In the matter of the General Data Protection Regulation

DPC Case Reference: IN-21-2-5

In the matter of VIEC Limited t/a

Virtue Integrated Elder Care Ltd.

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

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

DECISION

Decision-Maker for the Data Protection Commission:

_____

Helen Dixon
Commissioner for Data Protection

20 December 2022

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Contents

A. Introduction

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

2. Virtue Eldercare t/a Virtue Integrated Eldercare (**'VIEC'**) was provided with the draft decision (**'the Draft Decision)** on this inquiry on 11 November 2022 to give it the final opportunity to make submissions. This Decision is being provided to VIEC pursuant to section 116(1)(a) of the 2018 Act in order to give VIEC notice of the Decision, the reasons for it, and the corrective powers that I have decided to exercise.

3. This Decision contains corrective powers under section 115 of the 2018 Act and Article 58(2) of the General Data Protection Regulation ('the GDPR') arising from the infringements which have been identified herein. In this regard, VIEC is required to comply with these corrective powers, and it is open to this office to serve an enforcement notice on VIEC in accordance with section 133 of the 2018 Act.

B. Legal Framework for the Inquiry and the Decision

i) Legal Basis for the Inquiry

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

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

ii) Data Controller

6. In commencing the Inquiry, the DPC considered that VIEC may have been the controller, within the meaning of Article 4(7) GDPR, in respect of personal data that was the subject of the personal data breach notification. In this regard, VIEC had stated that it was the controller in its notification of 19 August 2020.[1]

[1] C.1.a Breach Notification 19 Aug 2020

iii) Legal Basis for the Decision

7. The decision-making process for the Inquiry which applies to this case is provided for under section 111 of the 2018 Act, and requires that the DPC must consider the information obtained during the Inquiry to decide whether an infringement is occurring or has occurred and, if so, to decide on the corrective powers, if any, to be exercised. As the sole member of the DPC as defined in section 15 of the 2018 Act, I perform this function in my role as the decision-maker in the DPC. In so doing, I am required to assess all of the materials and submissions gathered during the Inquiry and any other materials which I consider to be relevant, in the course of the decision-making process.

8. A full schedule of all documentation considered by me for the purpose of the preparation of this Decision is appended hereto.

9. Having considered the information obtained in the Inquiry, I am satisfied that the Inquiry has been correctly conducted and that fair procedures have been followed throughout. I have also had regard to the submissions that VIEC decided to make in respect of the Draft Decision on 1 December 2022 before proceeding to make this final Decision under section 111 of the 2018 Act.

C. Factual Background

10. VIEC operates and manages five nursing homes on the Southside of Dublin and in County Louth. It is headquartered in Dun Laoghaire, County Dublin.

11. VIEC is overseen by a Board of Directors made up of an independent Chair, four independent non-executive Directors, two executive Directors and one personal advisor.[2]

12. The issue became known following a report to the VIEC IT helpdesk on 15 August 2020 from a user indicating that they were being blocked from sending emails.

13. The DPC received notification of a personal data breach from VIEC on 19 August 2020. VIEC outlined that it had discovered that the email address of one of its managers had been subject to a phishing attack and that emails had been rerouted to a third party gmail account.

14. This breach notification was logged by the DPC as BN-20-8-401. The documentation received and correspondence related to the DPC's handling of this notified breach are exhibited at Appendix C.1.[3]

15. Based on the analysis undertaken of the breach notification and subsequent documentation provided during the breach handling process, the DPC considered that the matter concerned a possible "*breach of security potentially leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"* by VIEC.[4]

---

2 https://www.virtue.ie/board-of-directors/ accessed on 5 May 2021

3 Appendix C.1a Breach Notification

4 Definition of Personal Data Breach per Article 4(12) GDPR

16. The decision to commence the Inquiry was taken having regard to the circumstances of the personal data breach notified by VIEC. The Commencement Letter informed VIEC that the Inquiry would examine whether or not VIEC discharged its obligations in connection with the subject matter of the personal data breach and determine whether or not any provision(s) of the 2018 Act and/or the GDPR had been contravened by VIEC in that context. In this regard, the scope of the Inquiry was stated to include:

    - the steps taken by VIEC to comply with the principle of integrity and confidentiality pursuant to Article 5(1)(f) GDPR;
    - the technical and organisational measures taken by VIEC to ensure security of processing pursuant to Article 32(1) GDPR;
    - the ability of VIEC to demonstrate ongoing confidentiality, integrity, availability of personal data pursuant to Article 32(1)(b) GDPR;
    - the process employed by VIEC for regularly testing the effectiveness of measures for ensuring appropriate security pursuant to Article 32(1)(d) GDPR;
    - the ability of VIEC to demonstrate that it had assessed the risk to processing special category information.[5]

17. The Commencement Letter set out that the Inquiry would formally document the facts as they relate to the subject matter of the Inquiry. The facts, as established during the course of the Inquiry, are set out below in this Decision.

18. In its submissions of 6 April 2021 VIEC outlined the relevant technical and organisational measures in place to meet the requirements of the GDPR prior to the breach including policies and procedures, staff training and quality assurance sampling in relation to data protection governance.[6] It also listed steps that had been taken since the personal data breach in order to comply with the GDPR, including details of certain revised organisational and technical measures. The submissions appended a number of documents, which are considered throughout this Decision.

19. The DPC prepared an Inquiry Issues Paper to document the relevant facts established and the issues that fell for consideration by me, as Decision Maker, for the purpose of making a decision under section 111 of the 2018 Act in respect of this Inquiry. The DPC furnished VIEC with the Inquiry Issues Paper on 23 August 2021 and invited VIEC's submissions on any inaccuracies and/or incompleteness of the facts.

20. VIEC provided submissions on the Inquiry Issues Paper on 30 September 2021.[7] This included mitigating factors to be considered in relation to the data breach along with some textual amendments and supplemental information relating to the facts as set out in the Inquiry Issues Paper. Further information on enhanced organisational and technical measures introduced

---

5 Appendix C.1.s Commencement Letter 8 March 2021
6 Appendix C.2a VIEC Submission 6 April 2021
7 Appendix C.4.a pages 6-8 VIEC Submissions 30 September 2021

were also included. These comments were analysed and considered by me in the preparation of this Decision.

21. Ortus, the security provider for VIEC, completed a report and indicated that the most likely root cause of the breach was that the credentials of a user account at the Four Ferns nursing home were captured on a fake website. [8][9][10] The link to that fake website was likely received in a phishing email. The originating email that delivered the malicious link was not identified by Ortus. The email account was accessed by an unauthorised third party, using the captured credentials. This resulted in unauthorised access to stored emails and allowed the bad actor to set up email forwarding of all inbound emails to a third party email account. The presence of the forwarding rules indicated ongoing unauthorised access to and unauthorised disclosure of personal data. The breach notification of 19 August 2020 indicated that the issue had been ongoing since 18 July 2020.

22. On 30 September 2021, VIEC provided submissions in response to the DPC's Issues Paper. VIEC stated:

> "*Virtue DPO was aware of the requirements to report the breach within 72 hour and that this timeline had been exhausted by the time knowledge of the breach reached the DPO desk. In haste the DPO proceeded with the report based on the first notification received (**see attached Exhibit A**[11]) however, this proved not to be reflective of the true scope of the breach after investigation. Virtue submitted an amendment to the original report reflecting this."*[12]

23. I would like to highlight that, as per Article 33 GDPR:

> *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… [**Emphasis added**]*

24. The Guidelines on Personal Data Breach Notification included:

> *WP29 considers that a controller should be regarded as having become "aware" when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.* [13]

25. I note that in this instance VIEC provided a notification, after becoming aware of the personal data breach and supplemented this notification with additional information thereafter. This is an example of good practice on the part of a data controller following a personal data breach.

26. Ortus carried out the following mitigation measures:

> *"The password for the affected account was reset and a forced logout was performed to remove any current sessions. A check was performed for forwarding and sweep*

---

8 Appendix C.1p Ortus Incident Summary

9 Actual email address provided by VIEC has been redacted

10 (●●●●●●●●●●manager@fourferns.ie)

11 Appendix C.4d

12 Appendix C.4b Minor Corrections and Clarifications page 1

13 Working Party Guidelines on Data Breach Notification WP250rev.01, as adopted by EDPB, Page 10-11

rules in Outlook Web App which revealed that a forwarding rule was in place. A search was then conducted on the entire e-mail domain to find the particular email that may have caused this issue, but it could not be identified within the stored emails or the log files (which were only retained for 90 days). The forwarding rule which was in place was then removed."

