In the matter of the General Data Protection Regulation

DPC Case Reference: IN-21-2-4

In the matter of Centric Health 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

23 January 2023

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'**) 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. Centric Health Ltd ('**Centric**') was provided with the Draft Decision ('**the Draft Decision**') on 11 October 2022 to give it the final opportunity to make any further submissions. Centric made submissions on the draft decision on 31 October 2022. This Decision is being provided to Centric pursuant to section 116(1)(a) of the 2018 Act in order to give Centric 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. It should be noted, in this regard, that Centric will be required to comply with any corrective powers that are contained in the (final) Decision, and it is open to this office to serve an enforcement notice on Centric 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 Centric might be the controller, within the meaning of Article 4(7) of the GDPR, in respect of personal data that was the subject of the personal data breach notification. In this regard, Centric confirmed that it was the controller in its notification of the personal data breach to the DPC on 5 December 2019.

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 that 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 Centric made in respect of the Draft Decision on 31 October 2022 before proceeding to make this final Decision under Section 111 of the 2018 Act.

C. Factual Background

10. Centric provides Primary Healthcare General Practitioner ('**GP**') and dental services, specialist care and occupational services to over 400,000 patients across Ireland. It has over 500 staff and is headquartered in Balally, Dublin 16.[1]

11. The DPC received a personal data breach notification from Centric on 5 December 2019 related to the patient data of [redacted] GP practices in seven clinics in County Kildare and County Dublin. The data breach notification concerned a ransomware attack, which resulted in unauthorised access, alteration, and destruction of personal data. This attack led to the permanent deletion of some of that personal data.

12. In the breach notification form, Centric advised that staff reported their inability to access the Patient Administration System on 3 December 2019. An investigation by Centric's IT on that day discovered malware on the system, which had encrypted patient data and requested payment for return of the data files. [2]

13. The categories of patient data affected included name, date of birth, PPSN and contact details. The personal data records of some 70,000 patients were affected.[3] The nature of the personal data encompasses clinical data, which is special category health data.

14. Data on the system was backed up nightly and a snapshot of data was taken each day, but these back-ups were also affected by the malware. Data was partially restored from other backups, but a [redacted] period was identified between [redacted]

1 Centrichealth.ie – accessed on 19 Mar 2021 at 14:00
2 C.1.1
3 C.1.1

where data generated was irretrievably deleted. A forensic consultants firm was engaged to assist with the data recovery.

15. The external forensic analysts ('**Forensic Analysts**') formed the view that patient data generated between [redacted] was deleted, with the personal data records of approximately 2,500 patients affected. Centric stated that:

> *"These data subjects consist for the most part of patients who visited one of our clinics between [redacted]."* [4]

16. Centric had begun, on 9 December 2019, to contact the affected data subjects. In addition, Centric placed notices in its clinics and alerts in patient appointment texts. Centric informed the HSE and the Garda National Cyber Crime Bureau about the incident.

17. Centric outlined that the incident affected legacy Primacare systems under the control of Centric Health. Primacare Health Professionals CLG is a subsidiary of Centric Health, which was acquired in August 2016.[5]

18. The legacy Primacare systems were in the process of being phased out when the Incident occurred. The seven clinics (that hosted eleven GP practices) affected by the incident were all former Primacare clinics.

19. Centric noted the efforts made to restore the affected data from backups:

> *"A representative of the Forensic Analysts attended Centric's offices on Friday, 6 December 2019 to take a copy of the operating systems of the affected servers. This copying occurred concurrently with a member of Centric's IT team performing a backup of the Affected Data, in order that it would be transferred to a 'clean' system to be decrypted.*
>
> *"It was discovered during the course of the attempted backup that the server containing the Practice Management system database no longer existed."*[6]

20. In relation to its backup of data, Centric explained that:

> *"The locally stored backups of the affected systems were affected by the malware. However, backups of patient data up to [redacted] were available through cloud storage. As a result, the Affected Data – effectively backups of patient data generated between [redacted] are not available. The available backup of the Affected Data was restored to a separate server environment and this process was completed during the evening of Wednesday, 4 December 2019."*[7]

