DPC wrote again to CDETB inquiring if it had identified details relating to individuals that may have been disclosed and whether the affected data subjects had received a communication about the breach. The DPC recommended that, if no communication had been sent, CDETB should consider communicating the data breach to all affected data subjects. The DPC further asked CDETB to notify the DPC of the following:

    - When contact had been made with affected data subjects;
    - The method of communication used to do so;

---

[19] exSite Report on SUSI Breach, (received by DES 16 October 2018 and by DPC 19 November 2018), 3.

[20] Email DPC to CDETB, Request for Further Information Regarding Breach, 27 November 2018.

- The recommendations or advice that CDETB provided to data subjects to mitigate the risks they might experience as the result of this incident.[21]

33. On 30 November 2018, SUSI, exSite and Ward Solutions had a discussion on the findings and recommendations contained in the report being prepared by Ward Solutions. A copy of this report[22] was delivered to CDETB on 3 December 2018. The report was dated 29 November 2018. CDETB provided the DPC with the results of this investigation report.

34. On 3 December 2018, CDETB responded to the DPC's queries restating the categories of personal data and special category personal data that it had identified as disclosed in its breach notification form of 16 November 2018. CDETB did not provide any further details on the records relating to the data categories involved. CDETB confirmed it was considering making contact with the affected data subjects and would inform the DPC on when and how it would do so, and the contents of any message to affected individuals.[23]

35. On 5 December 2018, CDETB further responded to the DPC's request of 27 November 2018 and provided additional documentation in the form of an incident investigation report prepared by Ward Solutions and a record of processing activities for the categories of personal data listed in the breach notification form.[24]

36. On 7 December 2018,[25] SUSI's Governance & Compliance Manager informed the DPC that:

> CDETB/SUSI will be informing data subjects of the personal data breach as defined in Article 4(12) of GDPR and Section 69(1) of the Data Protection Act 2018 and in line with Section 87 of the Data Protection Act 2018 [sic].[26]

37. CDETB further specified that preparations were

---

21 Email DPC to CDETB, Request Based on SUSI Notification Form, 30 November 2018.

22 Ward Solutions Report (received by DPC 5 December 2018).

23 CDETB to DPC, Response to Request for Further Information, 3 December 2018.

24 CDETB Response with Records of Processing Activities, 5 December 2018.

25 Email CDETB to DPC, Response Indicating Intention to Communicate Data Breach to Data Subjects, 7 December 2018.

26 The sections of the 2018 Act appear to have been referred to by mistake. The two sections give effect to provisions of Directive (EU) 2016/680 ('the Law Enforcement Directive') that respectively correspond to Articles 4(12) GDPR (definition of 'personal data breach') and Article 34 GDPR (communication of a breach to data subjects).

underway to make direct contact via email on Monday next, 10th December. SUSI will confirm with your office once this is done.[27]

38. However, on 10 December 2018, SUSI's Head of Operations informed the DPC by email that 'we will not be notifying this incident to data subjects today pending further consideration [of legal advice received]'.[28] CDETB indicated that this legal advice related to determining the level of any potential impact on the rights and freedoms of data subjects.

39. On 14 December 2018, CDETB's Head of Operations further outlined that it was proceeding urgently with a detailed analysis of the data subjects who may have been affected by the security incident on the basis of the legal advice it had received. CDETB stated that it had also requested an independent security company to perform a forensic investigation of the SUSI website, its webserver and the stored data it contained, the results of which CDETB expected to receive by mid-January 2019.[29] The security company referred to was Ward Solutions, who had already conducted a forensic investigation.

40. In the correspondence above, CDETB informed the DPC that, for the purpose of the administration of the Student Grant Scheme by SUSI, the Department of Education and Science (**'DES'**) acted as a joint controller with CDETB and that, upon being notified of the incident, the DES requested that its joint controller status be notified formally to the DPC. CDETB did not provide any further details on its arrangement with the DES as a joint controller.

41. On 20 December 2018, SUSI's Head of Operations informed staff of the DPC that CDETB would forward to the DPC a report it had prepared for the DES containing the reasons it had not notified data subjects to date. Following the telephone call on 20 December 2018, the DPC received by email a draft of the report prepared by CDETB and issued to the DES. The covering email asserted that this report would help to answer the DPC's questions regarding CDETB's rationale for the steps it was now taking.[30]

42. The CDETB report to the DES was dated 14 December 2018.[31] In it, SUSI outlined the history of the matter including the discovery of suspicious code by SUSI IT during firewall testing on 16 October 2018 and the subsequent discovery that data and forms

---

[27] Email CDETB to DPC, Response Indicating Intention to Communicate Data Breach to Data Subjects, 7 December 2018.

[28] Email CDETB to DPC, Update Informing DPC of Intention to Suspend Notifying Data Subjects, 10 December 2018, 1.

[29] Email CDETB to DPC, Further Update Regarding Potential Forensic Investigation of Website, 14 December 2018.

[30] CDETB Email Update Following Phone Conversation, 20 December 2018.

[31] Confidential Report CDETB_SUSI to DES, 14 December 2018 (received by DPC 20 December 2018).

were being retained on the webserver due to an error in the website design. (The report qualified the date of discovery of retained data with 'TBC').

43. The report to the DES related to how CDETB had requested a security report from exSite, which it received on 19 October 2018, and, based on that, an independent external report from Ward Solutions on 21 November 2018, as outlined in paragraph 26 above.

44. The report to the DES further stated that CDETB had requested Ward Solutions to extend its forensic work in relation to the website, its webserver and the stored data it contained, with a report due by mid-January 2019. Once the report on that work was complete, CDETB expected to be in a position 'to make an informed decision on the risk to the rights and freedoms of affected data subjects before deciding whether to notify them of the security incident.'[32]

45. On 15 January 2019, the DPC emailed CDETB giving a direction under Article 34(4) GDPR to communicate details of the breach to data subjects:

> On further review of your report, this office [is] of the opinion that the potential risk to the rights and freedoms of affected data subjects could be ***severe***. This opinion was formed due to the nature of the breach, and the nature of the data which you have indicated may have been subject of this breach. Therefore, this office is now issuing you as the data controller a direction that contact is to be made directly with all affected data subjects under the provisions of Article 34(4) of the GDPR. It is also noted that this office is also of the opinion, based on the current information provided that the conditions of Article 34 (3) have yet to be met and further more specific details may be required.[33]

46. In the same email, the DPC also asked CDETB for confirmation of the following:

- the time-frame in which CDETB intended to notify all affected data subjects;
- the date contact was made with all affected data subjects;
- the method(s) of communication which was utilised to contact all affected data subjects;
- details of any specific recommendations or advice provided to data subjects to mitigate the risks they may experience as the result of this incident. A copy of the template communication which issued;
- a copy of the template communication which issued;

---

[32] Confidential Report CDETB_SUSI to DES 14 December 2018, 6 (received by DPC 20 December 2018).

[33] Email DPC to CDETB, DPC Direction to SUSI, 15 January 2019. Emphasis in original.

- an update on the forensic report that CDETB had expected to receive in mid-January 2019.

47. On 16 January 2019, CDETB responded, asking the DPC whether the direction to notify data subjects was based solely on the original breach notification/report submitted on 16 November 2018, or if the DPC had taken into account the contents of the report to the DES.[34] CDETB stated that the report to the DES, based on the Ward Solutions report of 3 December 2018, indicated that the identified nature of the SUSI website security issue had changed substantially since the breach notification of 16 November 2018. However, CDETB did not provide the DPC with an update on its examination of the two datasets it had previously stated were central to its determination of the risk to the rights and freedoms of data subjects affected by the breach. CDETB stated that it expected the updated Ward Solutions report within the week.

48. On 22 January 2019, SUSI's Head of Operations contacted the DPC Breach Notification Team by telephone seeking to explore the DPC's rationale for directing CDETB to notify data subjects of the breach. The Head of Operations informed the DPC that CDETB was not going to notify data subjects pending receipt of the expanded Ward Solutions report, and would write to the DPC expanding on its response of 16 January 2019.[35]

49. On 31 January 2019, CDETB emailed the DPC reiterating its view that the risk posed by the breach did not pose a sufficient degree of risk to require communicating information about it to data subjects.[36] The correspondence included:

- a summary of CDETB's report to the DES (discussed in paragraph 42 above) and
- a copy of the final forensic report by Ward Solutions.[37]

b) Commencement of the Inquiry

50. The DPC issued an Inquiry Commencement Letter (**'the Commencement Letter'**) by email and registered post to CDETB on 19 July 2019. This notified CDETB that the DPC had commenced an Inquiry under and in accordance with section 110(1) of the 2018 Act.[38] Appendix 1 to the Commencement Letter included a request for information in the form of a series of questions. The DPC asked CDETB to provide responses by 1 August 2019.

---

[34] Email CDETB Response to Direction, 16 January 2019.

[35] DPC Note on Phone Call from CDETB-SUSI, 22 January 2019.

[36] Email CDETB to DPC, Update on Investigation, 31 January 2019.

[37] Incident Response Investigation Report from Ward Solutions (received by DPC 31 January 2019).

[38] DPC to CDETB, Commencement Letter, 19 July 2019.

51. The DPC's decision to commence the Inquiry was taken having regard to the circumstances of the personal data breach notified by CDETB. The Commencement Letter informed CDETB that the inquiry would examine whether or not CDETB 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 CDETB in that context.

52. The Commencement Letter stated that the Inquiry would formally document the facts as they related to the subject of the Inquiry. That in turn would lead to a draft inquiry report, on which CDETB would be invited to make submissions, and ultimately to a final inquiry report that would be submitted to the DPC's decision-making process. The relevant facts confirmed to the DPC via written responses provided by CDETB were set out in the Commencement Letter. The facts, as established during the course of the Inquiry, are set out in this Decision.

53. On 1 August 2019, CDETB provided its responses to the Commencement Letter. This included responses to requests for information in Appendix 1, together with supporting documents.

54. The DPC wrote to CDETB on 22 May 2020[39] seeking information on measures in place before the security incident (malicious files present on the SUSI webserver discovered between 14 and 16 October 2018) to comply with Article 32 GDPR, with reference to the principles set down in Article 5(1)(f) and Article 5(2) GDPR, in terms of:

- An assessment of the risks of varying likelihood and severity associated with the forms of data processing at issue in the breach.
- Appropriate technical and organisational measures to counter those risks.
- Capability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- Processes for regular testing, assessment and evaluation of the effectiveness of the technical and organisational measures for ensuring the security of the processing.

55. The DPC further requested the following documentation to support CDETB's submission of 1 August 2019:

- A copy of any signed service level and/or support agreement that was in place between CDETB and exSite before the security incident discovered between 14 and 16 October 2018.
- A copy of the document that demonstrates exSite had signed up to CDETB's data processing terms, in compliance with CDETB's third party engagement

[39] Letter DPC to CDETB, Article 32 Questions, 22 May 2020.

protocol, prior to the security incident that was discovered between 14 and 16 October 2018.

56. On 8 June 2020,[40] CDETB provided its response, which included supporting documents, including the SUSI-exSite Support Agreement 2015. CDETB listed documents it viewed as specifically relevant to ensuring the security of data processing systems within SUSI at the time and prior to the security incident:
    - CDETB IT Business Continuity/Disaster Recovery Plan (Revised November 2018);
    - DR Run Book November 2018;
    - CDETB-SUSI ICT BCP- DR 2018 - Audit Version (Revised August 2018);
    - CDETB ICT Usage Policy (Revised April 2018);
    - Records Management Policy and Schedule (May 2018);
    - Data Protection Policy (June 2018);
    - CDETB IT Security Policy (Revised July 2018); and
    - Data Breach Protocol (June 2018).

57. Having received CDETB's submissions, the DPC prepared a draft inquiry report (**'the Draft Inquiry Report'**) to document the relevant facts established and the issues that fell for consideration by the DPC for the purpose of making a decision under section 111 of the 2018 Act in respect of this Inquiry. The DPC furnished CDETB with the Draft Inquiry Report on 14 October 2020 and invited CDETB's submissions on any inaccuracies and/or incompleteness in the facts.

58. On 12 November 2020, CDETB provided comments on the Draft Inquiry Report.[41] The comments included clarifications of matters discussed in the Draft Inquiry Report, namely, the precise time when a potential data breach was identified, communication of the breach to affected data subjects and the adequacy of measures implemented by CDETB in respect of the SUSI website. Those comments were analysed and the DPC has considered them as part of this Decision.

59. On 16 December 2020,[42] CDETB informed the DPC that CDETB had notified all the affected data subjects on that date, including details of the methods of communication and details of specific recommendations or advice given to data subjects to mitigate the risks they may experience as a result of the incident. The DPC has considered that information as part of this Decision.

60. Having considered CDETB's comments on the Draft Inquiry Report, a final inquiry report was prepared, which issued to the DPC's decision-makers on 30 November 2020 (**'the**

---

[40] CDETB to DPC, Response to Article 32 Questions, 8 June 2020.

[41] CDETB-SUSI to DPC Response to Draft Inquiry Report, 12 November 2020.

[42] Email from Head of SUSI to DPC, 16 December 2020.

Final Inquiry Report'). The DPC wrote to CDETB on 21 March 2024, notifying CDETB of the commencement of the decision-making stage of the Inquiry. The Inquiry team also provided CDETB with the Final Inquiry Report.

61. The DPC issued a Draft Decision to CDETB on 21 February 2025 and requested CDETB to make submissions on that Draft Decision. CDETB provided submissions on 20 March 2025. The DPC has carefully considered all of CDETB's submissions in making this Decision.

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

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

63. The scope of the Inquiry, which was set out in the Inquiry Commencement Letter, was to examine whether or not CDETB has 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 has been contravened by CDETB, in that context.

64. The temporal scope of the Inquiry concerns the period from 25 May 2018 to 16 December 2020.

65. Having regard to the Commencement Notice, this Decision has considered CDETB's compliance with its obligations under Articles 5(1)(f), 32(1), 32(2), 33(1), 34(1) and Article 34(4) GDPR.