27. On 27 August 2020 VIEC informed the DPC that the forwarding rule copying the emails to the phishing account had been in place longer than initially reported.

> *"The records available through Microsoft 365 only go back for 90 days and we can see this was ongoing throughout that period but cannot identify how much longer it has been in effect."*[14]

28. VIEC provided further information on the 90 day retention period[15]:

> *"This is the default retention period for Office 365 audit logs.*
> *Additional Microsoft service required to extend logs retention past 90 days.*
> *VIEC do not have this service."*[16]

29. VIEC outlined that the categories of personal data disclosed as a result of the breach included special category personal data:

- Name
- Address
- Email address
- Telephone number
- PPSN
- Employee data – probation reviews and rosters
- Health data
- Biometric data[17]

30. VIEC provided a timeline in relation to the incident, which noted that a communication was sent from the VIEC DPO on 6 October 2020 to all staff affected by email forwarding and another communication from the VIEC DPO on 7 October 2020 to all residents and external third parties affected by the email forwarding.[18] In both communications, the recipients were informed of the incident in the following terms:

> *"…the Four Ferns email system has been subject to an email redirection/forwarding scheme put in place by an unknown third party.*
>
> *"Investigation indicates that the purpose of this scheme was to collect details relating to company processes, however while attempting to extract this information the third party also diverted a number of operational emails containing information relating to staff and residents at the Four Ferns. We have reviewed the content of emails that*

---

14 Appendix C.1b Breach Update 27 August 2021
15 Appendix C.1q Commission Queries 24 Nov 2020
16 Appendix C.1r Response to Commission Queries (12) 4 Dec 2020 page 3
17 Appendix C.1d Response to DPC Queries 8 Oct 2020
18 See appendix C.1e and C.1f

were shared with the third party and have identified emails, containing information relating to you, were included in this breach.…"

31. VIEC provided details to the DPC of the unauthorised email forwarding rule logic as:

> "*Forward copy of incoming message to ●●●●●●●●●●@gmail.com if the subject or body of the mail includes one of the below specific words:*
>
> • *Bank transfer*
>
> • *Bank details*
>
> • *Payment*
>
> • *Invoice*
>
> • *Deposit*
>
> • *Quote*
>
> • *Bacs*
>
> • *Due"*[19]

32. I note VIEC notified potentially at-risk data subjects that the purpose of the phishing attack was to *"collect details relating to company processes".* However, I would query as to how VIEC came to such a conclusion given the nature of the words triggering the forwarding rule that suggest a fraudulent aim.

33. VIEC indicated that while it had contained the spread of the phishing email, it was unable to identify the source of the attack.

34. In response to further questions on 24 November 2020[20] from the DPC team handling the breach notification, VIEC clarified that the forwarding rule "Block external forwarding" had not been in place prior to 15 August 2020 on the affected manager's account.[21]

35. VIEC provided a description of its IT infrastructure including in relation to:

- Firewalls
- Workstations
- Domain Controllers
- App Servers

36. VIEC stated that it had system logs for the previous three months. An audit of the available logs indicated no suspicious activity related to this breach during that period:

> *"Audit covers sending/ receiving mail and file and folder access for user. No suspicious activity for the last 3 months."*[22]

VIEC conducted a deep scan on all workstations and servers and it provided a copy of the outcome report to the DPC.[23] The scan identified two instances of a potentially unwanted

---

19 Appendix C.1d Response to Commission Queries 8 Oct 2020 page 2
20 Appendix C.1q Commission Queries 24 Nov 2020
21 Appendix C.1r Response to Commission Queries (12) 4 Dec 2020 page 2
22 Appendix C.1d Response to Commission Queries 8 Oct 2020
23 Appendix C.1i Workstation and Server Scans

programme ('PUA') called Mindspark and also three triggers from a generic heuristic Trojan check.

37. In its submissions dated 6 November 2020, VIEC provided additional documentation, including a log file of activity within the affected ●●●●●●●●●●manager@fourferns.ie email account.[24]

38. VIEC conducted the following reviews and actions in order to ascertain if any other employee email accounts had been affected:

> *"Scan mailboxes for forwarding rules*
>
> *Site wide password reset completed*
>
> *Full site wide anti-virus and anti-malware scan"*[25]

39. VIEC clarified that 213 individuals had their personal data compromised. Of that number, VIEC stated that:

> *"129 residents had special category data compromised*
>
> *117 individuals had health data compromised in the breach*
>
> *12 residents had biometric data compromised in the breach"*[26]

40. In response to further questions on 24 November 2020 from the DPC team handling the breach notification, [27] VIEC clarified that there were 170 files affected by the breach relating to the 213 individuals and that:

> *"none of the emails or attachments were password protected."*[28]

41. On 11 November 2022 I provided the Draft Decision to VIEC. VIEC was afforded the opportunity to make submissions on the proposed infringements that were provisionally identified in the Draft Decision and the corrective powers that I proposed to exercise. On 1 December 2022 VIEC made submissions on the Draft Decision. I have had full regard to those submissions and I have reached conclusions that infringements of data protection legislation have occurred and that it is necessary to exercise certain corrective powers. Those infringements and corrective powers are set out in this Decision.

D. VIEC's submissions in relation to the Draft Decision

42. The Draft Decision was provided to VIEC on 11 November 2022, and VIEC was requested to furnish any submissions it wished to make to the DPC by 2 December 2021. VIEC furnished its submissions in respect of the Draft Decision on 10 August 2021 ('**Submissions in relation to the Draft Decision'**). VIEC stated that its submissions were in respect of the proposed administrative fine, which VIEC considered excessive.

---

24 Appendix C.1m Forensic Analysis Log File
25 Appendix C.1l Response to Commission Queries (35) 6 Nov 2020 page 2
26 Appendix C.1l Response to Commission Queries (35) 6 Nov 2020 pages 2-3
27 Appendix C.1q Commission Queries 24 Nov 2020
28 Appendix C.1r Response to Commission Queries (12) 4 Dec 2020 page 1

43. I have had regard to VIEC's submissions in relation to the administrative fine in Part L below.

44. VIEC made further submissions regarding the effect of the Covid-19 pandemic on its ability to take actions and implement improvements in relation to the security of processing of patient data. VIEC made reference to the final report of the Oireachtas Special Committee on Covid-19 regarding the preparation of nursing homes during the pandemic and the disproportionate threat that Covid-19. VIEC stated that:

> "*As local management were impacted by Covid-19 sick leave, many senior managers were redirected to the frontline, an example of this happened in the Four Ferns where this breach was detected, the Director of Operations worked for 5 straight weeks, with minimal breaks on front line management."*[29]

45. VIEC also referenced the increased regularity of phishing attacks as a result of the Covid-19 pandemic.

> *"The F5Labs 2020 Phishing and Fraud Report has shown that COVID-19 continued to "significantly embolden cybercriminals phishing and fraud efforts" and stated that phishing incidents rose 220% during the height of the global pandemic."*[30]

46. While I do recognise that the Covid-19 pandemic brought additional challenges to all those working within the healthcare sector and healthcare providers themselves, I consider that the shortcomings in VIEC's processing of personal and special category data existed since the implementation of the GDPR. It is incumbent on controllers to implement appropriate technical and organisational measures to ensure appropriate security of the personal data they process. Regrettably, in recent years it has been shown that malicious actors will target healthcare providers through phishing and/or malware attacks and this increases the importance of having robust security systems in place to ensure the rights and freedoms of the data subjects are protected.

47. [redacted]

[redacted]

[redacted]

[29] Appendix C.7.a page 2

[30] Appendix C.7.a page 3

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

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

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

50. In this regard, the Commencement Letter specified that the Inquiry would focus on VIEC's organisational and technical measures in place to ensure security of the personal data. In particular, the Commencement Letter expressly stated that the scope of the Inquiry would include Articles 5(1)(f) and 32(1) GDPR. The Commencement Letter stated that the Inquiry would focus on the areas of Data Protection Governance, Training and Awareness, Records Management and Security of Personal Data. The Commencement Letter also noted that:

> *"the Commission reserves the right to include in its findings from the Inquiry one or more determinations as to VIEC's compliance with Articles 5(2), 30 and/or 31 GDPR*."