4 C.1.4
5 C.1.7
6 C.1.7 page 5
7 C.1.7 pages 5-6

21. Centric made further efforts to recover the data, but ultimately its investigations determined that:

> *"…approximately 2,500 data subjects were materially affected by the Incident as a result of the loss of availability of personal data obtained during the course of clinical appointments with their doctors and nurses."*[8]

22. Meanwhile, between 3 and 6 December 2019, Centric was in contact with the bad actors who had provided contact details in a ransom note.[9] Centric subsequently paid the ransom in return for a decryptor key. Centric established that the key did not pose any threat, but that:

> *"…the decryptor could not be applied to the Affected Data as it had been deleted in the interim."*

23. Centric provided the DPC with copies of the communications issued to affected data subjects as a result of the incident and its notification to the HSE.[10] In its communication to the data subjects, Centric stated that:

> *"We have no evidence that your patient data has been moved off site or accessed by a third party."*

This statement is incorrect. While it may be the case that there was no evidence that data was disclosed to a third party, any data that was encrypted in the ransomware attack was, by definition, accessed.

24. As noted above, Centric originally stated that 70,000 data subjects were impacted by the breach in the initial breach notification. However, communications were only issued to the 2,500 data subjects who suffered irretrievable loss of their personal data. Article 34(1) GDPR requires that a controller shall communicate a data breach to the affected data subjects without undue delay where the breach

> *is likely to result in a high risk to the rights and freedoms of natural person*

25. The malware that affected Centric's system was 'Calum' ransomware.[11]

---

8 C.1.7 page 6

9 C.1.8 and C.1.9

10 C.1.10 to C.1.13

11 Calum is malicious software belonging to the Phobos ransomware family. Malware under this classification is designed to encrypt data and demand ransom payments for decryption. See also www.pcrisk.com/removal-guides/16425-calum-ransomware

26. Centric provided the DPC with a description of its IT system and infrastructure. Centric stated that:

> *"The system was configured that whilst we did have a firewall present and active, the firewall logs were not enabled. Server security logs were reviewed and did not show anything suspicious.*
>
> *"As an additional measure, bandwidth traffic was also monitored 5 weeks around the Incident and did not show any suspicious traffic leaving the network"* [12]

27. Centric also provided copies of its Data Protection Policy, Record of Processing Activities and ICT Policy that, it stated, were in place at the time of the personal data breach.[13]

28. Centric's response to the DPC of 23 December 2019 indicated that it expected the work of the Forensic Analysts to be completed by the end of January 2020.

29. On 4 February 2020, the DPC requested a copy of the forensic analysis report. [14]

30. On 6 February 2020, Centric responded stating that:

> *"Centric Health engaged the services of independent forensic experts (the "Forensic Analysts") in order to support our response to the breach incident (the "Incident") and to try and identify the root cause of the Incident. To date we have been advised by the Forensic Analysts that there was no evidence found, using the data available, of any data exfiltration. This is consistent with our own internal findings which are also that we have found no evidence of any data exfiltration."*
>
> *"Centric Health also engaged the Forensic Analysts to investigate the issue around the deletion of patient data. However, due to the very nature of the deletion we understand that it is unlikely that it will be possible to conclusively determine the cause. Nevertheless, we will update the DPC in the event that any further material information comes to light."*[15]

31. On 6 February 2020, the DPC requested Centric to clarify if a written report had been compiled by the Forensic Analysts and, if so, to provide a copy to the DPC.[16]

32. On 7 February 2020, Centric responded stating that:

> *"To date we have been advised by the Forensic Analysts that there was no evidence found, using the data available, of any data exfiltration. We have not, however, received a report. As this stage and due to the nature of the deletion which took place*

[12] C.1.7 page 9
[13] C.1.19 to C.1.21
[14] C.1.23
[15] C.1.24
[16] C.1.25

we have not a definitive date of completion. I will keep you and your office updated if any further material information pertaining to this incident arises."[17]

33. On 13 July 2020, the DPC requested supporting information from Centric to demonstrate how the Forensic Analysts had come to the conclusion that there was no exfiltration of data as a result of the personal data breach.[18]