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

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

67. Article 4(1) GDPR defines 'personal data' as follows:

> 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

68. The material scope of the GDPR under Article 2 applies to processing of personal data. The personal data that are processed by CDETB via its website, including personal details of applicants, their nationality and residency, course details, previous education and other sources of financial support of applicants, details of dependent children and relevant persons and income details of parent and guardians, spouses, civil partners or cohabitants, as applicable[43] all come within the definition of personal data in Article 4(1) GDPR. In addition, according to the breach notification,[44] the following special categories of data were disclosed: data revealing racial or ethnic origin and health data.

69. Article 4(7) GDPR defines 'controller' as:

> the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data...

Based on the powers of CDETB under the Student Support Act 2011 and the information provided to the Inquiry concerning SUSI and CDETB's operation of it, the DPC is satisfied that CDETB is the controller of the personal data that were the subject of the personal data breach notification.

70. Article 4(12) GDPR defines a 'personal data breach' as:

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

As the breach notified by CDETB arose from unauthorised access to CDETB's server, and allowed unauthorised access to personal data processed by CDETB, the DPC is satisfied that the incident notified by CDETB comes within the GDPR's definition of a personal data breach.

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

> processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

---

[43] https://www.susi.ie/how-to-apply/your-new-application-form-guide-/ (retrieved 6 August 2024).

[44] Breach Notification Form, 16 November 2018.

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

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

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

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

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

75. Article 34 GDPR places obligations on a data controller with regard to communicating a personal data breach, as follows:

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

...

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

F. Issues for Determination

76. Having reviewed the Commencement Notice, the Final Inquiry Report, and all of the information gathered during the Inquiry, the DPC considers that the following issues arise for determination in this Decision:

Issue 1: Articles 5(1)(f), 32(1) and (2)

Whether CDETB had appropriate technical and organisational measures in place to ensure the security of the personal data being processed, ensured the ongoing confidentiality, integrity, availability and resilience of its processing systems and services, and took into account the particular risks presented by the processing being carried out when assessing the appropriate level of security.

Issue 2 – Article 33(1) GDPR

Whether CDETB's notification of the breach to the DPC met its obligations under this Article.

Issue 3 – Article 34(1) GDPR

Whether CDETB fulfilled its obligation to communicate the personal data breach to the data subjects without undue delay.

Issue 4 – Article 34(4) GDPR

Whether the DPC's direction to CDETB on 15 January 2019 to notify data subjects of the breach and to provide all information required under Article 34(3) GDPR was properly made and, if so, whether CDETB had complied with that direction.

77. Therefore, having considered the Commencement Letter, the Draft Inquiry Report, CDETB's submissions thereon, and the other relevant materials, the DPC must determine in this Decision whether CDETB has complied with its obligations under Articles 5(1)(f), 5(2), 32(1), 32(2), 33(1), 34(1) and 34(4) GDPR.

G. Analysis of the Issues for Determination

a) Issue 1: Articles 5(1)(f), 32(1) and 32(2) GDPR

78. Article 5(1)(f) GDPR provides for the principle of integrity and confidentiality and has been set out in paragraph 71 above.

79. Article 32(1) GDPR elaborates on the principle of integrity and confidentiality in Article 5(1)(f) GDPR by setting out criteria for assessing what constitutes 'appropriate security' and 'appropriate technical or organisational measures' and has been quoted in full in paragraph 72 above.

80. 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.

81. Article 32(2) GDPR provides:

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

i. Assessment of the Risks

82. The level of security that controllers and processors are obliged to implement must be appropriate to the risk posed to the rights and freedoms of natural persons by the personal data processing. Regarding CDETB's processing of personal data on its website, those risks include the risk of unauthorised access or disclosure of personal data to third parties. They also include risks of accidental or unlawful destruction,

alteration or loss of availability of the personal data processed on the website. The data processed included approximately 13,000 data subjects, identifiable by email address, who had submitted supplementary forms through the SUSI website during 2017 and 2018.[45] The personal data at risk due to the security incident, included data subject identity (name, surname, and birth date), PPSN, contact details, identification data and special categories of data such as data revealing racial or ethnic origin and health data.[46]

83. The SUSI website was not originally intended to process personal data. However, in April 2017, CDETB added functionality to enable the submission of supplementary requests and information through online forms provided on the website. Due to inadequate project scoping and risk assessment by CDETB, the personal data were being stored locally on the webserver[47] as well as being emailed to the final receiver, in this case SUSI.[48]

84. In implementing measures required by Articles 5(1)(f) and 32 GDPR, the controller must have regard to the risks of varying likelihood and severity for the rights and freedoms of natural persons posed by the processing.

85. Recital 75 to the GDPR provides examples of relevant risks to the rights and freedoms of natural persons:

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

---

[45] Confidential Report from CDETB_SUSI to DES, 14 December 2018 (received by DPC 20 December 2018).

[46] Breach Notification Form, 16 November 2018.

[47] SUSI Submission on Draft Decision, 20 March 2025, 4.

[48] CDETB Response to DPC Request of 27 November 2018, dated 5 December 2018, 5.

86. 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.

87. Therefore, in complying with Articles 5(1)(f) and 32, it is appropriate to first identify the risks to the rights of data subjects that a violation of the principles presents, and further to have regard to the likelihood and severity of those risks, and implement measures to effectively mitigate them.

88. It is necessary to carry out an objective assessment of the risks presented by the processing to determine the appropriate level of security. Risk must be assessed by reference to (i) the likelihood of the risk, and (ii) the severity of the risk to the rights and freedoms of natural persons. Hence, the risk assessment for CDETB's processing should have considered first the likelihood of unauthorised access to, or of alteration, destruction or disclosure of, personal and special category data. Secondly, the severity of that risk to the rights and freedoms of the data subjects should have been assessed. These objective assessments should have been made by reference to the nature, scope, context and purposes of the processing. In considering these factors, regard should also have been had to the quantity of personal data processed and to the sensitivity of those data.

89. CDETB was asked to provide information on the measures in place at the time of the notified breach to comply with Article 32 GDPR, by reference to the principle set down in Article 5(1)(f) GDPR, in terms of an assessment of the risks of varying likelihood and severity associated with the forms of data processing activities involved in the notified breach.[49]

90. In response, CDETB stated that 'the advice of independent data protection experts was sought from the earliest stages of the project'. CDETB added that it commissioned a review of data protection compliance in 2016, which 'included a revised assessment of data processing risks and recommended a number of additional and enhanced data protection measures in anticipation of the GDPR, which have been or are in course of being, implemented by CDETB and SUSI.'[50]

---

[49] Letter DPC to CDETB, Article 32 Questions, 22 May 2020.

[50] Response to Article 32 Questions, 8 June 2020.

91. According to CDETB, risk assessments were carried out and 'technical and operational measures implemented in respect of the processing of data by SUSI through its intended processes and channels'.[51] However, according to CDETB, a 'dedicated website was not contemplated on the establishment of SUSI in 2011 and therefore the assessment of risk specifically associated with the processing of data via a public website was not included in the independent expert advice sought at that time.'[52] In short, because the processing via the website which gave rise to the breach was not intentional, no risk assessment was carried out.

92. CDETB stated it performed a risk assessment of the online form template data fields in line with a risk assessment framework from the European Union Agency for Network and Information Security Agency (**'ENISA'**).[53] CDETB identified from this that ''if the data contained in these fields were breached, the risk to data subjects would be considered to be high in accordance with the strict criteria of that framework''.[54] However, the assessment that must be conducted under Article 34 GDPR is distinct to that provided for by the ENISA guidelines and this risk assessment was carried out after the breach.

93. Regarding the application of Article 5(1)(f) and Article 32 GDPR, in the circumstances, the DPC finds that CDETB's processing of personal and special category personal data created a high risk to the rights and freedoms of natural persons in terms of both likelihood and severity. The severity of these risks was high in circumstances where CDETB's processing affected a significant amount of personal data and some special category data, access to which ought to have been limited to appropriate persons authorised by CDETB.

94. The SUSI website, which was storing personal data uploaded to it, was found to have malicious software on it, a WSO Shell. Ward Solutions executed the WSO Shell and performed the operations associated with it. This included demonstrating that it would have been 'possible to retrieve sensitive documents using the WSO Shell'.[55] The risk arising from this processing of personal data on the CDETB website included that an unauthorised person could gain access to applicants' data, for example, using the WSO Shell, which would pose a high risk to the rights and freedoms of data subjects, including loss of control over the data subjects' personal data, the possibility of phishing attacks and identity theft.

---

[51] Response to Article 32 Questions, 8 June 2020, 2.

[52] Response to Article 32 Questions, 8 June 2020, 2.

[53] EU Agency for Network and Information Security (ENISA) Recommendations for a methodology of the assessment of severity of personal data breaches Working Document, vl.0, December 2013.

[54] CDETB Response Letter to Direction, 31 January 2019, 2.

[55] Ward Solutions Report, (received by DPC 5 December 2018), 5.

95. The likelihood of the risks to the rights and freedoms of data subjects was also high. The DPC makes this finding in light of the quantity of the personal data processed, the purposes of that processing, and the fact that the processing took place on a public-facing web-server, where there was a significant risk of cyber-attacks. This processing affected a significant amount of personal data and some special category data, access to which ought to have been appropriately restricted by CDETB. Therefore, having regard to this high risk, it was incumbent on CDETB to implement appropriate technical and organisational measures, as set out in Article 32 GDPR.

96. The DPC finds that CDETB's processing of personal and special category personal data on the CDETB website created a high risk to the rights and freedoms of natural persons in terms of both likelihood and severity. Insofar as CDETB was not aware that personal data were being stored locally on the webserver from April 2017, there were no technical and organisational measures in place to ensure that these personal data were being kept secure. Therefore, the risk of unlawful access to the personal data processed on the website was high in the absence of appropriate technical and organisational measures. The severity of this risk was also high as some of the data processed included special category data.

ii. Measures Implemented by CDETB to Address the Risks

97. The principle of integrity and confidentiality in Article 5(1)(f) GDPR requires that the controller 'ensures appropriate security of the personal data when processing using appropriate technical or organisational measures'. Article 32(1) GDPR requires the controller to assess the risk to data subjects of the particular processing and to implement 'appropriate technical and organisational measures to ensure a level of security appropriate to the risk', taking into account various factors. Article 32(2) GDPR expressly requires the risk presented by unauthorised disclosure or access to be considered when assessing the appropriate level of security.

98. The original SUSI website did not have functionality to upload documents, however, in April 2017 this functionality was added. Once documents were uploaded to the webserver, an email was automatically sent to SUSI. The personal data should then have been automatically deleted from the webserver. However, instead the personal data continued to be stored locally on the webserver.[56] A risk assessment should have been carried out and organisational and technical measures should have been put in place to protect these data, including, for example, the use of firewalls, restriction of access to the webserver via whitelisting of IP addresses, automatic software updates and regular scanning.

[56] CDETB Response to DPC Request of 27 November 2018, dated 5 December 2018, 7-8.

99. The appropriate measures to address the risk need to be considered in light of the high risk to the rights and freedoms of the data subjects involved in the processing of personal data, including special category data.

100. CDETB has not demonstrated what IT provisioning risk analysis it undertook to identify, analyse or address any threats to its processing activities in relation to the susi.ie website prior to the breach. A comprehensive risk assessment requires an assessment of the probability of an incident and of the potential consequences to the data subjects affected. However, CDETB was unaware that personal data were processed on its SUSI webserver, as it stated itself to the DPC:

> CDETB/SUSI wishes to clarify that the hyperlinks used were implemented by an external service provider. As we noted in our previous submission to the DPC on 1 August 2019, this implementation caused the system to store data on the webserver, which was not intended by CDETB/SUSI. Additionally, CDETB/SUSI submits that it was not initially aware of this exposure as it was relying on the technical expertise of the external service provider.[57]

As a result, CDETB failed to take account of the risks of unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed on the webserver, that were posed by its processing.

101. CDETB's submissions outlined the technical and organisational measures that it had in place at the time of the personal data breach to ensure the ongoing confidentiality and integrity of its processing of personal data. These measures can be categorised within the areas of scope specified in the Commencement Letter as follows:

a) Data protection governance
b) Security of personal data
    i. Technical measures
    ii. Organisational measures
c) Record of processing activities

Security of personal data

Technical measures

102. In addition to the policies and procedures noted above, CDETB described the technical measures that it stated were in place at the time of the breach. These included:

[57] CDETB-SUSI Response to Draft Inquiry Report, 12 November 2020.

- a central dashboard called Plesk, which controls the updating and monitoring of all the client websites, including the SUSI website.
- remote access to ICT systems, which is provided by means of a Secure Sockets Layer Virtual Private Network (SSL VPN).
- a server firewall.

103. CDETB had not implemented measures around the archiving of access, event and error logs to store them or to protect them from later manipulation. This was noted in the Ward Solutions report which stated that '[t]he current Server is configured to hold up to two weeks of Apache access logs and then overwrite them' and 'there were no firewall logs available to investigate'. As a result, 'in the event of another compromise of the website there would be no evidence to investigate due to inadequate logs'.[58]

104. The Ward Solutions report stated that its analysis of the Apache access logs showed no evidence of malicious activity. However, the DPC notes that the Apache access logs available for analysis were only for the period from 29 April to 7 May 2018 (i.e. 9 days). Any exfiltration of personal data could have taken place prior to or after this period, given that the WSO Shell was present on the webserver from 12 January to 16 October 2018.

105. CDETB's failure to implement measures around the archiving of access, event and error logs during the temporal scope resulted in a failure to implement appropriate technical measures in the circumstances. The DPC notes that CDETB has stated that, since the data breach, CDETB has implemented audit logs which enable the monitoring of user activity within the system.[59]

106. The key security breach remains the fact that the server processing personal data (collecting from the web and forwarding to another machine) had been infected by malware. For example, the header.php was modified on 27 April 2018 when JavaScript was injected into it. When activated, the malicious JavaScript within the header.php file would try to access a site called boxtubex.com. The Ward Solutions updated report stated that its threat intelligence indicated that boxtubex.com had been associated with phishing campaigns and identified in malicious campaigns to disseminate malware.[60]

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

---

[58] CDETB-SUSI Response to Draft Inquiry Report, 12 November 2020, para 2.5, recommendation R.2.

[59] CDETB-SUSI Submission on Draft Decision, 20 March 2025, 15.

[60] Incident Response Investigation Report from Ward Solutions, 19 (received by DPC 31 January 2019).