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

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

[redacted]

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

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

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

> *'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;*

54. Article 9 GDPR provides for the prohibition of processing of health data:

> *Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.*

55. Article 9(2)(h) GDPR provides for an exception to this prohibition in circumstances where:

> *processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3*

56. However, this exception is subject to the requirement in Article 9(3) GDPR that:

> *Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.*

57. In this case, the breached data was processed by means of an email system and contained the personal data of VIEC's customers along with special category (health and biometric) data. The breach concerned a phishing attack, which resulted from unauthorised access to personal and special category data held by VIEC. Therefore, the personal data processed by VIEC fell within the scope of the GDPR.

58. Recital 15 GDPR provides guidance for interpreting the material scope of the GDPR:

In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.

59. 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.*

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

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

61. 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. This term "*state of the art*" is not defined within the GDPR. By dictionary definition, it is defined as "*using the latest techniques or equipment*".[32]

[32] Concise Oxford Dictionary, (8th ed., BCA & Oxford University Press, 1991)

F. Issues for Determination

62. The Inquiry Issues Paper identified that the following questions arise for determination:

a) **An assessment of the risks** of varying likelihood and severity for the rights and freedoms of natural persons associated with VIEC's processing of personal data on its email systems, having regard to VIEC's own assessment of these risks.

b) An evaluation of the **adequacy of the risk assessment that VIEC carried out** prior to the breach of the risks of varying likelihood and severity for the rights and freedoms of natural persons associated with VIEC's processing of personal data on its email system.

c) Whether the **measures implemented by VIEC prior to the breach were appropriate** to ensure the ongoing confidentiality of the processing of personal data on the email system, particularly where the controller has indicated that it processes special category personal data. In assessing the appropriateness of the measures implemented, the DPC will have particular regard to steps taken to ensure that the email filing system was not used as a repository of personal data, and that any pertinent data was properly filed into a formal filing system that had appropriate security measures, such as proper backups/restore functionality, encryption at rest, properly applied retention schedules, ability to service subject access requests amongst others. Furthermore, regard will be given to the level of governance implemented over the policies and procedures relating to security and access; the level of training and awareness provided to staff; technical measures, and any other measures that VIEC implemented at the time of the personal data breaches; and

d) Whether the measures implemented by VIEC were appropriate in light of any obligation that it may have been under to implement a process for **regularly testing, assessing and evaluating the effectiveness of its technical and organisational measures** in respect of the security of the email system.

e) Whether the measures implemented by VIEC prior to **and after the breach** were appropriate in light of the obligation that it was under to demonstrate compliance with the principles of GDPR.

63. Therefore, having considered the Commencement Letter, the Inquiry Issues Paper and the other relevant materials, it falls for me to determine in this Decision whether VIEC has complied with those aspects of its obligations under Articles 5(1)(f) and 32(1) GDPR when implementing appropriate technical and organisational measures to ensure appropriate security of the personal data of customers.

G. Analysis of the Issues for Determination

a) Assessment of the Risks

64. 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 processing. Regarding VIEC's processing of personal and special category data on its email system, those risks include the risk of unauthorised access and unauthorised disclosure of personal data to third parties of personal data processed within the system.

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

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

66. *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources and others* provides further guidance on the risk assessment.[33] In this case, the Court of Justice of the European Union ('the **CJEU**') declared the Data Retention Directive invalid.[34] The Directive required electronic communication service providers to retain certain data for a period of time. The Court held that the Directive did not ensure effective protection of the data retained against the risk of abuse and unlawful access in circumstances where it did not lay down specific rules in relation to:

> *(i) the vast quantity of data whose retention is required by that directive,*
>
> *(ii) the sensitive nature of that data and*
>
> *(iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality.*[35]

67. 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 VIEC's processing of personal data must consider, first, the likelihood of unauthorised disclosure of, or access to, the personal data, and second, the severity of that risk in respect of the rights and freedoms of the data subjects. These objective assessments should have been made by reference to the nature, scope, context and purposes

---

33 Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, intervener: Irish Human Rights Commission, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others, judgment of 8 April 2014 (ECLI:EU:C:2014:238).

34 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

35 Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd, op. cit, para 66.

of the processing. In considering these factors, regard must also be had to the quantity of personal data processed and the sensitivity of that data.

68. The assessment within this section of the Decision is concerned with how VIEC evaluated the risk arising in respect of the security of personal data and, in particular, the risk arising from the use of the email system to process personal data. As stated above, those risks arose due to VIEC's use of its email system to process personal data, including special category data.

69. VIEC processed the data of 213 data subjects through its email system including, among others, name, address, email address, telephone number, and PPSN. VIEC also stated that employee data, such as probation reviews and rosters, formed part of the breached data although VIEC did not provide any information to the DPC as to the number of employees that were affected.

70. Moreover, VIEC processed data deemed to be special categories of personal data under Article 9 GDPR including health data, and biometric data. These kinds of data are high risk with regard to the fundamental rights and freedoms of individuals as loss of control of special category or financial personal data is likely to cause serious distress. There is a prohibition on processing of special categories of personal data due to their sensitive nature, however this may be derogated from for the management of healthcare services, subject to suitable safeguards. Thus, the nature of personal data processed by VIEC increases the severity of the risks, as illustrated in Recital 75 GDPR and there was a corresponding requirement to take more robust measures to protect the security of the processing.

71. The nature of VIEC's processing of personal data via its email system is considered to be high risk as it included health and biometric data pertaining to residents which is defined as special category data under Article 9 GDPR.

72. VIEC provided copies of its 'Risk Management Policy', 'Quality and Risk Framework', 'Quality Safety and Risk Committee Terms of Reference' and draft terms of reference for Quality Board Level Sub Committee.[36]

73. VIEC outlined that it carried out data protection impact assessments for what it classified as high risk data processing activities. VIEC indicated that such assessments were carried out with the implementation of its Vcare and Cemplicity software since 2019.

> *"The company recognises the value and importance of these assessments during the pre-implementation process to ensure regulatory compliance and proactively manage any data protection risks that are identified as part of the assessment."*[37]

74. 'The Risk Management Policy' outlined the various roles, which make up VIEC's risk management process, including staff, the Executive Management Team and the Quality Safety

[36] Appendix C.2b-e VIEC Submission 6 April 2021 Risk Management Policy, Quality and Risk Framework, Quality Safety and Risk Committee TOR, Quality Board Sub Committee TOR

[37] Appendix C.2a VIEC Submission 6 April 2021 Response page 2

and Risk Committee. The Quality Safety and Risk Committee's terms of reference notes that the Committee's purpose is to:

> *"…manage risks at the organisational, service and system levels…"*[38]

However, there were no specific references to data protection in terms of risk.[39]

75. A further document provided by VIEC, the 'Quality Board Sub Committee – Terms of Reference' stated that part of the remit of the Sub Committee is:

> *"to assist the Board in fulfilling its oversight responsibilities in the areas relating to….. data protection…."*[40]

However, there was no further elaboration in the document on how this role was to be carried out. The document was undated and in draft format.

76. VIEC stated that:

> *"The Quality Board Sub Committee was a new initiative in progress at the time of the last submission, and the TOR had not yet been ratified by the Board therefore were in draft. They have since been signed off and the Quality Board Sub Committee will meet quarterly to review and advise on risk items including GDPR risks. A Quality, Safety and Risk Manager has now been appointed and will commence Dec 2021 who will take over the role of DPO, lead the discussions at the sub-committee and manage the data protection risk register for presentation at the forum. Until then the data protection risk register is managed by the Acting DPO reporting to the CEO directly on any additions or amendments."*[41]

77. In this case, VIEC's use of its email system as a means to store and share patient records created the risk of unauthorised access and unauthorised disclosure of personal data to third parties of personal and special category data processed within the email system. In particular, the storage of biometric data on VIEC's email system created a high risk in relation to the rights and freedoms of the relevant data subjects. An adequate assessment of the risks created would have queried the necessity of using the email system in such a manner.