34. On 28 July 2020, Centric responded providing a copy of a forensic analysis report ('**the Forensic Report**')[19] dated 17 July 2020 carried out by a [redacted] firm called [redacted]. The response also contained a further submission from Centric setting out various measures it had put in place subsequent to the personal data breach. [20]

35. The Forensic Report noted that on 6 December 2019, [redacted] had observed that:

> "*The CEN-PRIME Operating system licence was expired*"
> …
> "*The configuration to save logs in Malwarebytes was not enabled. Analysis of the system later highlighted that Malwarebytes version 4.0.4.49 was installed on 03/12/2019 and that the earliest detection from was at 11:55 pm on 3/12/2019, where it had detected evidence of Phobos ransomware*."[21]

36. In relation to the question of exfiltration of data, the Forensic Report stated that it:

> *"…did not identify any evidence of data exfiltration. No evidence of archive files consistent with the attacker compressing large amounts of data for exfiltration were found on any of the systems, but this does not definitively rule it out."*

37. The Forensic Report identified that the configuration of Centric's system at the time of the personal data breach left the network firewall "*fully exposed, allowing all inbound and outbound traffic through*", and ran the Remote Desktop Protocol (RDP) service on the host server that "*was fully exposed to the internet with a password which could have been brute-forced without much difficulty*".[22]

38. The Forensic Report stated that:

> *"There was log file evidence that repeated unsuccessful login attempts were made to [redacted]" account before a successful login occurred.*
> …
> "*Centric Health provided [redacted] with a list of administrator passwords to log into the CEN-PRIME server. These passwords appeared to follow a common organizational*

17 C.1.26
18 C.1.27
19 C.1.29
20 C.1.30
21 C.1.29 page 3
22 C.1.29 page 4

format and would not meet password security standards for internet-facing services."[23]

39. The Forensic Report concluded that:

> "*Conclusions drawn from the above are that "CEN-PRIME" was likely the initial point of infection for this attack. This cannot be definitively proven due to the system restore that took place, which inevitably deleted crucial logging data. However, it can still be determined that encrypted* [sic] *had taken place on this system first. The earliest encrypted files were created on the Hypervisor "CEN-PRIME" at 07:13:27 03/12/2019, whereas the earliest encrypted files identified on the virtual machines was at 09:22:23 03/12/2019, specifically on the system "PC-AS02".*
>
> *Throughout the morning of the 3rd December, there were several unsuccessful attempts to log on to "PC-AS02" using the* [redacted] *user account from the "PC-RS02" system. This indicates a sustained attempt to brute force the account with password guessing.*
>
> *At 09:22:19 03/12/2019, shortly before the files were encrypted on "PC-AS01", an 'anonymous' login occurred from "PC-RS02". There was a remote connection to "PC-RS02" from IP address 192.168.8.79 using the account "gmsuser" at 10:31:01 03/12/2019. Two minutes after this login at 10:33:44 03/12/2019, the same user "gmsuser" executed the ransomware executable "12.10.2019Taskmngr.exe".*
>
> *Both* [redacted] *and "gmsuser" user accounts are believed to have been compromised. The security logs on system "CEN-PRIME" only go back to 21:45 on 03/12/2019 whereas the first encrypted file on the system appears at 07:13 on the same day. Without the earlier security logs prior to the system restore of "CEN-PRIME", it is not possible to determine an exact time of compromise for these accounts.*
>
> [redacted] *did not identify any evidence of data exfiltration. No evidence of archive files consistent with the attacker compressing large amounts of data for exfiltration were found on any of the systems, but this does not definitively rule it out*."[24]

40. The forensic analysis conducted by [redacted] was unable to confirm if exfiltration of personal data had taken place as a result of the breach, but could not conclude that it had not. The Forensic Report highlighted that the C drive of the host CEN-PRIME server had been wiped and restored by Centric on 4 December 2019, which removed vital forensic traces.