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

...

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

108. In 2015 CDETB carried out a PEN test[61] and security audit of its susi.ie website and webserver and the findings and recommendations from the report were implemented by exSite at the time. However, no PEN test was carried out after the added functionality enabling applicants to upload forms was introduced on the website in 2017. The DPC notes that CDETB stated that, following the breach, a Data Processing Agreement was signed between SUSI and exSite Communications Ltd on 7 February 2020. The DPC also notes that, according to CDETB, it has since launched a new website with a new website provider, and that it engaged an independent third-party cyber-security company to conduct a penetration test of the website.[62]

109. CDETB did not conduct any analysis to determine whether technical security had been negatively affected when functionality was added in April 2017 to the SUSI website which allowed applicants to submit supplementary requests and information through online forms.

110. CDETB did not implement measures around the archiving of access, event and error logs to protect them from later manipulation. This was noted in the Ward Solutions report in that in the event of another compromise of the website 'there would be no evidence to investigate due to inadequate logs'.

111. Moreover, the Ward Solutions report made a number of recommendations to CDETB to prevent a reoccurrence of the security breach, including the following:

- Configure the new server to ensure that logs are kept for at least six months;
- Install a Web application Firewall in front of the Web servers;
- Move the logs to a centralised logging server;
- Ensure all servers are hardened against a SUSI hardening guide; and
- Test security on servers regularly to ensure continued compliance (e.g. annually and after significant change.)

112. Recalling that it was on 14 November 2018 that CDETB discovered that uploaded forms and documents were being stored locally on the webserver, CDETB could not have assessed the appropriate level of security required to address the risks to the data

[61] https://www.webopedia.com/TERM/P/penetration-testing.html

[62] CDETB-SUSI Submission on Draft Decision, 20 March 2025, 12.

subjects of the storage of personal data on that webserver system in circumstances where CDETB was not even aware that it was processing personal data on that system.

113. CDETB did not sufficiently archive access, event and error logs to store them or to protect them from later manipulation. This meant that in the event of unauthorised access to the webserver, there was inadequate storage of logs to investigate this. The server was infected with malware, which put the personal data at risk. After the SUSI website was upgraded to allow the uploading of documents, no PEN testing was carried out to identify any vulnerabilities in the system. It was only in November 2018 that CDETB discovered that personal data were being stored on the webserver. Therefore, it was not possible for CDETB to have appropriate security measures in place to protect personal data that CDETB was not even aware that it was processing in this manner. The technical measures demonstrated by CDETB during the course of the Inquiry, as discussed above, do not show sufficient regard to the nature of the risks posed by its processing having regard to the state of the art, and other relevant factors. Therefore, the DPC finds that the technical security measures in place at the time of the breach did not meet the standard required by Article 5(1)(f) or Article 32(1) GDPR.

Organisational measures

114. CDETB outlined that it had a range of organisational measures relating to security,[63] including the following:

- CDETB IT Security Policy document;
- Web Process with Calendar and SOP-C-0007 Website Content Management;
- Attached Web Process document;
- Project calendar – planning meetings and key dates;
- Project plan – prioritised lists of ICT and non-ICT change Items;
- CDETB Data Breach Protocol;
- implementation of data processing agreements with data sharing partners, outsourced suppliers and other parties;
- high-profile deployment of SUSI-specific DP statement and privacy statement throughout the application submission process;
- segregated data entry for parties to application form;
- consent framework for discussion/disclosure of application/data with and across;
- applicant parties and also with third parties;
- DP protocols deployed on inbound/outbound calls;

[63] Response to Commencement Letter, 1 August 2019.

- consent protocol for receipt and processing of sensitive personal information;
- data minimisation in exchanges with data sharing partners;
- emphasis on clean desk and substantially paperless assessment work practices; and
- internal quality review process includes review of DP rigour in application casework.

115. CDETB stated that its ICT department is responsible for maintaining and supporting all SUSI ICT systems alongside the underlying architecture and infrastructure on which its systems run. The department is headed by an ICT Manager who manages a multidisciplinary ICT team, which covers the disciplines of client/server administration, networking/security, business analysis and core business systems support.[64]

116. CDETB stated that exSite's Plesk dashboard controls the updating and monitoring of all its client websites. Any updates, security scans and uptime monitor notifications come through this dashboard, which is monitored by exSite's support team. Configuration changes required by the SUSI unit are submitted via the nominated SUSI manager to exSite directly. A ticket is raised and SUSI is kept informed of progression and signs off on drafts.

117. CDETB stated that it permits SUSI staff members (as a unit of CDETB) to have remote access to its ICT systems. CDETB further stated that this remote access is provided by means of an SSL VPN. Access is controlled to provide specific user Remote Desktop Access (RDP) to specific resources only. Remote Access uses two-factor authentication as an additional security layer through One Time Password (OTP) authentication delivered via cellular SMS.[65]

118. CDETB had organisational measures in place to ensure the security of applicants' personal data. However, the failure to be aware of what processing was being carried out via the SUSI website shows a lack of organisational measures in place to test and check what data processing was being carried out and how. The lack of PEN testing after the increased website functionality was added in 2017 greatly increased the possibility of a data breach occurring, as the purpose of webserver PEN testing is to identify any vulnerabilities before they are exploited by a threat actor.

119. Similarly, the failure of audit log management, that is, to adequately archive logs rendered the discovery of the scope and nature of the breach much more difficult.

---

[64] Response to DPC Request of 27 November 2018, dated 5 December 2018, Q 2.

[65] Note that this information was corrected on the basis of page 7 of the submission on the Draft Inquiry Report, which highlighted previous correspondence from CDETB/SUSI of 2 December 2018.

Again, in circumstances where the data being processed gave rise to a high risk to data subjects, CDETB should have implemented measures to satisfy Article 32(1)(d) GDPR and Article 5(1)(f) GDPR. Article 32(1)(d) requires a controller to have, where appropriate:

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

120. As outlined above, CDETB had some organisational security measures in place at the time of breach. However, the lack of controls and reviews means that adequate organisational measures were not in place to ensure the ongoing security of personal data being processed, namely, CDETB being unaware of the processing being carried out, the lack of PEN testing and inadequate error log management. Therefore, the DPC finds that organisational measures in place at the time of the breach did not meet the standards required by Article 5(1)(f) or Article 32(1) GDPR.

Data protection governance

121. CDETB outlined[66] that it had a range of policies and procedures in relation to data protection governance. Its data protection governance structure included:

- setting up of dedicated Governance and Compliance Unit within SUSI having specific responsibility for DP oversight and compliance;
- appointment of senior manager at Assistant Principal Officer level within SUSI overseeing Data Protection, Compliance and Governance;
- appointment and training of data stewards;
- deployed governance, ICT, process and physical security/access controls, procedures and policies to support effective management and protection of data; and
- commissioning of external audit of SUSI to identify the level of compliance with the 2018 Act and readiness for GDPR and implementation of recommended changes arising.

122. In the same communication, CDETB also stated that it had the following policies and procedures in place:

- deployment of DP governance controls through staff handbook and related compliance measures including declaration of interests, confidentiality agreement, etc. for staff;

[66] Response to Commencement Letter Appendix, 1 August 2019.

- implementation of DP-specific Standard Operating Procedures ('SOPs') for data breaches and subject access requests;
- implementation of DP protocols in SOPs for internal processes and external (customer) interfaces;
- joint data controller agreement with the Department of Education and Skills; and
- data privacy impact assessments implemented through project planning for annual and longer term change configuration projects.

123. CDETB had a range of data protection governance policies and procedures in place to ensure the accuracy and security of customers' personal data. However, CDETB discovered on 14 November 2018 'that applicant data being submitted through contact forms and upload documents facility online was being stored on the webserver',[67] instead of being forwarded to SUSI and deleted from the web server. This applicant data retained on the server was not encrypted.

124. As noted above, CDETB was unaware of this retention or of the use by an external service provider of hyperlinks directly to the stored documents and information on the webserver. Prior to this discovery on 14 November 2018, CDETB was unaware that personal data were processed on its SUSI webserver and it failed to analyse risks to the rights and freedoms of the data subjects of processing in that manner. Appropriate technical and organisational measures in the circumstances in light of the high risk included governance measures that clearly documented for CDETB, as a data controller, where its storage of personal data occurred. In circumstances where CDETB failed to implement such governance measures, it did not put in place adequate security measures to ensure the data could not be accessed by or disclosed to unauthorised persons. This is in contravention of CDETB's obligations under Articles 5(1)(f) and 32 GDPR, which requires CDETB to carry out processing in a manner that ensures appropriate security of the personal data.

125. Therefore, the DPC finds that CDETB did not implement appropriate data protection governance measures to meet the standard required in light of the risk posed by the processing.

iii. Processes to test, assess and evaluate effectiveness of measures

126. The severity of the risk to the rights and freedoms of natural persons arises from CDETB's processing of personal data (including special category data) via its website. The technical and organisational measures that CDETB implemented should have been

[67] Breach Notification Form, 16 November 2018, 3.

appropriate to the risks to the rights and freedoms of those data subjects arising from such processing. CDETB had an obligation to run tests on their technical and organisational measures to assess, evaluate and, where appropriate, improve, the effectiveness of the measures implemented pursuant to Article 32(1)(d) GDPR.

Testing data protection governance

127. Creating policies and procedures is essential for implementing an appropriate level of security. However, policies and procedures alone are not sufficient to mitigate the risk to data subjects. A controller must regularly assess and evaluate the effectiveness of measures in place. Therefore, there must be an ongoing and verifiable oversight of how the staff members give effect to the controller's policies and procedures. CDETB's lack of awareness of the extent of data processing being carried out on the webserver indicates that insufficient testing of data protection measures was in place.

Testing security of personal data

128. Article 32(1)(d) GDPR requires that, where appropriate, the controller shall implement technical and organisational measures to include a process for **regularly** testing, assessing and evaluating the effectiveness of existing security measures. Such testing, assessing and evaluating applies to both **technical and organisational measures**. Personal data breaches may cause significant harm to data subjects and, pursuant to Article 32(1)(d) GDPR, controllers must take the initiative to test, assess, and evaluate their organisational and technical security measures.

Technical measures

129. An appropriate level of security includes **technical measures** that have, among other things, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. It is apparent that technical measures were not in place to ensure appropriate archiving of firewall and Apache access logs and that CDETB's failure to be aware of what processing was being carried out via the website introduced a risk of allowing unauthorised access to applicants' data.

Organisational measures

130. CDETB was not aware that its webserver was being used to process applicants' personal data. This indicates that CDETB was not carrying out appropriate testing of organisational measures, as such weaknesses or gaps in its organisational measures were not identified until after CDETB became aware of the breach. Therefore, the DPC

finds that the organisational security measures in place at the time of the breach did not meet the standard required by Articles 5(1)(f) and 32(1) GDPR and that these Articles were infringed. The DPC notes that CDETB has stated that, since the breach, the SUSI Governance Unit has implemented processes and procedures to strengthen the management and safeguarding of personal data, including a comprehensive corporate policy suite and a risk management policy. These policies are reviewed and updated on a scheduled basis. In addition, CDETB stated that in 2024 it launched a new data protection training programme for all staff and targeted training to staff in high-risk teams. Cyber security training is currently offered to staff across the organisation periodically, including phishing exercises.[68]

iv. Findings

Articles 5(1)(f) and 32(1)

131. As outlined above, CDETB failed to adequately archive access, event and error logs, did not undertake PEN testing, did not operate a web application firewall, and was not aware that documents uploaded to SUSI were being retained on the webserver. These all contributed to the vulnerabilities that permitted the breach to occur and show that processing was not in accordance with the principle of integrity and confidentiality prescribed by Article 5(1)(f) GDPR.

132. Similarly, the absence of technical and organisational measures such as regular and secure archiving of logs, encryption of personal data on the webserver, and regular testing, assessment and evaluation of the effectiveness of those measures, all point to a failure by CDETB to implement measures to ensure the security of processing appropriate to the risk posed by its processing, as required by Article 32(1) GDPR.

133. In its submissions on the Draft Decision, CDETB stated that it accepts these findings and furthermore:

> accept[s] this data breach occurred in 2018 as a result of our failure to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by our processing of personal data on the SUSI website's online supplementary form functionality.[69]

134. CDETB further stated in those submissions that in January 2023, SUSI launched a new website with a new website provider, which is certified to the ISO 27001 international standard and is audited twice a year. Improved security measures which CDETB stated

[68] CDETB-SUSI Submission on Draft Decision, 20 March 2025, 11-12.

[69] CDETB-SUSI Submission on Draft Decision, 20 March 2025, 2.

had been implemented after the breach include web filtering, patching, scans for malware and implementation of an information security management system. Furthermore, the SUSI website is no longer used for the submission of supplementary forms.[70]

135. Although the DPC acknowledges the relevant actions and measures to mitigate the issues after the breach, referred to by CDETB in its submissions on the Draft Decision, for the above reasons, the DPC finds that CDETB infringed Articles 5(1)(f) and 32(1) GDPR at the material time by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its processing of personal data on its website.

Article 32(2)

136. The DPC also finds that CDETB infringed Article 32(2) GDPR by failing to assess the appropriate level of security, including by not taking account of the risks that were presented by processing from unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed on the webserver. CDETB stated, in its submissions on the Draft Decision, that it accepts this finding.[71]

b) Issue 2 – Article 33(1) GDPR

i. The Obligation to Notify Without Delay

137. As set out in paragraph 74 above, Article 33 GDPR requires a controller to notify the supervisory authority of personal data breaches 'without undue delay and, where feasible, not later than 72 hours after having become aware of it'.

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

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

139. Article 33(1) requires notifications to be made 'without undue delay.' What constitutes undue delay must be assessed from when CDETB became aware of the personal data breach. The European Data Protection Board (**'EDPB'**) addressed the meaning of 'undue delay' in the context of the requirement to communicate a breach to affected

[70] CDETB-SUSI Submission on Draft Decision, 20 March 2025, 14-15.