78. In the absence of appropriate technical and organisational measures, and given that there was a large quantity of personal data processed through the email system, there was a high risk of unauthorised access to the personal and special category data processed by VIEC in this matter.

79. I find that VIEC's processing of personal and special category data on its email system created a high risk to the rights and freedoms of natural persons in terms of both likelihood and severity. As outlined above, the risk of unlawful access to the personal data processed in the email system is high in the absence of appropriate technical and organisational measures. The severity of that risk is also high in circumstances where the data processed is special category

---

38 Appendix C.2e VIEC Submission 6 April 2021 Quality Safety and Risk Committee TOR page 1
39 Appendix C.4b Minor Corrections and Clarifications page 2
40 Appendix C.2e VIEC Submission 6 April 2021 Quality Board Sub-Committee TOR
41 Appendix C.4b Minor Corrections and Clarifications page 4

in many instances and could result in a loss of control of medical data or fraud attacks through email redirection.

b) Measures Implemented by VIEC to Address the Risks

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

81. 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 sensitive patient data.

82. VIEC's submissions outlined the technical and organisational measures that it had in place at the time of the personal data breaches to comply with Article 32 GDPR and by reference to the principle set down in Article 5(1)(f) GDPR. The measures relevant to VIEC's processing of personal data as part of its email service can be categorised as:

    a. Data Protection Governance,

    b. Training and Awareness,

    c. Security of Personal Data.

a. Data Protection Governance

83. VIEC outlined that it had a range of policies and procedures in relation to data protection to ensure the accuracy and security of customers' personal data. :

- Data Protection Policy;[42]
- Employee Data Access Policy[43];
- Risk Management Policy[44];
- Management of Personal Data in line with Data Protection Requirements (incorporating GDPR).[45]

84. I note that the 'Data Protection Policy' referred to the Data Protection Acts 1988 and 2003 and did not make reference to the GDPR or the Data Protection Act 2018 which have been in force since May 2018. Similarly, the Employee Data Policy does not refer to the GDPR or the Data Protection Act 2018. VIEC claimed that this was an oversight on its part and would be rectified immediately. VIEC also stated that:

---

42 Appendix C.2n VIEC Submission 6 April 2021 Employee Handbook page 44
43 Appendix C.2n VIEC Submission 6 April 2021 Employee Handbook page 46
44 Appendix C.2b VIEC Submission 6 April 2021 Risk Management Policy
45 Appendix C.2k VIEC Submission 6 April 2021 Management of Personal Data Policy

"The principles listed within the handbook however are accurate in reflecting the most relevant areas for our staff teams to be aware of while discharging their duties."

85. VIEC's 'Management of Personal Data in line with Data Protection Requirements' (incorporating GDPR) outlines the use of personal passwords and the necessity to encrypt files that contain personal data where it is to be shared over external networks. [46]

86. The failure to implement such measures directly contributed to the data breach. I consider that VIEC did not implement appropriate Data Protection Governance measures to meet the standard required in light of the risk posed by the processing.

87. VIEC has also provided an overview of enhanced technical and organisational measures that have been implemented since the occurrence of the breach. This included the use of new data protection software across the organisation, the nomination of data protection champions in each location and the appointment of a Quality and Risk Manager. In relation to technical measures, VIEC has implemented conditional access for all email, multi-factor authentication, and a mobile device policy. As regards training, VIEC now requires staff to undergo HSEland "good information practices" training. Staff with access to a VIEC email account receive Security Awareness Training quarterly.

b. Training and Awareness

87. VIEC gave details of various training and awareness programmes including:

- Manager-led training on Employee Handbook for all new employees with associated staff sign off including Data Protection Policy and Employee Data Policy; [47]

88. VIEC also stated that upgrades to contracts for service were agreed to include security awareness training for two new sites, which joined the group in February 2020. However, all four locations were subject to Covid-19 outbreaks and HSE restrictions which impacted implementation timelines. [48]

89. VIEC confirmed that phishing and ransomware awareness training was provided to all staff in March 2021 following VIEC becoming aware of the breach on 15 August 2020. VIEC added it uses the HSE's training portal HSELand.[49] Similarly, user awareness training, security awareness training and security training for staff took place in March 2021.[50][51] However, VIEC did not provide any evidence of phishing training provided to staff prior to the data breach. I consider that the provision of phishing training is an appropriate security measure considering the risks and the sensitivity of the data processed by VIEC. Therefore, I consider that the failure

[46] Appendix C.2k VIEC Submission 6 April 2021 Management of Personal Data Policy page 14
[47] Appendix C.2a VIEC Submission 6 April 2021 Response page 2
[48] Appendix C.2a VIEC Submission 6 April 2021 Response page 14
[49] https://healthservice.hse.ie/staff/training-development/training/online-training-hseland.html
[50] Appendix C.2a VIEC Submission 6 April 2021 Response page 17
[51] Appendix C.2a VIEC Submission 6 April 2021 Response page 18

to implement such training prior to the data breach was an infringement of Article 5(1)(f) and Article 32.

90. In light of the sensitivity of the personal data handled by VIEC, I consider that an appropriate level of security must include regular data protection and awareness training to staff.

c. Security of Personal Data

i. Technical Measures

91. In addition to the policies and procedures noted above, VIEC described specific technical measures relating to the security of personal data it stated were in place at the time of the breach, including:

- Group policy to save mail sent from shared mailbox centrally for future review;
- Group policy to automatically encrypt (BitLocker) any desktop or laptop that is connected to VIEC domains;
- The review of operating systems to ensure that they were up to date;
- Announced and unannounced audits in relation to regulatory compliance;[52]
- Password policy.

92. VIEC outlined that prior to the data breach account passwords were required to satisfy certain parameters such as length, complexity, use of different characters and not to contain account name or usernames.[53] Furthermore, such passwords were required to be changed every 90 days. However, VIEC noted that:

> *"Majority of user's passwords set not to expire"*[54]

93. VIEC also stated that of the 170 files relating to the 213 individuals that were part of the breach:

> *"none of the emails or attachments were password protected."*[55]

94. 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, *inter alia,* as appropriate:

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

[52] Appendix C.2a VIEC Submission 6 April 2021 Response page 6
[53] Appendix C.2a VIEC Submission 6 April 2021 Response page 9
[54] Appendix C.1l Response to Commission Queries (35) 6 Nov 2020 page 8
[55] Appendix C.1r Response to Commission Queries (12) 4 Dec 2020 page 1

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

95. VIEC has described a range of technical measures, which it indicated were in place at the time of the breach, or have been subsequently introduced. However, at the time of the personal data breach, the majority of users' passwords were not set to expire and VIEC did not implement multifactor authentication for users logging into accounts. In those circumstances, I consider that VIEC failed to implement appropriate measures to protect the integrity of its users' passwords and consequently the security of the personal data processed in the email system. In the absence of multi factor authentication, VIEC ought to have implemented measures to ensure that all passwords expired after a period of time.

96. Although there are more secure means of doing so than through an email system, processing of health data by email is sometimes necessary for the efficient operation and management of nursing homes and to ensure provision of a sufficient level of care to patients. However, I consider that it is not necessary for unencrypted biometric data to be processed on VIEC email systems for the purposes of same. As such, an unnecessary risk was taken with the biometric data of patients.

97. I find that an appropriate level of security must also include a policy that mandates password protection for sensitive personal data transmitted by email. In VIEC's Management of Personal Data in line with Data Protection Requirements (incorporating GDPR), I note that reference is made to the fact that "*Transmission of personal data over external networks, such as the internet, should normally be subject to robust encryption (DPC, 2018g).*" However, there does not appear to have been any measures taken to achieve this aim.

98. I note in VIEC's submissions of 30 September 2021 that since the breach training has been provided on the use of shared drive links rather than the use of email attachments for the sharing of personal data and further training has been required on password protection of documents if necessary. The precise details of the policy mandating password protection, and any justifiable exceptions contained within that policy, must be informed by VIEC's risk assessment and its own functions. Therefore, when determining whether the appropriate level of security allows for certain exceptions to this policy, it is appropriate for VIEC to have regard to the need for its staff to urgently exchange information to protect the rights and freedoms of residents in some instances.