41. The DPC issued an Inquiry Commencement Letter ('**the Commencement Letter'**) by email and registered post to Centric on 1 March 2021 notifying the company that the DPC had commenced an Inquiry under and in accordance with section 110(1) of the 2018 Act. The letter

[23] C.1.29 page 10
[24] C.1.29 page 6

contained details of the personal data breach notified to the DPC that would be the subject of the Inquiry and contained thirty-two questions seeking further information from Centric.

42. The decision to commence the Inquiry was taken having regard to the circumstances of personal data breach notified by Centric. The Commencement Letter informed Centric that the Inquiry would examine whether or not Centric 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 Centric in that context. In this regard, the scope of the Inquiry was expressly stated to include the steps taken by Centric to comply with the principle of integrity and confidentiality pursuant to Article 5(1)(f) GDPR and the technical and organisational measures taken by Centric to ensure security of processing pursuant to Article 32(1) GDPR. These measures ought to have been in place in order to protect the rights and freedoms of each data subject from the implementation of the GDPR up until the commencement of the inquiry (the "**temporal scope**"). It was also stated in the Commencement Letter that the inquiry might focus on data protection governance, records management and security of personal data.

43. The Commencement Letter set out that the Inquiry would formally document the facts as they relate to the subject of the Inquiry. The relevant facts ascertained during the personal data breach notification and handling process were set out in the Commencement Letter. The facts, as established during the course of the Inquiry, are set out below in this Decision.

44. Centric provided submissions in response to the Commencement Letter on 9 April 2021. In its submissions, Centric outlined the technical and organisational measures that Centric had in place to meet the requirements of the GDPR. The submissions outlined policies and procedures, data protection governance, technical measures and security measures, which are considered throughout this Decision.

45. On 23 June 2021, Centric requested an extension to the deadline for its submissions. In its response of that date, the DPC's letter outlined that Centric had previously sought an extension for its submissions, which had been granted. Further to this, Centric had failed to make submissions on additional queries by 1 June 2021 and a second extension of one week was granted on 8 June 2021. Centric indicated that its submission was prepared in its email to the DPC of 15 June 2021, nonetheless Centric once more failed to make a submission by the deadline of 15 June 2021. On 21 June 2021, the DPC wrote to Centric granting a further extension until 24 June 2021 to make its submissions. Finally, in response to the request for an extension of *"3 to 4 weeks"* the DPC's letter of 23 June 2021 restated the obligation of Centric to cooperate with the DPC under Article 31 GDPR and outlined that a draft Issues Paper would be formulated on the basis of submissions received by close of business on Friday June 25 2021.

46. Centric provided further submissions on 25 June 2021 and 5 August 2021.

47. The submissions outlined the steps that Centric had taken since the personal data breach in order to comply with the GDPR including details of organisational and technical measures. The submissions appended a number of documents, which are considered throughout this Decision.

48. Having received Centric's submissions, 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 making a decision under section 111 of the 2018 Act in respect of this Inquiry. The DPC furnished Centric with the Inquiry Issues Paper on 29 October 2021 and invited Centric's submissions on any inaccuracies and/or incompleteness in the facts.

49. Centric provided comments on the Inquiry Issues Paper on 10 December 2021. The comments included remediation steps taken by Centric and improvements in relation to the security of processing of data along with additional information relating to the facts as set out in the Inquiry Issues Paper. Those comments were analysed and were considered as part of the Draft Decision.

50. Centric was provided with the Draft Decision on 11 October 2022. Centric was afforded the opportunity to make submissions on the proposed infringements that were identified in the Draft Decision and the corrective powers that I proposed to exercise. On 31 October 2022 Centric 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. Scope of the Inquiry and the Application of the GDPR

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

52. In this regard, the Commencement Letter specified that the Inquiry would focus on Centric'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 Article 5(1) and Article 32(1) GDPR. The Commencement Letter stated that the Inquiry might also focus on the areas of accountability pursuant to Article 5(2) GDPR, data protection governance and records management.

53. 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.*

54. 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;

55. 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;*

56. 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.*

57. 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*

58. 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.*

59. In this case, the breached data contained the personal data including name, date of birth, PPSN and contact details of Centric's patients along with some special category data in the form of health data. The breach concerned ransomware, which was present on the system as a result of unauthorised access to personal data held by Centric and led to alteration of the personal data by an unauthorised party and the permanent deletion of some of that personal data. Therefore, the processing of personal data by Centric via computing systems falls within the scope of the GDPR.