[71] CDETB-SUSI Submission on Draft Decision, 20 March 2025, 9.

individuals in its 'Guidelines on Personal Data Breach Notification under GDPR' (**'EDPB Breach Notification Guidelines'**).[72] The EDPB Breach Notification Guidelines outline reasons for this requirement:

> 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 focus of the notification requirement is to encourage controllers to act promptly on a breach, contain it and, if possible, recover the compromised personal data, and to seek relevant advice from the supervisory authority. Notifying the supervisory authority within the first 72 hours can allow the controller to make sure that decisions about notifying or not notifying individuals are correct.[73]

140. The EDPB Breach Notification Guidelines further provide that:

> ...a controller should be regarded as having become 'aware' when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.
>
> However, as indicated earlier, the GDPR requires the controller to implement all appropriate technical protection and organisational 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. 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.[74]

141. Recital 87 GDPR states:

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

---

[72] EDPB, 'Guidelines 9/2022 on personal data breach notification under GDPR' (Version 2.0, Adopted 28 March 2023), available at https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en

[73] Guidelines 9/2022, para 58.

[74] Guidelines 9/2022, paras 31-32. Emphasis added.

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

142. The EDPB Breach Notification Guidelines state that:

> ...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.[75]

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

ii. The breach notification

144. On 16 November 2018, the DPC received a breach notification (BN-18-11-258) from CDETB relating to a security incident on its www.susi.ie website. The notification stated that CDETB had discovered in November 2018 that its web server was retaining personal data in the form of contact forms and uploaded documents. CDETB stated that this discovery, combined with its detection of malicious malware contained on its web server in October 2018, now resulted in a realisation that personal data of grant applicants were being put at risk.

145. CDETB stated that it became aware between 14 and 16 October 2018 that a breach relating to the security of the processing of personal data had occurred on its SUSI webserver. CDETB requested a report from exSite who performed an internal investigation. On 19 October 2018, CDETB received a report on that investigation from exSite and an additional report that exSite had commissioned from Wordfence. The exSite report identified a number of malicious files present on the SUSI website server.

[75] Guidelines 9/2022, paras 11 - 12.

146. The breach notification received by the DPC on 16 November 2018 stated that the incident was detected on 14 November 2018, notwithstanding that CDETB had engaged exSite (and exSite had engaged Wordfence) to investigate the incident in October 2018, a month earlier. That breach notification offered no explanation of the delay from the date when CDETB became aware of the incident on 16 October 2018 to the date of notification to the DPC on 16 November 2018.

147. Recital 85 GDPR states 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 such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

Controllers are not obliged to notify the DPC if a personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. However, the DPC is satisfied that the personal data breach in this case did result in such a risk to rights, as the data security incident discovered on the SUSI webserver on 16 October 2018 exposed the personal data of both applicants and associated parties whose affairs were dealt with in submitted documents and information. CDETB was therefore obliged to notify the DPC without undue delay.

148. In assessing risk, objective regard must be had to both the likelihood and severity of the risk to the rights and freedoms of data subjects. The personal data affected by the breach notified on 16 November 2018 included sensitive personal data, which increased the risk to data subjects. It is also appropriate to have regard to the number of affected individuals. Approximately 13,000 data subjects, identifiable by email address, had submitted supplementary forms through the SUSI website during 2017 and 2018.[76]

149. It is also appropriate to have regard to whether the personal data have come into the possession of individuals whose intentions are unknown or possibly malicious, which may result in exposing data subjects to identity theft, financial fraud and phishing attacks. In this regard, the breach occurred due to the compromise of the website and the malicious insertion of malware.

[76] Confidential Report from CDETB-SUSI to DES, 14 December 2018, 2 (received by DPC 20 December 2018).

iii. Finding

150. In the circumstances, the DPC is satisfied that the personal data breach resulted in a risk to the rights and freedoms of data subjects, including but not limited to the risk of phishing attacks utilising the personal data compromised. Therefore, the DPC finds that CDETB was obliged to notify the DPC of the personal data breach without undue delay and that its failure to do so was in breach of Article 33(1) GDPR. In its submissions on the Draft Decision, CDETB stated that it accepts the DPC's finding and acknowledged that 'SUSI should not have awaited the outcome of the investigation completed by exSite before notifying the DPC.'[77]

c) Issue 3 – Article 34(1) GDPR

151. Article 34(1) GDPR states:

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

152. A key issue in this Decision is whether CDETB was required to send a communication to data subjects in respect of the personal data breach on the grounds the breach was 'likely to result in a high risk to the rights and freedoms of natural persons'. Recital 86 GDPR states that the purpose of this is to allow the data subject 'to take the necessary precautions'. Determining whether the personal data breach met the 'high risk' threshold is integral to determining whether Article 34(1) is engaged in respect of the breach CDETB reported to the DPC on 16 November 2018.

153. The level of risk associated with any particular breach can be gauged with respect to the possible damage data subjects may suffer. Recital 85 gives examples of different types of damage a data subject may suffer as a result of a personal data breach:

> 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 or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

[77] CDETB-SUSI Submission on Draft Decision, 20 March 2025, 3.

154. The EDPB Breach Notification Guidelines state:

> Accordingly, when assessing the risk to individuals as a result of a breach, the controller should consider the specific circumstances of the breach, including the severity of the potential impact and the likelihood of this occurring.[78]

155. The specific factors to be taken into consideration when assessing the risk to individuals as a result of a personal data breach include:

- The type of breach;
- The nature, sensitivity, and volume of personal data;
- Ease of identification of individuals;
- Severity of consequences for individuals;
- Special characteristics of the individual;
- Special characteristics of the data controller; and
- The number of individuals affected.[79]

156. In determining if CDETB has infringed Article 34(1) GDPR, consideration must also be given to Article 34(3). Article 34(3) lists a number of conditions, any one of which may exempt CDETB from having to send a communication to each data subject.

157. The breach was discovered as a result of CDETB finding malicious malware on its web server in October 2018. CDETB had identified that the following identifying information relating to individuals were at risk due to the security incident:

- Data subject identity (name, surname, birth date)
- PPSN (or other national identification number)
- Contact details
- Identification data (passports, licence data etc.)
- Economic or financial data
- Location data

It also included the following special categories of data:

- Data revealing racial or ethnic origin
- Health data[80]

158. In its breach notification, CDETB indicated that approximately 8,000 data subjects were potentially affected.[81] Following further analysis, CDETB stated that 13,000 data

---

[78] EDPB Breach Notification Guidelines, para 105.

[79] EDPB Breach Notification Guidelines, paras 106-108.

[80] Breach Notification Form, 16 November 2018.

[81] Breach Notification Form, 16 November 2018.

subjects had submitted supplementary forms through the SUSI website during 2017 and 2018 and were identifiable from e-mail addresses in those forms.[82] These 13,000 data subjects were therefore placed at risk by the security breach.

159. On 7 December 2018, SUSI's Governance & Compliance Manager informed the DPC that it would be informing data subjects of the personal data breach.[83] However, on 10 December 2018, SUSI's Head of Operations emailed the DPC to say that CDETB would not notify data subjects of the incident until it had considered legal advice it had received. CDETB indicated that this legal advice related to determining the level of any potential impact on the rights and freedoms of data subjects.[84]

160. On 14 December 2018, CDETB stated to the DPC that it was 'proceeding urgently with a detailed analysis of the data that may have been affected by the security incident' on the basis of the legal advice it had received. CDETB also stated that it had asked Ward Solutions to perform a forensic investigation of the SUSI website, its webserver and the stored data it contained. CDETB stated that it expected to receive the forensic report by mid-January 2019, '...whereupon SUSI may to [sic] be in a position to make an informed decision on the risk to the rights and freedoms of affected data subjects before notifying them of the security incident'.[85]

161. On 31 January 2019, after receiving the final Ward Solutions Incident Report, CDETB wrote to the DPC[86] stating that there was now:

> no evidence that data held on the SUSI Website webserver was accessed or viewed. It was on the basis of this determination by Ward Solutions (in conjunction with the other evidence available) that CDETB/SUSI determined that there was a low risk to the fundamental freedoms of the affected data subjects.[87]
>
> CDETB stated that in light of this, in its view, 'the threshold for notification to data subjects on the basis of there being a high risk to their rights and freedoms had not been met.'

162. The final Ward Solutions report states that Ward Solutions executed the WSO Shell and performed the operations associated with it. This included demonstrating that it would

---

82 Confidential Report from CDETB_SUSI to DES, 14 December 2018 (received by DPC 20 December 2018).

83 Response Intention To Communicate Data Breach To Data Subjects, 7 December 2018.

84 Update Inform DPC of Intention to Suspend Notifying Data Subjects, 10 December 2018.

85 Further Update re Potential Forensic Investigation of Website, 10 December 2018.

86 Response Letter to Direction, 31 January 2019.

87 Response to Commencement Letter Appendix 1, 1 August 2019.

have been 'possible to retrieve sensitive documents using the WSO Shell'.[88] Ward Solutions also states that 'while access to the uploaded documents was possible using the WSO shell, there is no evidence that the documents were accessed or viewed from the available logs'.[89] Typically, Apache access logs contain information about requests coming in to the webserver or requests processed by the webserver, while Apache error logs contain information about any internal errors encountered when the Apache web server starts or runs, as well as errors raised when processing a client request. According to Ward Solutions, there was no evidence of malicious activity on analysis of the Apache access logs. CDETB's conclusion that the data breach was not likely to result in a high risk to the rights and freedoms of natural persons was made on the basis that there was no evidence available in the logs that the data was accessed in line with the known function of the WSO Shell.

163. However, the Apache access logs available for analysis were very limited as they were only for the period from 29 April to 7 May 2018 (9 days). Any exfiltration of personal data could have taken place prior to or after this period, given that the WSO Shell was present on the webserver from 12 January to 16 October 2018. These insufficient logging levels, according to Ward Solutions, 'made it impossible to carry out a detailed investigation'.[90]

164. The absence of comprehensive access and error logs, along with the presence of malicious malware contained on the web server, leaves open the possibility that an external actor interfered with those logs to remove evidence of exfiltration or remote access to personal data.

165. Similarly, the absence of comprehensive webserver or firewall logs impeded the ability of CDETB to reconstruct events in relation to the security incident and to detect malicious actions such as exfiltration of personal data. The absence of those log files during extended periods when the malware was in place is not by itself evidence of unauthorised access or disclosure during the temporal scope of the Inquiry, but, as stated above, it leaves open the possibility that this occurred. That uncertainty is itself a risk arising from the breach.

166. The ability of a bad actor to store malware on the web server over an extended period itself indicates a significant lapse in security. CDETB's analysis of the risk profile concentrated on access to the student forms and attached files that it belatedly discovered were stored on the web server. There does not appear to have been a risk

---

88 Incident Response Investigation Report from Ward Solutions, 6 (received by DPC 31 January 2019).

89 Incident Response Investigation Report from Ward Solutions, 5 (received by DPC 31 January 2019).

90 Incident Response Investigation Report from Ward Solutions, 7 (received by DPC 31 January 2019).

analysis of the personal data that were processed through the web server as part of its normal operation, which would have been exposed to the malware on the server.

167. In the Commencement Letter,[91] CDETB was asked to describe the decision-making process and the factors taken into account when evaluating the risk to the rights and freedoms of affected data subjects in respect of Article 34 GDPR. In its response, CDETB stated that it looked at three strands to determine the risk to the rights and freedoms of the data subjects, as follows:[92]

1) an internal risk assessment of the online form template data fields was performed by SUSI in line with an ENISA risk assessment framework[93]
2) a sample data analysis of uploaded documents and free text data fields submitted through the online forms on the SUSI Website was carried out by SUSI in order to quantify their incidence and the nature of their contents[94]
3) an extended forensic analysis by Ward Solutions, an independent security company, of the available SUSI Website webserver logs and data that had been contained on it - this was central to the overall investigation and analysis that was being undertaken by the Incident Response Team.[95]

i. Strand 1

168. The ENISA guidance[96] provides a useful tool to help categorise a data breach. However, the rights and freedoms of the data subjects must be must be central when carrying out any personal data breach risk assessment. Assessing to what extent data subjects' rights and freedoms may have been infringed by a data breach is an essential element of a personal data breach risk assessment. This assessment is necessary in order to determine if and how a data controller has met its obligations under GDPR. Such an assessment is also a necessary element for a Supervisory Authority to assess the efficacy and appropriateness of a data controller's actions and incident response. The assessment that must be conducted under Article 34 GDPR is distinct to that provided for by the ENISA guidelines. Further, having applied the ENISA guidance, CDETB established that the risk was high, stating that 'if the data contained in these fields were

---

91 Commencement Letter, 19 July 2019.

92 Response to Commencement Letter Appendix 1, 1 August 2019.

93 Response to Commencement Letter Appendix 1, 1 August 2019, p. 16, para 3(a).

94 Response to Commencement Letter Appendix 1, 1 August 2019, 5(2 16, para 3(b).

95 Response to Commencement Letter Appendix 1, 1 August 2019, p. 16, para 3(c).

96 EU Agency for Network and Information Security (ENISA) Recommendations for a methodology of the assessment of severity of personal data breaches Working Document, vl.0, December 2013.

breached, the risk to data subjects would be considered to be high in accordance with the strict criteria of that framework'.[97]

ii. Strand 2

169. With regard to Strand 2, CDETB stated it conducted a sample data analysis of uploaded documents and free text data fields submitted through its online forms on the susi.ie website. CDETB did not conduct a full analysis of uploaded documents and free text submitted through its susi.ie website as it was unable to do so. CDETB stated in its report to the DES that:

> it appeared that any links between these documents and the individual forms to which they related had been severed in the course of the exercise undertaken to secure them, these documents could not readily be interrogated in an orderly manner to determine their association with either the primary data subjects or with the other data that these subjects had submitted and as represented in the form dataset.[98]

It is unclear from the above statement what analysis was conducted, how this action informed assessment of risks to the rights and freedoms of affected individuals, or how CDETB proposed to address those risks.