99. Regular testing of these measures would have gone some way to ensuring uptake and efficacy of same, however there was no evidence of such measures being employed. Therefore, I consider that the technical measures in place at the time of the breach did not meet the standard required by Articles 5(1)(f) and Article 32 GDPR.

ii. <u>Organisational Measures</u>

100. VIEC outlined organisational measures that were in place at the time of the breach, which included:

- Monitoring of risky sign ins;

- Managed antivirus installed on all workstations and servers;
- SonicWALL firewall scans that only allow certain traffic;
- Role based accounts
- Advanced Threat Protection enabled on inbound mail since 2 November 2018[56]

101. VIEC stated that while multi-factor authentication, conditional access, and mobile device management had been agreed for its sites, it had not been implemented due to Covid-19 restrictions.[57]

102. VIEC confirmed that there was no journaling in place for emails at the time of the breach and therefore it was unable to search for the original phishing email. VIEC used the tool Message Trace to review emails sent and received over the previous 90 days, however the original phishing email could not be located. Although default email settings for Microsoft 365 only stores log files for 90 days, system administrators may increase the mailbox's AuditLogAgeLimit value and retain log records for longer than the 90 day period.[58]

103. VIEC had organisational measures in place to ensure the accuracy and security of customers' personal data. However, the failure to implement multi-factor authentication, conditional access and mobile device management greatly increased the possibility of a data breach occurring as the result of a phishing attack. Similarly, the failure to ensure journaling of emails rendered the discovery of the scope of the breach and the identity of the party behind the phishing attack much more difficult. Again, in circumstances where the data being processed gave rise to a high risk to the data subjects, it was appropriate to implement 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*.

c) Processes to Test, Assess and Evaluate Effectiveness of Measures

104. The severity of the risk to the rights and freedoms of natural persons occurred due to VIEC's processing of personal data (including special category data) on its email system. The technical and organisational measures, which VIEC implemented should have been appropriate to the risks arising to the rights and freedoms of those data subjects from such processing of their personal data. As VIEC was processing special category data and there was a high risk to the rights and freedoms of the individuals, it was appropriate to run tests on their technical and organisational measures to test, assess and evaluate the effectiveness of the measures implemented, pursuant to Article 32(1)(d) GDPR.

(a) Testing Data Protection Governance

---

56 Appendix C.1d Response to Commission Queries 8 Oct 2020 page 4
57 Appendix C.2a VIEC Submission 6 April 2021 Response page 14
58 Appendix C.8.a Fireshot copy of Microsoft 365 mailbox auditing webpage

105. Creating policies and procedures is essential to implementing an appropriate level of security. However, policies and procedures alone are not sufficient to mitigate the risk to data subjects. Where staff store, transfer and process personal and special category data, there is an obligation on a controller to regularly assess and evaluate the effectiveness of measures in place and therefore, there must be an ongoing and verifiable oversight of how the staff members give effect to the controller's policies and procedures.

(b) Effectiveness of Training and Awareness

106. VIEC reflects the importance of training and awareness in its own policies and procedures. However, considering the high risk of the processing activities VIEC engages in, training needs to be frequent, regular and detailed. Training should also be informed by the risks arising from the processing activities, as outlined in risk assessments and should be regularly updated as the risk landscape changes.

(c) Testing Security of Personal Data

(i) Technical Measures

107. An appropriate level of security includes **technical measures** that have, *inter alia*, 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 enforce VIEC's password cycling policy and that failure to comply with the policy of transferring data by way of links to internal databases rather than by way of email attachment, introduced a risk of allowing unauthorised access to resident data. VIEC could have taken steps to monitor compliance with these measures on an ongoing basis and ensure uniform application as appropriate.

(ii) Organisational Measures

108. Article 32(1)(d) GDPR specifies 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) and Article 5(1)(f) GDPR, controllers must take the initiative to test, assess, and evaluate their organisational and technical security measures.

109. VIEC was aware that the use of its email system for the storage and transfer of personal and special category data may present risks to the integrity of the data. This is shown in its development of policies to avoid and minimise this risk. However, no follow up action was taken to ensure that these policies were being followed or were effective. This indicates that VIEC was not carrying out appropriate testing of organisational measures as such weaknesses or gaps in its organisational measures were not identified until VIEC became aware of the breach. Therefore, I consider that the organisational security measures in place at the time of the breach did not meet the standard required by Article 5(1)(f) and 32(1) GDPR and that these Articles were infringed.

H. Findings

110. I consider that the root cause of the personal data breach was that a phishing attack was carried out on VIEC's email system and that emails were rerouted to a third party email account The processing by VIEC failed to ensure that the personal *data was 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*. The processing by the author of the phishing attack was **unauthorised and unlawful.** The processing by VIEC itself of personal and special category data on its email system prior to the phishing attack, without adequate security measures, placed such data at risk of being unlawfully accessed.

111. While I do not wish to be prescriptive, adequate technical and organisational measures that may have been employed by VIEC could have included, among others, appropriate encryption of personal data being transferred over external networks, and provision of suitable phishing training. Regular testing of the measures employed would also go some way to ensuring the security of processing. In the absence of suitable measures and for the reasons set out above, I find that VIEC infringed Articles 5(1)(f) and 32(1) GDPR by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its processing of personal data within the VIEC email system.

I. Decision on Corrective Powers

112. I have set out above, pursuant to section 111(1)(a) of the 2018 Act, my decision to the effect that VIEC has infringed Articles 5(1)(f) and 32(1) GDPR.

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

114. 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…*

115. Having carefully considered the infringements identified in this Decision, I have 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 I have decided are appropriate to address the infringements in the particular circumstances are.

    a. An order pursuant to Article 58(2)(d) GDPR to VIEC to bring its processing operations into compliance with the GDPR in the manner specified below;

b. A reprimand to VIEC pursuant to Article 58(2)(b) GDPR; and

c. An administrative fine of €100,000 in respect of the infringement of Article 5(1)(f) pursuant to Article 58(2)(i) and Article 83 GDPR.

116. I set out further detail below in respect of each of these corrective powers that I will exercise and the reasons why I have decided to exercise them.

J. Order to Bring Processing into Compliance

117. 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*

118. In circumstances where I have found that the processing at issue was not in compliance with the GDPR, I make an order pursuant to Article 58(2)(d) GDPR. Therefore, I order VIEC to bring the relevant processing into compliance with Article 5(1)(f) and 32(1) GDPR in the terms set out in the table below through implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risks.

119. It is my view, these orders are appropriate, necessary and proportionate in view of ensuring compliance with Articles 5(1)(f) and 32(1) GDPR. In this regard, I acknowledge VIEC's on-going remedial actions, as outlined in submissions throughout the Inquiry.

120. The order I am imposing is set out in the following table:

Number	Issue and Action	Timescale
1.	Articles 5(1)(f) and 32(1) GDPR Lack of robust data protection policies, procedures and necessary audits to ensure compliance. I order that VIEC implement quality oversight controls to monitor whether staff are using encryption when sending sensitive documents where it is appropriate to do so.	VIEC is required to confirm to the DPC within 90 days of receipt of this Decision that this order has been complied with.

121. My decision to impose the order is made to ensure that full effect is given to VIEC's obligations under Articles 5(1)(f) and 32(1) GDPR. I consider that this order is appropriate, necessary and proportionate in view of ensuring compliance with the GDPR.

122. I consider that this order is necessary to ensure that full effect is given to VIEC'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 VIEC.

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

124. Having regard to the non-compliance in this Decision, in my view, such an order is proportionate and is the minimum order required in order to guarantee that compliance will take place in the future. I am satisfied that the order is a necessary and proportionate action.

125. I therefore require VIEC to comply with the above order within the time specified from the date of notification of any final decision. Further to this, I require VIEC to submit a report to the DPC within a further month detailing the actions it has taken to comply with the order.