170. Furthermore, CDETB did not provide the DPC with an update on its examination of the two datasets which it described as central to its determination of the risk to the rights and freedoms of data subjects affected by the breach. CDETB was unable to provide an accurate number of data subjects affected by the security incident or a comprehensive list of the personal data in the documents and forms uploaded to its webserver. In the absence of a complete record of processing related to this breach, it is the view of the DPC that CDETB had to rate the risk at its highest. Where, as in this case, it is known at the outset that the types of personal data affected and the categories of person it relates to pose high risks to at least some affected data subjects, it was not appropriate to determine the risk to all affected data subjects by use of a sample data analysis.

iii. Strand 3

171. The updated Ward Solutions report of 23 January 2019[99] identified a further security liability present on the SUSI website. It said that boxtubex.com was being used as part of an attack against SUSI website users with the aim of infecting users' machines with

---

97 CDETB Response Letter to Direction, 31 January 2019, 2.

98 Confidential Report CDETB_SUSI to DES, 14 December 2018, 5 (received by DPC 20 December 2018).

99 Incident Response Investigation Report from Ward Solutions, 20 (received by DPC 31 January 2019).

malware. This discovery of a further security vulnerability distinct from the webshell vulnerability points to a potential harmful effect on the rights and freedoms of applicants and other individuals whose personal data were processed on the SUSI website, by potentially exposing them to the risk of malware attacks. Communicating this breach to data subjects would have enabled them to take measures to mitigate the risks this may have posed.

iv. Finding

172. The DPC finds that CDETB infringed Article 34(1) GDPR by failing to communicate the personal data breach to the data subjects affected without undue delay. The DPC finds that such a notification ought to have been made by 15 January 2019 at the latest. Therefore, CDETB infringed Article 34(1) by failing to contact the individuals affected from 15 January 2019 to 16 December 2020, which was over two years after it became aware of the breach.

173. In coming to its finding of an infringement of Article 34(1) GDPR, the DPC has considered whether any of the conditions set out in Article 34(3) were met. Article 34(3) GDPR states that:

> The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
>
> a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
>
> b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
>
> c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

174. With regard to Article 34(3)(a), CDETB had not rendered the personal data unintelligible to any unauthorised person (malicious attacker) by means such as encryption.

175. Regarding Article 34(3)(b), it was not possible for CDETB to take subsequent measures to ensure that the risk to the rights and freedoms of the affected data subjects would

not materialise due the nature of the security breach and the extended timeframe. The malicious code was present on the webserver from 12 January 2018 to 16 October 2018. Further to this, CDETB was unable to categorically reconstruct the events or determine the malicious actions that took place, due to inadequate logs.

176. With regard to Article 34(3)(c), the communication of the breach to the affected data subjects would not have involved disproportionate effort, as CDETB had the contact details of all primary data subjects (applicants) who had submitted data through the 'form dataset' and 'documents dataset' on the SUSI website. In the case of secondary data subjects whose contact details were unavailable, a public communication (on SUSI's website or elsewhere) could have sufficed to inform all affected data subjects of the breach. Similarly, the communication to primary data subjects could have included a request that they bring the matter to the attention of any secondary data subjects (e.g. parents and guardians) who may have uploaded personal data to the SUSI webserver.

177. Therefore, CDETB was obliged to communicate the data breach to the data subjects and none of the exemptions outlined in Article 34(3) applied in this case.

178. On 15 January 2019, the DPC directed CDETB under Article 34(4) GDPR to notify data subjects of the breach. The DPC was justified in so doing because, as outlined above, the risk to data subjects posed by the breach was clearly high, CDETB had not at that date notified the data subjects, and the exemptions provided for in Article 34(3) did not apply.

179. CDETB did not communicate the personal data breach to either primary or secondary affected data subjects as directed by the DPC on 15 January 2019. However, on 16 December 2020,[100] the Head of SUSI sent an email to the DPC team that had handled the breach notification, stating that SUSI had contacted the affected data subjects earlier that day.

d) Issue 4 – Article 34(4) GDPR

180. Article 34(4) GDPR states:

> if the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

181. On 15 January 2019, the DPC wrote by email to CDETB communicating that the:

[100] Email from Head of SUSI to DPC, 16 December 2020.

> ...potential risk to the rights and freedoms of affected data subjects could be severe. This opinion was formed due to the nature of the breach, and the nature of the data which you have indicted may have been subject of this breach. Therefore, this office is now issuing you as the data controller a direction that contact is to be made directly with all affected data subjects under the provisions of Article 34(4) of the GDPR. It is also noted that this office is also of the opinion, based on the current information provided that the conditions of Article 34(3) have yet to be met and further more specific details may be required.[101]

182. On 16 January 2019,[102] CDETB responded to the DPC stating that the identified nature of the SUSI website security issue had changed substantially since the breach notification on 16 November 2018, and that CDETB was in the process of determining what data subjects might be affected and how they might be affected. However, the correspondence issued to the DES on 14 December 2018 based on the Ward Solutions report did not change the nature of the breach or the notification threshold to data subjects.

183. CDETB subsequently informed the DPC on 31 January 2019[103] that it would not be notifying data subjects as, in CDETB's judgement, the threshold for notification to data subjects on the basis of there being a high risk to their rights and freedoms had not been met. CDETB stated the following reasons:

    1. The personal data stored on the webserver was not demonstrated to have been accessed or ex-filtrated,
    2. The identified use of malicious code present on the webserver was not to access or exfiltrate data, and
    3. There was no evidence that SUSI was the target of a specifically focussed attack in this case.[104]

184. With regard to the first reason raised by CDETB, as discussed in paragraph 163 above, the absence of system log files during extended periods when the malicious code was in place cannot be taken as evidence that no unauthorised access or unauthorised disclosure occurred during the temporal scope of the inquiry.

185. Regarding CDETB's second reason, Ward Solutions[105] stated it accessed a copy of the WSO Shell from a rebuilt copy of the site to investigate the actions that the attacker

---

[101] DPC Direction to CDETB_SUSI To Communicate Data Breach To Data Subjects, 15 January 2019.

[102] Response to DPC from CDETB_SUSI re Direction, 16 January 2019.

[103] Response Letter to Direction, 31 January 2019.

[104] Response Letter to Direction, 31 January 2019.

[105] Ward Solutions Report (received by DPC 5 December 2018).

may have carried out. To execute access to the WSO Shell, Ward Solutions reverse engineered the WSO Shell and extracted the password to it. Ward Solutions then executed the WSO Shell and performed the operations associated with it. This included demonstrating that it would have been 'possible to retrieve sensitive documents using the WSO Shell.'[106]

186. Ward Solutions observed that when accessing sensitive documents via the WSO Shell, entries were produced in the Apache error logs. The Apache error log entries recorded Ward Solutions' IP address when the WSO was executed. From its analysis of the available Apache error logs, Ward Solutions stated that it was not possible to show that sensitive documents were accessed using this method. However, it is not an uncommon practice for an attacker to erase any error messages or security events that were logged during an attack.

187. The Ward Solutions report stated that its analysis of the Apache access logs showed no evidence of malicious activity. However, the Apache access logs available for analysis were only for the 9 days from 29 April to 7 May 2018. An exfiltration of personal data could have taken place before or after those dates, including during the temporal scope of the Inquiry, as the WSO Shell was present on the webserver from 12 January to 16 October 2018. The absence of comprehensive logs impedes the ability of CDETB to detect malicious actions and to reconstruct events in relation to the security incident.

188. Concerning the third reason given by CDETB (that is, the absence of evidence that SUSI was the target of a specifically focussed attack), CDETB has not made clear how this is relevant to determining the risk to affected data subjects and in consequence whether information about the breach should be communicated to them. A malicious attack on a public-facing web server normally involves passively or actively gaining information about a target through the process of network footprinting, followed by engaging with the target to obtain information through network scanning and enumeration. An attacker will then use this information to perform a hack with the intention of gaining access to the target system. There may not be any evidence that the controller was specifically targeted, but the risk posed to data subjects is not any less for that reason.

i. Finding

189. Notwithstanding that SUSI contacted the affected data subjects on 16 December 2020, regarding the period from 15 January 2019 to that date, the DPC finds that CDETB infringed Article 34(4) GDPR by failing to communicate the personal data breach to data subjects when required to by the DPC as its supervisory authority on 15 January 2019.

[106] Ward Solutions Report (received by DPC 5 December 2018).

The DPC notes that CDETB in its submissions on the Draft Decision accepts this finding and also stated the following-

> In the much-delayed communication issued to data subjects on 16th December 2020, we apologised to those affected by the breach. We now wish to take this opportunity to also apologise to the Data Protection Commission, in particular for our failure to comply with Article 34(4) of the GDPR.[107]

190. The DPC acknowledges that CDETB in this manner accepts responsibility and apologises to both data subjects and the regulator, which response is appropriate for a statutory body charged with delivering public services to citizens.

H. Decision on Corrective Powers

191. The DPC has set out above, pursuant to section 111(1)(a) of the 2018 Act, its decision to the effect that CDETB has infringed Articles 5(1)(f), 32(1), 32(2), 33(1), 34(1) and 34(4) GDPR.

192. Under section 111(2) of the 2018 Act, where the DPC makes a decision (under section 111(1)(a)), it must, in addition, make a decision as to whether a corrective power should be exercised in respect of the controller or processor concerned and, if so, the corrective power to be exercised. The remaining question for determination in this Decision is whether any of those infringements merit the exercise of any of the corrective powers set out in Article 58(2) GDPR and, if so, which corrective powers.

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

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

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

    a. A reprimand to CDETB in respect of its infringements of Articles 5(1)(f), 32(1), 32(2), 33(1), 34(1) and 34(4) GDPR;

[107] CDETB_SUSI Submission on Draft Decision, 20 March 2025, 4.

b. An order to bring processing into compliance pursuant to Articles 5(1)(f), 32(1), 32(2), 33(1) and 34(1) in the manner specified below; and

c. Administrative fines for the infringements of Articles 5(1)(f), 32(1), 32(2), 33(1), 34(1) and 34(4).

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

I. Reprimand

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

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

197. The DPC hereby issues CDETB with a reprimand in respect of its infringements of Articles 5(1)(f), 32(1), 32(2), 33(1), 34(1) and 34(4) GDPR identified in this Decision. The purpose of the reprimand is to dissuade non-compliance with the GDPR. The reprimand will contribute to ensuring that CDETB and other controllers and processors take appropriate steps in relation to current and future processing operations in order to comply with their obligations under GDPR. In its submissions on the Draft Decision, CDETB stated that it accepts this reprimand.[108]

J. Order to Bring Processing into Compliance

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

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

199. In circumstances where it has been found that the processing at issue was not in compliance with the GDPR, the DPC makes an order pursuant to Article 58(2)(d) GDPR. Therefore, the DPC orders CDETB to bring its processing operations into compliance with Articles 5(1)(f), 32(1), 32(2), 33(1) and 34(1) GDPR.

200. It is the DPC's view that these orders are appropriate, necessary and proportionate in view of ensuring compliance with Articles 5(1)(f), 32(1) 32(2), 33(1) and 34(1) GDPR. In this regard, the DPC acknowledges CDETB's ongoing remedial actions, as outlined in its submissions throughout the Inquiry.

201. The orders that the DPC imposes are set out in the following table:

Number	Issue and Action	Timescale

[108] CDETB_SUSI Submission on Draft Decision, 20 March 2025, 10.

1.	Articles 5(1)(f) and 32(1)GDPR Lack of robust data protection policies, procedures and necessary audits to ensure compliance. Lack of security to enable the ongoing confidentiality, integrity, availability and resilience of the processing systems. Lack of a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. The DPC orders that CDETB put in place the necessary policies, procedures, security, training, testing and evaluation measures to comply with these articles.	CDETB is required to confirm to the DPC within 90 days of receipt of this Decision that this order has been complied with.
2.	Article 32(2) GDPR Lack of appropriate risk assessments. The DPC orders that CDETB perform the necessary risk assessments to inform the security measures needed for any data processing that it carries out.	CDETB is required to confirm to the DPC within 90 days of receipt of this Decision that this order has been complied with.
3.	Articles 33(1) and 34(1) GDPR Lack of timely notification of a data breach to the DPC. Lack of timely notification of a data breach to the relevant data subjects. The DPC orders that CDETB develop policies and provide staff training in order to respond to data breaches and data security incidents in ways that are appropriate to the risks posed and that ensure compliance with CDETB's obligations as a data controller under Articles 33(1) and 34(1) GDPR.	CDETB is required to confirm to the DPC within 90 days of receipt of this Decision that this order has been complied with.

202. It must be noted that implementing these measures does not relieve CDETB of its obligation to continually evaluate the effectiveness of its measures and the measures that are necessary to ensure a level of security that is appropriate to the dynamic risk presented by its processing.

203. The DPC's decision to impose the orders is made to ensure that full effect is given to CDETB's obligations under GDPR. The DPC considers that the orders are appropriate, necessary and proportionate in view of ensuring compliance with the GDPR.

204. The DPC considers that these orders are necessary to ensure that full effect is given to CDETB's obligations in relation to the data security infringements outlined above, having particular regard to the high quantity, highly sensitive personal and special category data of data subjects processed by CDETB.

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

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

207. The DPC therefore requires CDETB to comply with the above order within the time specified from the date of notification of any final decision. The DPC additionally requires CDETB to submit a report to the DPC within a further month detailing the actions it has taken to comply with the order.

K. Decision on administrative fines

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

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

209. The purpose of administrative fines is to strengthen the enforcement of the rules of the GDPR.[109] Fines sanction non-compliance and seek to re-establish compliance with the GDPR.

210. As the DPC has identified infringements of the GDPR above, it will decide whether to impose administrative fines in respect of those infringements. In conducting this assessment, the DPC has had regard to Article 83 GDPR, which sets out 'General

[109] Recital 148 GDPR.

conditions for imposing administrative fines.' The DPC has also had regard to EDPB guidelines which are designed to ensure a harmonised approach to fining. These guidelines include the EDPB's Guidelines on the calculation of administrative fines (**'the EDPB Fining Guidelines'**),[110] and the Article 29 Working Party's Guidelines on the application and setting of administrative fines (**'the A29WP Fining Guidelines'**),[111] which have been endorsed by the EDPB.

211. As a first step, the DPC will consider whether to impose a fine by applying the criteria set out in Article 83(2) GDPR. If the outcome of the assessment is that a fine should be imposed, then the DPC will proceed to calculate the amount, by reference to the criteria in Article 83(2) GDPR and by considering the other factors set out in Articles 83(1)-(9) that apply in this case. In particular, Article 83(1) GDPR requires fines to be effective, proportionate and dissuasive. These principles will inform the calculation of any fine that is imposed in this Decision.

a) Whether to impose an administrative fine

212. Article 83(2) GDPR states:

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

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

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

214. Article 83(2)(a) requires consideration of each criterion by reference to 'the infringement' as well as 'the processing concerned.' The phrase **'the processing concerned'** in this Article 83(2) analysis should be understood to mean all of the

[110] European Data Protection Board, 'Guidelines 04/2022 on the calculation of administrative fines under the GDPR', version 2.1, adopted on 24 May 2023.

[111] Article 29 Data Protection Working Party, 'Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679', WP253, adopted on 3 October 2017, endorsed by the EDPB on 25 May 2018.

processing operations that CDETB carries out on the personal data in connection with the subject matter of the breach, specifically the personal data processed on the website.

215. Considering next the meaning of 'infringement', it is clear from Articles 83(3)-(5) that 'infringement' means an infringement of a provision of the GDPR. Above, CDETB was found to have infringed Articles 5(1)(f), 32(1), 32(2), 33(1), 34(1) and 34(4) GDPR. Thus, '**the infringement**', for the purpose of the DPC's assessment of the Article 83(2) criteria, should be understood (depending on the context in which the term is used) to mean an infringement of Articles 5(1)(f), 32(1), 32(2), 33(1), 34(1) and 34(4) GDPR. While each is an individual 'infringement' of the relevant provision, they all relate to the processing concerned and, by reason of their common nature and purpose, are likely to generate the same, or similar, outcomes in the context of some of the Article 83(2) assessment criteria. Accordingly, and for ease of review, the DPC will assess all of these infringements simultaneously, by reference to the collective term '**infringements**', unless otherwise indicated.

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

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

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

218. The nature of the processing can include:

> the context in which the processing is functionally based (e.g. business activity, non-profit, political party, etc.) and all the characteristics of the processing.'[112]

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

> where the purpose is to monitor, evaluate personal aspects or to take decisions or measures with negative effects for data subjects, where there is a clear

[112] EDPB Fining Guidelines, para 53.b.i.

> imbalance between the controller and data subjects or where the processing involves children or other vulnerable data subjects.[113]

220. The nature of the processing in this case is the collection, organisation and analysis of the personal data of grant applicants (and in some cases, of third parties) for the purpose of administering a grant scheme. The processing included the data on the health, family background and other sensitive matters of data subjects, some of whom were vulnerable persons.

221. The scope of the processing is assessed:

> with reference to the local, national or cross-border scope of the processing carried out and the relationship between this information and the actual extent of the processing in terms of the allocation of resources by the data controller... The larger the scope of the processing, the more weight the supervisory authority may attribute to this factor.[114]

222. The scope of the processing relating to the infringements identified herein is broad. This is due to the quantity and variety of personal data processed and the broad scope of the processing on a national level.

223. The purpose of the processing:

> will lead the supervisory authority to attribute more weight to this factor. The supervisory authority may also consider whether the processing of personal data falls within the so-called core activities of the controller. The more central the processing is to the controller's or processor's core activities, the more severe irregularities in this processing will be. The supervisory authority may attribute more weight to this factor in these circumstances. There may be circumstances though, in which the processing of personal data is further removed from the core activities of the controller or processor, but significantly impacts the evaluation nonetheless (this is the case, for example, of processing concerning personal data of workers where the infringement significantly affects those workers' dignity).[115]

224. The purpose of the processing relating to the infringements identified herein is to allow applicants, after making their application to CDETB via its website, to submit supplementary requests and data through online forms, including requests for internal review of grant application (grant applicants), requests for cancellation of grant application (grant applicants), requests to be enabled to make late grant application

[113] EDPB Fining Guidelines, para 53.b.i.

[114] EDPB Fining Guidelines, para 53.b.ii.

[115] EDPB Fining Guidelines, para 53.b.iii.

(grant applicants and non-applicants), submitting formal complaints to SUSI (grant applicants and non-applicants) and reporting suspicious activity to SUSI (grant applicants and non-applicants). This processing is an integral function of CDETB, i.e. a part of the grant application process. The purpose of the processing was determined by CDETB.

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

> The higher the number of data subjects involved, the more weight the supervisory authority may attribute to this factor. In many cases, it may also be considered that the infringement takes on 'systemic' connotations and can therefore affect, even at different times, additional data subjects who have not submitted complaints or reports to the supervisory authority. The supervisory authority may, depending on the circumstances of the case, consider the ratio between the number of data subjects affected and the total number of data subjects in that context (e.g. the number of citizens, customers or employees) in order to assess whether the infringement is of a systemic nature.[116]

226. An estimated 13,000 data subjects who had submitted supplementary forms through the SUSI website during 2017 and 2018 were affected by the personal data breach discussed in this Decision. CDETB's processing entailed a significant amount of personal and some special category data, access to which ought to have been limited to CDETB.

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

> The reference to the 'level' of damage suffered, therefore, is intended to draw the attention of the supervisory authorities to the damage suffered, or likely to have been suffered as a further, separate parameter with respect to the number of data subjects involved (for example, in cases where the number of individuals affected by the unlawful processing is high but the damage suffered by them is marginal). Following Recital 75 GDPR, the level of damage suffered refers to physical, material or non-material damage. The assessment of the damage, in any case, be limited [sic] to what is functionally necessary to achieve correct evaluation of the level of seriousness of the infringement as indicated in paragraph 60 below, without overlapping with the activities of judicial authorities as tasked with ascertaining the different forms of individual harm.[117]

---

[116] EDPB Fining Guidelines, para 53.b.iv.

[117] EDPB Fining Guidelines, para 53.b.v.

228. In assessing the level of damage suffered by the data subjects, the DPC has had regard to the loss of control suffered by them over their personal data. The personal data affected by the breach included data subject identity (name, surname, birth date), PPSN (or other national identification number), contact details, identification data (passports, licence data etc.), economic or financial data, location data, criminal convictions, offences or security measures. In addition, the following special categories of data were disclosed: data revealing racial or ethnic origin and health data.

229. The risk arising from this processing of personal data on the CDETB website included that an unauthorised person could gain access to the applicants' data, which would pose a high risk with regard to the fundamental rights and freedoms of data subjects, with loss of control over the data subjects' personal data, loss of confidentiality and the possibility of phishing attacks and identity theft.

The nature of the infringements

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

> review the interest that the infringed provision seeks to protect and the place of this provision in the data protection framework. In addition, the supervisory authority may consider the degree to which the infringement prohibited the effective application of the provision and the fulfilment of the objective it sought to protect.[118]

231. In line with the text of the GDPR, the nature, gravity and duration of the infringements are all assessed by taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them.[119]

232. The nature of CDETB's infringements of Articles 5(1)(f) and 32(1) identified herein, comprises a failure of CDETB to comply with its obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk in respect of its processing operations. The objective of Articles 5(1)(f) and 32(1) GDPR is to protect the rights and freedoms of natural persons by ensuring that their personal data are processed in a manner that ensures appropriate security. A failure to implement an appropriate level of security increases the risk of personal data breaches, as does a failure to implement processes for testing and evaluating the effectiveness of technical and organisational security measures. This, in turn, poses a threat to the rights

[118] EDPB Fining Guidelines, para 53.a.

[119] Article 83(2)(a) GDPR.

and freedoms of data subjects because of the potential for damage to data subjects where personal data breaches occur, leading to, inter alia, destruction of essential personal data or unauthorised access, alteration or disclosure of those personal data. Therefore, compliance with Articles 5(1)(f) and 32(1) is central to the protection of the rights and freedoms of natural persons pursuant to the GDPR. As such, non-compliance with this obligation has serious consequences in that it has the potential to result in damage to data subjects.

233. The nature of the infringement of Article 32(2) GDPR identified herein is that CDETB did not take account of the risks that were presented by processing from unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed on the webserver. Not taking account of the risks involved in processing has the potential to result in damage to data subjects.

234. The nature of the infringement of Article 33(1) GDPR, identified herein is, because the personal data breach resulted in a risk to the rights and freedoms of data subjects, CDETB was obliged to notify the DPC of the personal data breach without undue delay, which it failed to do. The purpose of Article 33(1) is to ensure prompt notification of data breaches to supervisory authorities. This enables a supervisory authority to assess the circumstances of the data breach, including the risks to natural persons. It can then decide whether the interests of those persons must be safeguarded to the extent possible, by mitigating the risks to them arising from a data breach.[120]

235. The nature of infringement of Article 34(1) GDPR, identified herein is CDETB's failure to contact the data subjects affected by the data breach without undue delay. Instead this notification was carried out on 16 December 2020, which was over two years after CDETB became aware of the breach. Notification of a data breach to the data subjects allows the data subjects to take action to mitigate the risks to them which may result from the breach.

236. The nature of the infringement of Article 34(4) GDPR, identified herein is the failure of CDETB to communicate the personal data breach to data subjects when required by the DPC as its supervisory authority on 15 January 2019. Instead the personal data breach was communicated to data subjects on 16 December 2020.

[120] Recital 85 GDPR.

The gravity of the infringements

237. The gravity (as well as the nature and duration of the infringements) is assessed taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them.[121]

238. The gravity of the infringement of Articles 5(1)(f), 32(1) and 32(2) GDPR is high in circumstances where the infringement resulted in the personal data breach. CDETB's lack of technical and organisational measures at the time of the breach contributed to the unauthorised processing of personal and special category data of a large number of data subjects. The DPC considers that the gravity of CDETB's failure to implement sufficient and appropriate technical and organisational measures to ensure the confidentiality, integrity, availability and resilience of its processing systems to be high.

239. The gravity of the infringements of Article 33(1) GDPR is high. The personal data breach concerned the personal data of a significant number of data subjects and the DPC has found that there was an infringement of the GDPR in CDETB's failure to notify the DPC of the personal data breach at the required time. The personal data breach resulted in a risk to the rights and freedoms of data subjects. In these circumstances, and in light of the importance of the notification process in protecting the rights and freedoms of data subjects, the gravity of the infringement of Article 33(1) is high.

240. The gravity of the infringement of Article 34(1) GDPR is high. The personal data breach resulted in a risk to the rights and freedoms of data subjects. Communicating the breach to data subjects would have enabled them to take measures to mitigate the risks the breach posed. Contacting the affected data subjects immediately after CDETB became subjectively aware of the breach may not have been possible due to the scale of the breach. However, CDETB failed to contact the individuals affected until over two years after it became aware of the breach. The infringement of Article 34(1) indicates a lack of recognition of the serious effects of personal data breaches on the individuals affected and the risks to which they are exposed.

241. The gravity of the infringement of Article 34(4) GDPR is also high. On 15 January 2019, the DPC directed CDETB under Article 34(4) GDPR to notify data subjects of the breach as the risk to data subjects posed by the breach was high and the exemptions provided for in Article 34(3) did not apply. However, CDETB did not communicate the personal data breach to affected data subjects as directed by the DPC until 16 December 2020. The infringement of Article 34(1) indicates a lack of recognition of and the need for accountability to CDETB's supervisory authority.

[121] Article 83(2)(a) GDPR.

The duration of the infringement

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

> a supervisory authority may generally attribute more weight to an infringement with longer duration. The longer the duration of the infringement, the more weight the supervisory authority may attribute to this factor.[122]

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

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

b) failure to take appropriate preventive measures, or

c) inability to put in place the required technical and organisational measures.[123]

244. The duration (as well as the nature and gravity of the infringements) is assessed taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them.[124]

245. In this case, the duration of the infringement of Articles 5(1)(f), 32(1), and 32(2) commenced at the application of the GDPR on 25 May 2018. The obligation to implement and be able to demonstrate the appropriate organisational and technical measures applied from 25 May 2018. The infringements of those Articles found herein were ongoing until at least January 2019, when Ward Solutions identified the last piece of malware (WSO Shell) which had been added in January 2018. Therefore, for the purposes of deciding whether to impose an administrative fine, and for calculating the appropriate amount if applicable, the DPC proceeds on the basis that the infringement of Articles 5(1)(f), 32(1) and 32(2) GDPR lasted at least from 25 May 2018 until January 2019, a period of seven months.

246. With regard to the duration of the infringement of Article 33(1) GDPR found here, it is the DPC's finding that there are no circumstances concerning this breach that justify a failure to notify the DPC within 72 hours of when CDETB became aware of it. CDETB ought to have notified the DPC within 72 hours. However, the breach notification was sent to the DPC on 16 November 2018. Therefore, for the purposes of deciding whether to impose an administrative fine, and for calculating the appropriate amount if applicable, the DPC proceeds on the basis that the duration of the infringement was 72 hours after the date CDETB became aware of the incident on 16 October 2018 to the

---

[122] EDPB Fining Guidelines, para 53.c.

[123] A29WP Fining Guidelines, 11.

[124] Article 83(2)(a) GDPR.

date of notification to the DPC on 16 November 2018. This notification was over three weeks later than it should have been.

247. With regard to the infringement of Article 34(1) GDPR, in this case it would not have been reasonably feasible for CDETB to contact the individuals affected immediately due to the scale of the breach. However, the DPC finds that it would have been reasonably feasible for CDETB to notify the data subjects by 15 January 2019 at the latest.

248. With regard to the infringement of Article 34(4) GDPR, on 15 January 2019 the DPC wrote by email to CDETB stating that it was 'issuing you as the data controller a direction that contact is to be made directly with all affected data subjects under the provisions of Article 34(4) of the GDPR.'

249. With regard to the duration of the infringements of Article 34(1) and 34(4) GDPR found here, for the purposes of deciding whether to impose an administrative fine, and for calculating the appropriate amount if applicable, the DPC proceeds on the basis that these infringements continued until the individuals affected were contacted by CDETB on 16 December 2020.[125] Therefore, the duration of both infringements was one year and 11 months.

Assessment of Article 83(2)(a)

250. Taking account of all of the factors assessed in this section, the DPC assesses the infringements of Articles 5(1)(f), 32(1) and 32(2) GDPR to be of a serious nature, high gravity and of a substantial duration. CDETB's processing of personal data via its website resulted in unauthorised access of personal data to third parties. CDETB failed to analyse risks to the rights and freedoms of the data subjects of processing in that manner, or to put in place adequate security measures to ensure the data could not be accessed by or disclosed to unauthorised persons. According to Recital 85 GDPR:

> [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 or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

251. In addition, CDETB did not implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including a process for

[125] Email from Head of SUSI, 16 December 2020.

regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing on the webserver. CDETB did not take account of the risks that were presented by processing on the webserver. CDETB did not demonstrate what appropriate technical security measures it implemented in relation to the susi.ie website as a result of the work it undertook around data protection governance and compliance at the time of the notified breach.