K. Reprimand

126. 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*

127. I issue VIEC with a reprimand in respect of its infringements of Article 5(1)(f) and Article 32(1) GDPR identified in this Decision. The purpose of the reprimand is to dissuade non-compliance with the GDPR. The infringements resulted in the unauthorised disclosure of residents' personal and special category data along with employee personal data, and in the late notification of the breach to the DPC. Reprimands are appropriate in respect of such non-compliance in order to formally recognise the serious nature of the infringements and to dissuade such non-compliance. The reprimand is necessary and proportionate in addition to the order imposed in this Decision . While the order would require specific remedial action on the part of VIEC, the reprimand formally recognises the serious nature of these infringements. I consider that it is appropriate to formally recognise the serious nature of the infringements with a reprimand in order to deter future similar non-compliance by VIEC and other controllers or processors carrying out similar processing operations. By formally recognising the serious nature of the infringements, the reprimand will contribute to ensuring that VIEC and other controllers and processors take appropriate steps in relation to current and future processing operations in order to comply with their obligations with regard to the security of personal data.

L. Administrative Fine

128. 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*

129. This makes it clear that the DPC may impose administrative fines in addition to, or instead of, the order and reprimand also imposed in this Decision. Section 115 of the 2018 Act mirrors this

by providing that the DPC may do either or both of imposing an administrative fine and exercising any other corrective power specified in Article 58(2) GDPR.

130. Article 83(2) GDPR provides that when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case, due regard shall be given to the following:

> *(a) the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;*
>
> *(b) the intentional or negligent character of the infringement;*
>
> *(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;*
>
> *(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;*
>
> *(e) any relevant previous infringements by the controller or processor;*
>
> *(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;*
>
> *(g) the categories of personal data affected by the infringement;*
>
> *(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;*
>
> *(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;*
>
> *(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and*
>
> *(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.*

131. The decision as to whether to impose an administrative fine in respect of an infringement is a cumulative decision which is taken having had regard to all of the factors as set out in Article 83(2)(a) to (k) GDPR. Therefore, I will now proceed to consider each of these factors in turn in respect of the infringement of Article 5(1)(f) identified in this Decision.

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;

132. In considering the nature, gravity and duration of VIEC's infringement, I have had regard to the analysis in Part G of this Decision concerning the nature, scope, context and purposes of the processing. Article 83(2)(a) GDPR requires that I take these matters into account in having regard to the nature, gravity and duration of the infringement. Article 83(2)(a) GDPR also requires me to take into account the number of data subjects affected by the infringement and the level of damage suffered by them. Therefore, I will first consider these issues before proceeding to consider the nature, gravity and duration of the infringement.

133. 213 individuals were affected by the personal data breach considered in this Decision through having their data accessed by the third party gaining access to the information stored on that manager email account and potentially disclosed to unauthorised people through the email forwarding rule established. As noted above, 129 residents had special category personal data compromised. Furthermore, a number of VIEC employees were affected by the disclosure data relating to probation reviews. The DPC did not receive submissions as to how many residents and employees VIEC has, however all of these residents and employees may have potentially been affected in that the failure to have appropriate technical and organisational measures in place could have resulted in any resident's or employee's personal data being erroneously disclosed to unauthorised people.

134. The failure to implement appropriate technical and organisational measures contributed to a situation where sensitive data of multiple data subjects was rendered extremely vulnerable to unauthorised access. The fact that such unauthorised access occurred in this case as a result of the data breach was contributed to by the failure of the controller to implement appropriate technical and organisational measures.

The nature of the infringement

135. The nature of VIEC's infringement of Article 5(1)(f) concerns its failure to implement appropriate measures designed to implement data protection principles in an effective manner; and to integrate appropriate technical and organisational measures to ensure that personal and special category data are not made accessible to unauthorised natural persons. Having regard to the nature and scope of the data processing, I consider that this failure to implement appropriate measures by VIEC to be serious.

The gravity of the infringement

136. In assessing the gravity of the infringement, I have had regard to the number of data subjects affected and the level of damage suffered by them. While the breaches affected 213 data subjects, other data subjects were at potential risk due to the use of the email system as a means to share and store personal data that related to both residents and staff. I have also had regard to how the infringement increased the risks posed by the processing to the rights and freedoms of data subjects. These risks include the risk of unauthorised access and unauthorised disclosure of personal data to third parties of personal data processed within the email system.

137. In those circumstances, I find that the gravity of VIEC's failure to ensure technical and organisational measures sufficient to ensure the security of its processing of personal data is serious.

The duration of the infringement

138. The duration of VIEC's infringement of Article 5(1)(f) regarding the processing commenced at the application of the GDPR on 25 May 2018. The obligation to implement the appropriate organisational and technical measures required by these Articles applied from 25 May 2018. The infringement was ongoing from the application of the GDPR until the commencement of this inquiry (the '**temporal scope**'). 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 under Article 5(1)(f) lasted at least from 25 May 2018 until 8 March 2021.

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

139. In assessing the character of the infringement, I note that the GDPR does not identify the factors that need to be present in order for an infringement to be classified as either 'intentional' or 'negligent'. The WP29 considered this in its 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679' (the '**Administrative Fines Guidelines'**) as follows:

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

140. The Guidelines proceed to detail how supervisory authorities should determine whether wilfulness or negligence was present in a particular case:

> *The relevant conclusions about wilfulness or negligence will be drawn on the basis of identifying objective elements of conduct gathered from the facts of the case*.

141. In determining whether an infringement was intentional, I must determine whether the objective elements of conduct demonstrate both knowledge and wilfulness in respect of the characteristics of the infringement at the time under consideration.

142. In determining whether an infringement was negligent, I must determine whether, despite there being no knowledge and wilfulness in respect of the characteristics of the infringement, the objective elements of conduct demonstrate that the controller ought to have been aware in the circumstances that it was falling short of the duty owed at the time under consideration.

143. VIEC's infringement of Article 5(1)(f) GDPR regarding the processing, concerns its failure to implement appropriate measures to implement data protection principles in an effective

manner and to integrate the necessary safeguards into the processing. Hence, the characteristics of this infringement concerns that lack of appropriate technical and organisational measures for the duration of the infringement. In order to classify the infringement as intentional, I must be satisfied that (i) VIEC wilfully omitted to implement appropriate technical and organisational measures and (ii) that it knew at the time that the measures that it implemented were not sufficient to meet the standards required by Article 5(1)(f) GDPR. Having considered the objective elements of VIEC's conduct, I do not consider that VIEC wilfully omitted to implement appropriate measures. While VIEC's attempts to implement appropriate measures were not sufficient for the purposes of Articles 5(1)(f) GDPR, I do not consider that this failure was wilful on VIEC's part. However, it is clear that VIEC ought to have been aware that it was falling short of the duty owed under Articles 5(1)(f) GDPR. I find that VIEC's failure to implement appropriate measures pursuant to Articles 5(1)(f) GDPR in respect of its processing was negligent in the circumstances.

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

144. VIEC put in place additional measures after it discovered the data breaches. Once appropriate measures were fully implemented, recurrence of similar breaches was prevented. These measures included the use of new data protection software, the nomination of data protection champions and the appointment of a Quality and Risk Manager. Furthermore, conditional access for all email, multi-factor authentication, and a mobile device policy were implemented by VIEC. Finally, HSEland "good information practices" training and Security Awareness Training quarterly for staff with access to an email account were introduced. I have had regard to these implemented measures as a form of mitigation.[59] However, it is not always possible to retrospectively correct a past lack of control, as personal data had already been breached and data subjects may already have suffered consequential damage as a result.

145. I note that the above actions by VIEC may have reduced the probability of further breaches causing additional risk of damage to data subjects after the infringement occurred for the purpose of Article 83(2)(c) GDPR. In its Submissions in relation to the Draft Decision, VIEC requested the additional measures it implemented which prevented the recurrence of similar breaches be taken into consideration in relation to any administrative fine to be made.[60] Having regard to these actions for the purpose of Article 83(2)(c) GDPR, I am of the view that the actions provided limited mitigation of the damage the data subjects suffered in relation to the breach. As these measures solely prevented the occurrence of further, similar breaches, I can only consider that the actions are of low to moderate mitigating value.

[59] Appendix C.4.c

[60] Appendix C.7.a page 2

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 GDPR;

146. As outlined above, VIEC infringed Article 5(1)(f) GDPR by failing to implement appropriate technical and organisational measures regarding its processing of personal and special category data on its email system.

147. I consider that VIEC holds a high degree of responsibility for this infringement and that the absence of sufficiently robust technical and organisational measures must be deterred. However, in circumstances where this factor forms the basis for the finding of the infringement of Article 5(1)(f) GDPR against VIEC, this factor cannot be considered aggravating in respect of the infringement.