252. With regard to the infringements of Article 33(1) GDPR, the DPC assesses the infringements to be of a serious nature, high gravity and of a substantial duration. The personal data breach resulted in a risk to the rights and freedoms of natural persons and so should have been notified to the DPC within 72 hours of becoming aware of it. Such notifications are crucial for enabling supervisory authorities to assess the circumstances of the data breach, including the risks to data subjects, and decide whether action is required to mitigate those risks.

253. The DPC assesses the infringement of Article 34(1) GDPR as serious in nature, of high gravity and of a lengthy duration. Communicating the breach to data subjects would have enabled them to take measures to mitigate the risk it may have posed to them.

254. With regard to the infringement of Article 34(4) GDPR, the DPC assesses this infringement as serious in nature, of high gravity and of a lengthy duration.

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

255. The A29WP Fining Guidelines state:

> in general, intent includes both knowledge and willfulness in relation to the characteristics of an offence, whereas 'unintentional' means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law.[126]

256. The EDPB Fining Guidelines state:

> The intentional or negligent character of the infringement (Article 83(2)(b) GDPR) should be assessed taking into account the objective elements of conduct gathered from the facts of the case. The EDPB highlighted that it is generally admitted that intentional infringements, 'demonstrating contempt for the provisions of the law, are more severe than unintentional ones'.[127] In case of an intentional infringement, the supervisory authority is likely to attribute more

[126] A29WP Fining Guidelines, 11.

[127] Footnote from EDPB Fining Guidelines: Guidelines WP 253, 12.

weight to this factor. Depending on the circumstances of the case, the supervisory authority may also attach weight to the degree of negligence. At best, negligence could be regarded as neutral.[128]

257. In this case, the DPC finds that the infringements are of a negligent character. CDETB's infringement of Articles 5(1)(f), 32(1), and 32(2) GDPR regarding the processing, concerns its failure to implement appropriate measures to protect the rights and freedoms of natural persons by ensuring that their personal data are processed in a manner that ensures security appropriate to the level of risk involved, lack of implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing, and its failure to take account of the risks that were presented by processing. Hence, the characteristics of this infringement concerns the lack of appropriate technical and organisational measures for the duration of the infringement. To classify this infringement as intentional, the DPC would have to be satisfied that (i) CDETB wilfully omitted to implement appropriate technical and organisational measures and to document those measures and (ii) that it knew at the time that the measures that it implemented were not sufficient to meet the standards required by Articles 5(1)(f) and 32(1) and (2) GDPR.

258. While CDETB's attempts to implement appropriate measures were not sufficient for the purposes of those Articles, the DPC does not consider that CDETB knew that the measures implemented were not sufficient at the time. However, in the circumstances, CDETB ought to have been aware that it was falling short of the duty owed under those Articles. The DPC is of the view that these infringements indicate a medium degree of negligence on the part of CDETB, as CDETB ought to have been aware in the circumstances that it was falling short of the duty owed at the time under consideration.

259. The DPC finds that CDETB's infringement of Article 33(1) was also of a negligent character, because it ought to have been aware of its obligation to inform the DPC within 72 of becoming aware of a data breach and that, in failing to do so, it was falling short of the standards required by Article 33(1). The DPC categorises this infringement as being of a negligent – rather than intentional – character.

260. With regard to Article 34(1), the DPC finds that CDETB's infringement was intentional in nature. CDETB was aware from at the latest 30 November 2018 that the nature of the disclosed personal data posed a high risk to data subject, as was made clear in the DPC's advice to CDETB on 30 November 2018. In fact, CDETB indicated to the DPC on 7

[128] EDPB Fining Guidelines, para 56.

December 2018 that it planned to notify data subjects of the breach, but reversed that decision on 10 December 2018. The intentional nature of the infringement is underscored by CDETB's failure to comply with the DPC's direction to notify, which it received on 15 January 2019, but did not comply with until 16 December 2020.

261. Regarding Article 34(4), the DPC finds that CDETB's infringement was intentional in nature in respect of the period from 15 January 2019 to 16 December 2020. In order to classify this infringement as intentional, the DPC must be satisfied that (i) CDETB wilfully omitted to contact the data subjects as instructed by the DPC and (ii) that it knew at the time that this was required. On 15 January 2019, CDETB was instructed by the DPC to communicate the personal data breach to data subjects as follows:

> this office is now issuing you as the data controller a direction that contact is to be made directly with all affected data subjects under the provisions of Article 34(4) of the GDPR.[129]

262. However, CDETB intentionally chose not to comply with this instruction until 16 December 2020. Therefore, the DPC categorises this infringement as intentional, as opposed to negligent, in character.

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

263. According to the A29WP Fining Guidelines:

> This provision acts as an assessment of the degree of responsibility of the controller after the infringement has occurred. It may cover cases where the controller/processor has clearly not taken a reckless/ negligent approach but where they have done all they can to correct their actions when they became aware of the infringement.[130]

264. CDETB put in place various mitigation measures after it discovered the data breach. As detailed in CDETB's response to the Commencement Letter on 1 August 2019, these included:

- removal of all malware, infected files and personal data from the SUSI webserver, and change of all passwords,

[129] CDETB Response Letter to Direction, 31 January 2019.

[130] A29WP Fining Guidelines, 12-13.

- reconfiguration of the webserver to remove the forms functionality and to limit access to its control panel to the SUSI IP address,
- increased firewall restrictions, regular anti-malware scanning, full implementation of the recommendations of the Wordfence Malware Removal Report, and penetration testing by independent third parties,
- daily monitoring and analysis of network traffic and user activity,
- changes in organisational arrangements and change-management processes to limit administration-level access to the webserver, clarify reporting lines and strengthen management oversight of the SUSI webserver and its operations.

265. However, it is not always possible to correct a lack of control retrospectively, and these actions did not mitigate the risk to the confidentiality of the data belonging to the affected data subjects. Despite the delay in notifying the DPC of the breach, CDETB took steps to investigate the security incident prior to notifying the DPC. Having regard to these actions for the purpose of Article 83(2)(c) GDPR, the DPC is of the view that the actions provided limited mitigation of the damage to data subjects.

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

266. The key question in relation to this provision is whether CDETB 'did what it could be expected to do' given the nature, the purposes or the size of the processing, seen in light of the obligations imposed on it by the GDPR.[131]

267. In its submissions, CDETB outlined the measures that it had in place to prevent any potential breach of data protection. The DPC has had full regard to those measures in this Decision. This Decision assesses whether CDETB complied with its obligations under Articles 5(1)(f), 32(1), 32(2) GDPR by implementing appropriate technical and organisational measures to ensure appropriate security of the personal data processed in CDETB's servers. As stated above, the DPC finds that CDETB infringed those provisions.

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

[131] EDPB Fining Guidelines, para 77.

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

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

270. In line with the EDPB Fining Guidelines, prior infringements are those already established before the decision is issued.[132]

271. According to the A29WP Fining Guidelines, '[t]his criterion is meant to assess the track record of the entity committing the infringement.'[133]

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

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

273. The extent to which CDETB has cooperated with the inquiry is relevant to consider under this heading.[134] CDETB submitted breach notification forms in respect of the personal data breach to the DPC and gave updates regarding CDETB's progress in remediating the breach. The DPC acknowledges CDETB's cooperation with the DPC during the course of the Inquiry. However, the DPC notes that CDETB is, in any event, under a duty, in light of Article 31 GDPR, to cooperate, on request, with the supervisory authority in the performance of its tasks. While CDETB failed to cooperate with the DPC in terms of its notification of the breach to data subjects, in circumstances where this failure forms part of the basis for the finding of the infringement of Article 33 and 34 GDPR against CDETB, this factor cannot be considered aggravating in respect of the infringements.

---

[132] EDPB Fining Guidelines, para 82.

[133] A20WP Fining Guidelines, 14.

[134] A29WP Fining Guidelines, 14.

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

274. By way of example of the categories that may be relevant to consider here, the A29WP Fining Guidelines suggest considering whether the infringements concern Article 9 or 10 data, whether the data are directly or indirectly identifiable, whether the data are encrypted or whether the processing involves data whose dissemination would cause immediate damage or distress to the individual.[135]

275. The processing in this case includes data subject identity (name, surname, birth date), PPSN (or other national identification number), contact details, identification data (passports, licence data etc.), economic or financial data, location data, criminal convictions, offences or security measure. It also includes special category data, namely data revealing racial or ethnic origin and health data. The data were not encrypted. These personal data, by their nature, carry a risk with regard to the fundamental rights and freedoms of data subjects, in particular in relation to financial fraud and/or identity theft.

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

276. According to the A29WP Fining Guidelines, this section can be used to consider whether the DPC became aware of the infringement 'as a result of investigation, complaints, articles in the press, anonymous tips or notification by the data controller.'[136]

277. The A29WP Fining Guidelines also note that:

> The controller has an obligation according to the Regulation to notify the supervisory authority about personal data breaches. Where the controller merely fulfils this obligation, compliance with the obligation cannot be interpreted as an attenuating/ mitigating factor. Similarly, a data controller/processor who acted carelessly without notifying, or at least not notifying all of the details of the infringement due to a failure to adequately assess the extent of the infringement may also be considered by the supervisory authority to merit a more serious penalty i.e. it is unlikely to be classified as a minor infringement.[137]

---

[135] A29WP Fining Guidelines, 14.

[136] A29WP Fining Guidelines, 15.

[137] A29WP Fining Guidelines, 15.

278. In this case, the DPC became aware of the infringements on 16 November 2018 as a result of a breach notification (BN-18-11-258)[138] from CDETB. This was found to be an undue delay and in breach of Article 33(1) GDPR.

[138] Breach Notification Form, 16 November 2018.

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

279. The A29WP Fining Guidelines state:

> As opposed to the criteria in (e), this assessment criteria only seeks to remind supervisory authorities to refer to measures that they themselves have previously issued to the same controller or processors 'with regard to the same subject matter'.[139]

280. Corrective powers have not previously been ordered against CDETB with regard to the subject matter of this Decision.

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

281. Such considerations do not arise in this case.

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

282. The EDPB Fining Guidelines state:

> Article 83(2)(k) GDPR gives the supervisory authority room to take into account any other aggravating or mitigating factors applicable to the circumstances of the case. In the individual case there may be many elements involved, which cannot all be codified or listed and which will have to be taken into account in order to ensure that the sanction applied is effective, proportionate and dissuasive in each individual case.
>
> Article 83(2)(k) GDPR mentions examples of 'any other aggravating or mitigating factor applicable to the circumstances of the case,'... It is considered that this provision is of fundamental importance for adjusting the amount of the fine to the specific case. In this sense, it is considered that it should be interpreted as an instance of the principle of fairness and justice applied to the individual case.[140]

---

[139] A29WP Fining Guidelines, 15.

[140] EDPB Fining Guidelines, para 108.

283. In this case, CDETB expressly accepted each of the DPC's findings of infringement as set out in its Draft Decision, and has acknowledged full responsibility for the breach. CDETB indicated that it has since implemented substantive technical and organisational measures in order to reduce the likelihood of similar breaches occurring in future. These measures included the following:

- A dedicated SUSI Governance Unit is responsible for SUSI data protection matters which has implemented processes, procedures and policies to strengthen the management and safeguarding of personal data.
- A risk management policy and corporate risk register have been implemented.
- Data Processing Agreements have been put in place with relevant providers.
- A new SUSI website was launched in 2023 certified to the ISO 27001 international standard. It is audited twice yearly and has an Advanced Shield Firewall.
- The Grant Application System now has its own portal and is separate to the website.
- The Content Management System (CMS) is locked down to the City of Dublin ETB network.
- Audit logs of user activity are available and penetration testing has been carried out.
- Data Protection training across the organisation has been expanded, including in general staff training, SUSI-specific staff training, as well as targeted and role specific training.
- Cybersecurity training is provided monthly, including periodic phishing exercises.
- Security desk and security card system are in place in offices.
- The internal network is segmented and a SIEM (Security Incident and Event Management) system is used for threat detection and analysis, as well as endpoint threat detection and response tools.
- Backup software is in use.
- MFA (Multi Factor Authentication) is in place for all SUSI users.
- Monthly patching of computers and servers is carried out.
- Web filtering via firewalls, including real-time blacklisting, content filtering and malware scanning is in place.
- Implementation of Information Security Management System (ISMS), which includes audits, testing and evaluations.

284. The DPC notes the interpretation given in the EDPB Fining Guidelines to Article 83(2)(k) as outlined in paragraph 282 above, which suggests that a wide range of factors may be considered by supervisory authorities as potentially mitigating or aggravating under this heading, with the overriding consideration being the principle of fairness and justice as applied to the circumstances of the case at hand.

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

> Regulatory experience from SAs under the 95/46/EC Directive has previously shown that it can be appropriate to show some degree of flexibility to those data controllers/processors who have admitted to their infringement and taken responsibility to correct or limit the impact of their actions.[141]

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

287. Taking all the above into account, the DPC considers that CDETB's actions in

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

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

xii. Decision on whether to impose administrative fines

288. The decision to impose an administrative fine 'needs to be taken on a case-by-case basis, in light of the circumstances of each individual case.'[142]

289. Taking into account the assessment of the criteria at (a) to (k) above, the DPC has decided to impose an administrative fine for the infringements of Articles 5(1)(f) and 32(1). The DPC has also decided to impose administrative fines for infringements of Articles 32(2), 33(1), 34(1) and 34(4) GDPR. The infringements were considered above to be of a high seriousness by reference to their nature, gravity and duration in line with Article 83(2)(a). This is an aggravating factor, which indicates that a fine should be imposed. Under Articles 83(2)(b) and (g), the DPC found that CDETB was negligent to a medium degree with respect to the infringements of Articles 5(1)(f), 32(1), 32(2), 33(1)

[141] A29WP Fining Guidelines, 13.
[142] EDPB, Binding Decision 1/2023.

and 34(1) and that the infringements affected personal data which, by their nature, carry a risk with regard to the fundamental rights and freedoms of data subjects, in particular in relation to identity theft. The infringement of Article 34(4) was found to be intentional in nature.

290. These are aggravating factors indicating that a fine should be imposed. The DPC considers that the measures adopted by CDETB under Article 83(2)(c) to mitigate the damage to data subjects is mitigating to a low degree, and this factor does not negate the need for administrative fines in this Inquiry. Similarly, the DPC considers that the factors assessed in relation to Article 83(2)(k) are mitigating but do not negate the need for administrative fines in this Inquiry. The DPC considers that the factors assessed in relation to Articles 83(2)(e), (f), (h), (i), and (j) are neither mitigating nor aggravating.

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

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

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

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

    b. Regarding the infringements, the DPC considers that CDETB's non-compliance with its obligations under these Articles must be strongly dissuaded. Such dissuasive effect is crucial for protecting the rights and freedoms of those data subjects by implementing appropriate measures.

    Therefore, the DPC considers that administrative fines are appropriate and necessary in order to dissuade non-compliance.

293. Having regard to the nature, gravity and duration of the infringements, the DPC also considers that administrative fines are proportionate in the circumstances in view of ensuring compliance. The DPC considers that administrative fines are proportionate to responding to CDETB's infringement of Articles 5(1)(f), 32(1),32(2), 33(1), 34(1) and 34(4) GDPR with a view to ensuring future compliance. The DPC considers that administrative fines do not exceed what is necessary to enforce compliance in respect of the infringements identified in this Decision.

294. The DPC considers that the negligent character of CDETB's infringements of Articles 5(1)(f), 32(1), 32(2), 33(1) and 34(1) GDPR and the intentional nature of the infringement of Article 34(4) carry weight when considering whether to impose administrative fines, and if so, the amount of those fines. It suggests that administrative fines are necessary to ensure that CDETB directs sufficient attention to its obligations under these Articles of the GDPR in the future.

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

296. The DPC has had regard to the lack of previous relevant infringements by CDETB, which is a slightly mitigating factor. As noted in paragraphs 265 and 287 above, the DPC has also had regard to the actions taken by CDETB as a result of the breach. In light of the negligent and intentional character of the infringements, and CDETB's failure to comply with its obligations with regard to data protection, the DPC considers that dissuasive administrative fines are necessary in the circumstances to ensure future compliance.

b) Decision on the amount of the administrative fine

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

i. Article 83(3) GDPR

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

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

299. As outlined previously, the infringements identified herein all relate to the processing concerned, i.e. via CDETB's website.

300. In respect of the interpretation of Article 83(3) GDPR, the DPC is mindful of its obligations of cooperation and consistency in, *inter alia*, Articles 60(1) and 63 GDPR. Accordingly, it is necessary to follow the EDPB's interpretation of Article 83(3) GDPR set out in the EDPB's binding decision 1/2021, which was made in relation to an inquiry conducted by the DPC.[143]

301. The relevant passage of that binding decision is as follows:

> 315. All CSAs argued in their respective objections that not taking into account infringements other than the 'gravest infringement' is not in line with their interpretation of Article 83(3) GDPR, as this would result in a situation where WhatsApp IE is fined in the same way for one infringement as it would be for several infringements. On the other hand, as explained above, the IE SA argued that the assessment of whether to impose a fine, and of the amount thereof, must be carried out in respect of each individual infringement found and the

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

assessment of the gravity of the infringement should be done by taking into account the individual circumstances of the case. The IE SA decided to impose only a fine for the infringement of Article 14 GDPR, considering it to be the gravest of the three infringements.

316. The EDPB notes that the IE SA identified several infringements in the Draft Decision for which it specified fines, namely infringements of Article 12, 13 and 14 GDPR, and then applied Article 83(3) GDPR.

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

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

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

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

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

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

323. Indeed, the approach pursued by the IE SA would lead to a situation where, in cases of several infringements of the GDPR concerning the same or linked processing operations, the fine would always correspond to the same amount that would be identified, had the controller or processor only committed one – the gravest – infringement. The other infringements would be discarded with regard to calculating the fine. In other words, it would not matter if a controller committed one or numerous infringements of the GDPR, as only one single infringement, the gravest infringement, would be taken into account when assessing the fine.

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

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

> 326. Although the fine itself may not exceed the legal maximum of the highest fining tier, the offender shall still be explicitly found guilty of having infringed several provisions and these infringements have to be taken into account when assessing the amount of the final fine that is to be imposed. Therefore, while the legal maximum of the fine is set by the gravest infringement with regard to Articles 83(4) and (5) GDPR, other infringements cannot be discarded but have to be taken into account when calculating the fine.
>
> 327. In light of the above, the EDPB instructs the IE SA to amend its Draft Decision on the basis of the objections raised by the DE SA, FR SA and PT SA with respect to Article 83(3) GDPR and to also take into account the other infringements – in addition to the gravest infringement – when calculating the fine, subject to the criteria of Article 83(1) GDPR of effectiveness, proportionality and dissuasiveness.

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

303. In this case, infringements were identified of Articles 5(1)(f), 32(1), 32(2), 33(1), 34(1) and 34(4) GDPR. The gravest infringements is that of Article 5(1)(f) in the circumstances, which represents an infringement of a core principle of GDPR. In this case, a cap of €1,000,000 is set out in section 141(4) of the 2018 Act (see section ii below). Thus, €1,000,000 is the cumulative cap for the fines set out in this Decision.

ii. Categorisation of the infringements under Articles 83(4)-(6) GDPR

304. Articles 83(4)-(6) GDPR set out the caps that apply under GDPR. The EDPB Fining Guidelines say that the categorisation of infringements under Article 83(4)-(6) GDPR can be used to determine the starting point for further calculation. Those Guidelines note that:

> With this distinction, the legislator provided a first indication of the seriousness of the infringement in an abstract sense. The more serious the infringement, the higher the fine is likely to be.[144]

[144] EDPB Fining Guidelines, para 50.

305. The categorisation of infringements under Articles 83(4) or (5) is a relevant consideration in assessing the seriousness of the infringements in this case. The infringement of Article 5(1)(f) found in this case relates to the basic principles of processing and is ascribed considerably greater significance, with the legislator providing for, in general, maximum administrative fines double those applicable to the infringements of Articles 32(1), 32(2), 33(1), 34(1) and 34(4).

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

306. The EDPB Guidelines state that the factors assessed in relation to Articles 83(2)(a), (b) and (g) GDPR indicate the seriousness of the infringement.[145] These factors were assessed in paragraphs 230 to 262 and 274 to 275 above. The Guidelines also state that:

> This assessment is no mathematical calculation in which the abovementioned factors are considered individually, but rather a thorough evaluation of the concrete circumstances of the case, in which all of the abovementioned factors are interlinked. Therefore, in reviewing the seriousness of the infringement, regard should be given to the infringement as a whole.[146]

307. Having regard to these factors as a whole, the infringements identified in this case are of a high seriousness. Under Article 83(2)(a), the infringements were found to be of a serious nature and have a high degree of gravity. The infringements were also found to have been of moderate and substantial duration. The infringements affected personal data which, by their nature, carry a risk with regard to the fundamental rights and freedoms of data subjects, as assessed under Article 83(2)(g). CDETB were also negligent with respect to the infringements, and intentional regarding the infringement of Article 34(4) as assessed under Article 83(2)(b). Therefore, balancing these factors, the DPC considers that the infringements were of high seriousness.

iv. Imposing an effective, dissuasive and proportionate fine

308. Article 83(1) GDPR requires a fine to be effective, proportionate and dissuasive in each individual case. As the guidelines also say that this does not 'dismiss a supervisory authority from the responsibility to carry out a review of the effectiveness, dissuasiveness and proportionality at the end of the calculation,'[147] Article 83(1) will be considered again at the end of this calculation.

---

[145] EDPB Fining Guidelines, para 51.

[146] EDPB Fining Guidelines, para 59.

[147] EDPB Fining Guidelines, para 64.

v. Aggravating and mitigating circumstances

309. Articles 83(2)(a), (b) and (g) GDPR were considered above in relation to the starting point for the calculation of the fine. In line with the approach suggested in the EDPB Fining Guidelines,[148] this section considers the aggravating or mitigating impact of the remaining criteria in Article 83(2) GDPR.

310. In relation to Article 83(2)(c), it was noted that CDETB had not adopted measures to mitigate the damage to data subjects. However, as noted in paragraph 264, CDETB made a number of substantial technical and organisational changes as a result of this data breach and also took steps to investigate the security incident prior to notifying the DPC. This is considered to be a mitigating factor of low weight.

311. In relation to Article 83(2)(d), it was noted that CDETB had a high degree of responsibility for the infringements. CDETB appeared to be unaware that its website was processing personal data. This indicates that no adequate data protection risk analysis was undertaken; as a result, it was not possible for CDETB to implement technical and organisational measures that were appropriate to the risks. However, in circumstances where this factor forms the basis for the finding of the infringement of Article 32 GDPR against CDETB, this factor cannot be considered aggravating in respect of the infringements. Therefore, the DPC considers that this factor is neither aggravating nor mitigating in the circumstances.

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

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

314. In relation to Article 83(2)(h), it was noted that the manner in which the infringement became known to the DPC was through a breach notification. This factor is considered to be neither mitigating nor aggravating.

315. In relation to Article 83(2)(i), it was noted that orders had not been previously ordered by the DPC[149] with regard to the same subject matter. This factor is considered to be neither mitigating nor aggravating.

---

[148] EDPB Fining Guidelines, para 70.

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

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

317. In relation to Article 83(2)(k), it was noted that CDETB had admitted to the infringements set out in the Draft Decision and proactively took steps, without having been specifically directed to do so by the DPC, to limit the risk of similar incidents occurring in future. This is considered to be a mitigating factor of medium weight.

318. Taking into account all of the matters arising for consideration as part of the individual assessments required to be carried out pursuant to Article 83(2) together with the requirements of the Fining Guidelines, as detailed above, the DPC imposes the following fines:

- €50,000 for the infringement of Articles 5(1)(f), 32(1) and 32(2) GDPR.
- €15,000 for the infringement of Article 33(1) GDPR.
- €10,000 for the infringement of Article 34(1) GDPR.
- €50,000 for the infringement of Article 34(4) GDPR.

These fines, totalling €125,000, are substantially lower than the fining range proposed in the Draft Decision, the maximum of which was €210,000. The final fines reflect the mitigation occasioned by CDETB accepting each of the findings of infringements set out in the Draft Decision, acknowledging full responsibility for the breach, apologising to both the data subjects affected and the regulator and putting in place the measures set out above in order to reduce the likelihood of similar breaches occurring in future.

vi. The relevant legal maximums for the different processing operations

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

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

Effectiveness

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

Dissuasiveness

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

322. Each infringement is serious in nature and gravity as set out pursuant to Article 83(2)(a) GDPR. Infringements that are of a serious nature and gravity must be strongly dissuaded both in respect of the individual controller and in respect of other entities carrying out similar processing. Regarding the infringements of Articles 5(1)(f), 32(1), 32(2), 33(1), 34(1) and 34(4), the DPC considers that CDETB's non-compliance with its obligations under GDPR must be strongly dissuaded. Such dissuasive effect is crucial for protecting the rights and freedoms of those data subjects by implementing appropriate measures. Therefore, the DPC considers that the administrative fines are appropriate and necessary in order to dissuade non-compliance.

323. The DPC considers that the negligent character of CDETB's infringements of Articles 5(1)(f), 32(1), 32(2), 33(1) and 34(1) and CDETB's intentional infringement of Article 34(4) carries weight when considering the amount of those fines. This negligence suggests that the administrative fines are necessary to ensure that CDETB directs sufficient attention to its obligations under GDPR in the future.

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

325. The DPC has had regard to the lack of previous relevant infringements by CDETB, which is a slightly mitigating factor. The DPC has also had regard to the actions taken by CDETB as a result of the breach, including CDETB's actions in having admitted to the infringements set out in the Draft Decision, in apologising and in proactively taking steps, without having been specifically directed to do so by the DPC, to limit the risk of similar incidents occurring in future. These have also been considered as mitigating factors. In light of the negligent character of the infringements of Articles 5(1)(f), 32(1), 32(2), 33(1) and 34(1) and the intentional nature of the infringement of Article 34(4), combined with CDETB's failure to comply with its obligations with regard to data protection, the DPC considers that dissuasive administrative fines to the extent imposed are necessary in the circumstances to ensure future compliance.

Proportionality

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

327. Having regard to the nature, gravity and duration of the infringements, the DPC considers that the administrative fines to the extent imposed are proportionate in the circumstances in view of ensuring compliance. CDETB's infringements of GDPR were a primary cause of the data breach. In light of this damage, the DPC considers that the administrative fines are proportionate to responding to CDETB's infringements with a view to ensuring future compliance. The DPC considers that administrative fines do not exceed what is necessary to enforce compliance in respect of the infringements identified in this Decision.

L. Summary of Corrective Powers

328. In summary, the corrective powers that the DPC exercises are:

- A Reprimand to CDETB pursuant to Article 58(2)(b) GDPR regarding the infringements identified in this Decision; and
- An Order to bring processing into compliance in respect of CDETB's infringement of Articles 5(1)(f), 32(1), 32(2), 33(1) and 34(1) GDPR; and,
- Administrative fines, totalling €125,000, as follows:
    1. In respect of CDETB's infringement of Articles 5(1)(f), 32(1) and 32(2) GDPR, a fine of €50,000.
    2. In respect of CDETB's infringement of Articles 33(1) GDPR, a fine of €15,000.
    3. In respect of CDETB's infringement of Article 34(1) GDPR, a fine of €10,000.
    4. In respect of CDETB's infringement of Article 34(4) GDPR, a fine of €50,000.

M. Right of appeal

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

This Decision is addressed to:

City of Dublin Education and Training Board
1-3 Merrion Road,
Dublin 4,
D04 PP46, Ireland

Decision-Makers for the Data Protection Commission:

Dr. Des Hogan
Commissioner for Data Protection
Chairperson

Dale Sunderland
Commissioner for Data Protection