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

148. No relevant previous infringements arise for consideration in this context.

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;

149. I consider that VIEC cooperated fully with the DPC to remedy the infringement and to mitigate their adverse effects. In its breach notifications and during the Inquiry, it illustrated the steps that it had taken and was in the course of taking to remedy the infringement and the possible adverse effects. In its Submissions in relation to the Draft Decision, VIEC requested that I have regard to this prior cooperation when considering the amount of a potential administrative fine.[61] As per the draft decision, I have had regard to VIEC'S cooperation with the DPC when calculating the proposed administrative fine below. However, I consider that I can only attach minimal mitigation effect to this compliance in circumstances where this compliance is a statutory requirement under Article 31 GDPR.

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

150. The personal data affected by the infringement included financial data and special category data concerning health. It also concerned the personal data of residents of nursing homes, who may be more vulnerable to the risk of fraud arising from unauthorised access to their data. This represents a high risk to the rights and freedoms of the affected data subjects. I find that the sensitivity of these categories of personal data aggravates the infringement of Articles 5(1)(f) in circumstances where the personal data rerouted to an external email account was subject to unauthorised processing.

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;

---

[61] Ibid

151. VIEC became aware of the breach on 15 August 2020 and took immediate steps to engage Ortis to investigate the issue. Ortis informed VIEC of the forwarding issue on 15 August 2020, but the VIEC DPO was not informed until 19 August 2020. The DPC received notification of a personal data breach from VIEC on 19 August 2020. Controllers are obliged to notify personal data breaches to the DPC without undue delay and, where feasible, not later than 72 hours after having become aware of it.

152. In its Submissions in relation to the Draft Decision, VIEC stated that "*VIEC reported the matter to the DPC in line with its responsibilities on the 19th of August 2020*."[62]

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

> *"The controller has an obligation according to the Regulation to notify the supervisory authority about personal data breaches. Where the controller merely fulfils this obligation, compliance with the obligation cannot be interpreted as an attenuating/mitigating factor."*[63]

154. In the above circumstances, I cannot consider VIEC's notification of the breach in compliance with its duty to do so under Article 33 GDPR to be of mitigating value when calculating any administrative fine.

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

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

156. In its submissions in relation to the Draft Decision, VIEC submitted that I have due regard to the lack of corrective measures exercised against VIEC in this regard when calculating the administrative fine.[64]

157. However, the Administrative Fines Guidelines consider the relevance of such notifications regarding administrative fines.

> *The absence of any previous infringements, however, cannot be considered a mitigating factor, as compliance with the GDPR is the norm. If there are no previous infringements, this factor can be regarded as neutral*

158. In the above circumstances, I cannot consider the absence of corrective measures exercised against VIEC to be of mitigating value when calculating any administrative fine

---

62 Appendix C.7.a page 1

63 Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines, page 15

64 Appendix C.7.a page 2

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

159. Such considerations do not arise in this case.

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.

160. I am of the view that there are no other aggravating or mitigating factors in respect of the infringement of Article 5(1)(f)GDPR.

M. Decisions on Whether to Impose Administrative Fines

161. In deciding whether to impose an administrative fine in respect of the infringement of Article 5(1)(f) GDPR, I have had regard to the factors outlined in Article 83(2)(a) – (k) GDPR cumulatively, as set out above. However, I have considered each infringement separately when applying those factors, when deciding whether to impose an administrative fine and the quantum of same. I have also had regard to the effect of the order and reprimand imposed in ensuring compliance with the GDPR. The order will assist in ensuring compliance by mandating specific action on the part of VIEC in order to re-establish compliance with specific findings of infringements. The reprimand will contribute towards dissuading future non-compliance by formally recognising the serious nature of the infringements. However, I consider that these measures alone are not sufficient in the circumstances to ensure compliance. I find that an administrative fine would be appropriate, necessary and proportionate in view of ensuring compliance with the GDPR.

162. 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.*

163. While the order imposed in this Decision will re-establish compliance with the specific infringements identified, I do not consider this measure appropriate to deter other future serious infringements. While the reprimand will assist in dissuading VIEC and other entities from similar future non-compliance, in light of the seriousness of the infringement of Article 5(1)(f), I do not consider that the reprimand alone is proportionate or effective to achieve this end. I find that an administrative fine is necessary to deter other future serious non-compliance on the part of VIEC and other controllers or processors carrying out similar processing operations.

(1) The infringement of Article 5(1)(f) 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. I consider that VIEC'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, I consider that an administrative fine is appropriate and necessary in order to dissuade non-compliance.

(2) Having regard to the nature, gravity and duration of the infringement of Article 5(1)(f), I also consider that an administrative fine is proportionate in the circumstances in view of ensuring compliance. The higher risks incurred by the data subjects as a result of VIEC's infringement of Articles 5(1)(f) likely contributed to data breaches which affected 213 data subjects in this breach and where all residents and staff were at potential risk. I consider that the unauthorised access to special category health data constitutes significant damage in the circumstances. In light of this damage, I consider that a fine is proportionate to responding to VIEC's infringement of Article 5(1)(f) with a view to ensuring future compliance. I consider that the fine does not exceed what is necessary to enforce compliance in respect of the infringement of Article 5(1)(f) identified in this Decision.

(3) I consider that the negligent character of VIEC's infringement of Article 5(1)(f) GDPR carries weight when considering whether to impose an administrative fine, and if so, the amount of the fine. This negligence suggests that an administrative fine is necessary to effectively ensure that VIEC directs sufficient attention to its obligations under Article 5(1)(f) GDPR in the future.

(4) I consider that an administrative fine would help to ensure that VIEC 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. In these particular circumstances where the categories of user's data affected by VIEC's infringement carry a risk with regard to the fundamental rights and freedoms of data subjects, in particular where special category data is put at risk.

(5) I have also had regard to the actions taken by VIEC in order to minimise further breaches (as assessed above pursuant to Articles 83(2)(c) and (f) GDPR). I consider that these factors mitigated the damage to data subjects to an extent, and remedied the infringement to an extent. I have therefore taken these mitigating actions into account

when calculating the administrative fine. However, despite these factors, I consider that an administrative fine is appropriate, necessary and proportionate in respect of each infringement in order to ensure compliance with the GDPR. While the lack of previous relevant infringements is a mitigating factor, I consider that the need to dissuade non-compliance of this nature far outweighs the mitigation applied for this factor. Furthermore, despite the actions taken to mitigate against further breaches, the damage suffered has not been significantly mitigated for the affected data subjects. In light of the negligent character of the infringement, and VIEC's failure to comply with its obligations with regard to data protection, I consider that a dissuasive administrative fine is necessary in the circumstances to ensure future compliance.

164. Based on the analysis I have set out above, I impose a fine of €100,000 in respect of VIEC's infringement of Article 5(1)(f).

165. In having determined the quantum of the fine, I have taken account of the requirement, set out in Article 83(1) GDPR, for a fine imposed to be *effective, proportionate and dissuasive* in each individual case. I am satisfied that the fine specified above, if imposed on VIEC, would be effective, proportionate and dissuasive, taking into account all of the circumstances covered by the Inquiry.

166. In order for a fine to be *dissuasive*, it must dissuade both the controller/processor concerned, as well as other controllers and processors carrying out similar processing operations, from repeating the conduct concerned.

167. As regards the requirement for any fine to be *proportionate*, this requires me to adjust the quantum of any fines to the minimum amount necessary to achieve the objectives pursued by the GDPR. I am satisfied that the fine imposed above does not exceed what is necessary to enforce compliance with the GDPR taking into account the number of data subjects using VIEC services, the loss of control over personal and health data suffered by the data subjects, and how the infringement increased the risks posed by the processing to the rights and freedoms of the data subjects.

168. The amount of the administrative fine I have chosen to impose is at the bottom point of the scale proposed in the Draft Decision and I have given due regard to the totality of VIEC's submissions in determining this to be the appropriate amount.

169. I am satisfied that the fine specified above, if imposed on VIEC, would be effective, proportionate and dissuasive, taking into account all of the circumstances covered by the Inquiry.

Article 83(3) GDPR

170. Article 83(3) GDPR provides that:

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

171. I am imposing an administrative fine for VIEC's infringement of Article 5(1)(f). This infringement itself is the gravest infringement and I am acting in accordance with Article 83(3) in imposing this fine.

Article 83(5) GDPR

172. Turning, finally, to Articles 83(5) GDPR, I note that this provision operates to limit the maximum amount of any fine that may be imposed in respect of certain types of infringement.

173. Article 83(5) GDPR provides that:

> *Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:*
>
> > *(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;*

174. In order to determine the applicable fining 'cap', it is firstly necessary to consider whether or not the fine is to be imposed on *'an undertaking'*. Recital 150 clarifies, in this regard, that:

> *Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes.*[65]

175. Accordingly, when considering a respondent's status as an undertaking, the GDPR requires me to do so by reference to the concept of *'undertaking'*, as that term is understood in a competition law context. In this regard, the Court of Justice of the European Union ('**the CJEU**') has established that:

> *"an undertaking encompasses every entity engaged in an economic activity regardless of the legal status of the entity and the way in which it is financed"*[66]

176. The CJEU has held that a number of different enterprises could together comprise a single economic unit where one of those enterprises is able to exercise decisive influence over the behaviour of the others on the market. Such decisive influence may arise, for example, in the context of a parent company and its wholly owned subsidiary. Where an entity (such as a subsidiary) does not independently decide upon its own conduct on the market, but carries out, in all material respects, the instructions given to it by another entity (such as a parent), this means that both entities constitute a single economic unit and a single undertaking for the purpose of Articles 101 and 102 TFEU. The ability, on the part of the parent company, to exercise decisive influence over the subsidiary's behaviour on the market, means that the

---

65 Treaty on the Functioning of the European Union

66 *Höfner and Elser v Macrotron GmbH* (Case C-41/90, judgment delivered 23 April 1991), EU:C:1991:161, paragraph 21.

conduct of the subsidiary may be imputed to the parent company, without having to establish the personal involvement of the parent company in the infringement.[67]

177. In the context of Article 83 GDPR, the concept of 'undertaking' means that, where there is another entity that is in a position to exercise decisive influence over the controller/processor's behaviour on the market, then they will together constitute a single economic entity and a single undertaking. Accordingly, the relevant fining 'cap' will be calculated by reference to the turnover of the undertaking as a whole, rather than the turnover of the controller or processor concerned.

178. In order to ascertain whether a subsidiary determines its conduct on the market independently, account must be taken of all the relevant factors relating to the economic, organisational and legal links, which tie the subsidiary to the parent company, which may vary from case to case.[68]

179. The CJEU has, however, established[69] that, where a parent company has a 100% shareholding in a subsidiary, it follows that: the parent company is able to exercise decisive influence over the conduct of the subsidiary; and a rebuttable presumption arises that the parent company does in fact exercise a decisive influence over the conduct of its subsidiary.

180. The CJEU has also established that, in a case where a company holds all or almost all of the capital of an intermediate company which, in turn, holds all or almost all of the capital of a subsidiary of its group, there is also a rebuttable presumption that that company exercises a decisive influence over the conduct of the intermediate company and indirectly, via that company, also over the conduct of that subsidiary.[70]

181. The General Court has further held that, in effect, the presumption may be applied in any case where the parent company is in a similar situation to that of a sole owner as regards its power to exercise decisive influence over the conduct of its subsidiary[71]. This reflects the position that:

> *"… the presumption of actual exercise of decisive influence is based, in essence, on the premise that the fact that a parent company holds all or virtually all the share capital of its subsidiary enables the Commission to conclude, without supporting evidence, that that parent company has the power to exercise a decisive influence over the subsidiary without there being any need to take into account the interests of other shareholders when adopting strategic decisions or in the day-to-day business of that subsidiary, which does*

---

67 Akzo Nobel and Others v Commission, (Case C-97/08 P, judgment delivered 10 September 2009) EU:C:2009:536, paragraphs 58 – 60.

68 Ori Martin and SLM v Commission (C-490/15 P, judgment delivered 14 September 2016) ECLI:EU:C:2016:678, paragraph 60.

69 Akzo Nobel and Others v Commission, (C-97/08 P, judgment delivered 10 September 2009).

70 Judgment of 8 May 2013, Eni v Commission, Case C-508/11 P, EU:C:2013:289, paragraph 48.

71 Judgments of 7 June 2011, Total and Elf Aquitaine v Commission, T-206/06, not published, EU:T:2011:250, paragraph 56; of 12 December 2014, Repsol Lubricantes y Especialidades and Others v Commission, T-562/08, not published, EU:T:2014:1078, paragraph 42; and of 15 July 2015, Socitrel and Companhia Previdente v Commission, T-413/10 and T-414/10, EU:T:2015:500, paragraph 204.

not determine its own market conduct independently, but in accordance with the wishes of that parent company …"[72]

182. Where the presumption of decisive influence has been raised, it may be rebutted by the production of sufficient evidence that shows, by reference to the economic, organisational and legal links between the two entities, that the subsidiary acts independently on the market.

183. It is important to note that 'decisive influence', in this context, refers to the ability of a parent company to influence, directly or indirectly, the way in which its subsidiary organises its affairs, in a corporate sense, for example, in relation to its day-to-day business or the adoption of strategic decisions. While this could include, for example, the ability to direct a subsidiary to comply with all applicable laws, including the GDPR, in a general sense, it does not require the parent to have the ability to determine the purposes and means of the processing of personal data by its subsidiary.

184. In VIEC's draft accounts for the year ended 2021, it is stated that in relation to the 14 companies coming under the parent company of VIEC Limited "the controlling interest of the company is held by Bidco Emera SAS controlling a 70% interest in the parent company".[73] I find Bidco Emera SAS exercises a decisive influence over VIEC's affairs in light of its controlling interest, I therefore must take this turnover into account in determining what the fining cap is.

185. VIEC had a reported total turnover of €62,293,583 for the year ended 31 December 2021.[74] VIEC's ultimate holding company, Bidco Emera SAS, had a reported total turnover of €9,915,000 for the year ended 2021.[75] The sum of these two figures taken cumulatively is €72,208,583 and I calculate the administrative fine on this basis. I note the fine imposed is less than 4% of €72,208,583.

---

[72] Opinion of Advocate General Kokott in Akzo Nobel and Others v Commission, C-97/08 P, EU:C:2009:262, point 73 (as cited in judgment of 12 July 2018, The Goldman Sachs Group, Inc. v European Commission, Case T-419/14, ECLI:EU:T:2018:445, paragraph 51).

[73] Appendix C.5.b (SRCW Ltd, FFNH Ltd, Birdhaven Nursing Home Ltd, Benkai Consulting Ltd, Independent Home Care Ltd, VIEC Mgmt Ltd, Signa Care Waterford Ltd, Signa Care New Ross Ltd, SignaCare Killerig Ltd, Signa Care Bunclody Ltd, Glenageary Nursing Home Ltd, Moorehall Living Ltd, Moorehall Homecare Ltd, Moorehall Healthcare (Drogheda) Ltd)

[74] Appendix C.5.b

[75] https://www.infogreffe.fr/entreprise-societe/852683598-bidco-emera-060220B002630000.html?typeProduitOnglet=EXTRAIT&afficherretour=true

N. Summary of Envisaged Action

186. In summary, the corrective powers that I exercise are:

(1) An order pursuant to Article 58(2)(d) GDPR to VIEC to bring its processing into compliance with the GDPR in the manner specified in this Decision. This must be done within 90 days of the date of notification of this decision;

(2) A reprimand to VIEC pursuant to Article 58(2)(b) GDPR regarding the infringements identified in this Decision; and

(3) One administrative fine In respect of VIEC's infringement of Article 5(1)(f) GDPR of €100,000.

O. Right of Appeal

187. This Decision is issued in accordance with section 111 of the 2018 Act. Pursuant to section 150(5) of the 2018 Act, VIEC has the right to appeal against this Decision within 28 days from the date on which notice of the Decision is received by it. Furthermore, pursuant to section 142 of the 2018 Act, as this Decision imposes an administrative fine, VIEC also has the right to appeal under this section within 28 days from the date on which notice of this Decision is given to it.