60. 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.

61. 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.*

62. 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.*

63. 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. Article 32 GDPR includes an obligation to assess the risks and consider "*the state of the art*" with regard to measures available. The term "*state of the art*" is not defined within the GDPR. By dictionary definition, it is defined as "*using the latest techniques or equipment*".[25]

E. Centric's Submissions in relation to the Draft Decision

64. The Draft Decision was provided to Centric on 11 October 2022, and Centric was requested to furnish any submissions it wished to make to the DPC by 31 October 2022. Centric furnished its submissions in respect of the Draft Decision on 31 October 2022 ('**Submissions in relation to the Draft Decision**'). Centric stated that its submissions were in respect of:

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

- Rejection of the provisional administrative fine and reprimand issued by the DPC;
- The grounds on which the DPC issued a provisional reprimand;
- References to aggravating factors and negligence on the part of Centric;
- The proposed temporal scope of the draft decision;
- Security practices report from Paradyn, a network & security infrastructure services provider, opining that Centric's patching, firewalls and data backup procedures now adhere to Centre for Internet Security best practices.[26]

65. I have considered Centric's submissions in relation to the above. Part L deals with my further consideration and analysis of Centric's submissions regarding its view that the reprimand, as proposed in the Draft Decision, was not appropriate. Part M deals with deals with my further consideration and analysis of Centric's submissions regarding its view that the administrative fine proposed in the Draft Decision was excessive, references to aggravating factors and negligence on the part of Centric, and the proposed temporal scope of the Draft Decision.

F. Issues for Determination

66. The Inquiry Issues Paper identified that the following issues arose for determination:

- any risk analysis carried out ***prior*** to the personal data breach;
- whether appropriate technical and organisational measures were properly implemented to address the security risks that were (or should have been) identified in the risk analysis above ***prior*** to the personal data breach;
- whether the organisational and technical measures ensured the ongoing confidentiality, integrity, availability and resilience of the processing systems containing the personal data, so as to ensure the ability to restore availability and access to personal data ***at the time of the personal data breach***;
- whether the organisational and technical measures ensured the ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident, i.e. ***at the time of the personal data breach***;
- whether appropriate steps were taken ***after*** the personal data breach to ensure security of processing was restored for the personal data of data subjects impacted by the breach and whether appropriate steps were taken to ensure security of processing for the personal data of any other data subjects to be processed on the same systems.

67. Therefore, having considered the Commencement Letter, the Inquiry Issues Paper and submissions thereon, and the other relevant materials, it falls for me to determine in this Decision whether Centric has demonstrated pursuant to Article 5(2) GDPR that it has complied with those aspects of its obligations under Article 5(1)(f), and Article 32(1) GDPR to implement appropriate technical and organisational measures that ensure appropriate security of the personal data of its patients.

[26] C.10.2

G. Analysis of the Issues for Determination

a) Assessment of the Risks

68. The level of security that controllers and processors are obliged to implement must be appropriate to the risk posed to the rights and freedoms of natural persons by the personal data processing. Regarding Centric's processing of personal data on its servers, those risks include the risk of unauthorised access or unauthorised disclosure of personal data to third parties. It also includes the risk of accidental or unlawful destruction, alteration of or loss of availability of the personal data processed within the platform.

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

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

70. *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources and others*[27] provides further guidance on the risk assessment. In this case, the Court of Justice of the European Union ('**the CJEU**') declared the Data Retention Directive[28] invalid. The Directive required electronic communication service providers to retain certain data for a period of time. The Court held that the Directive did not ensure effective protection of the data retained against the risk of abuse and unlawful access in circumstances where it did not lay down specific rules in relation to:

> *(i) the vast quantity of data 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.*[29]

71. 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 Centric's processing must consider, first, the likelihood of unauthorised access to, or alteration/destruction/disclosure of, personal and special category health 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 of the processing. In considering these factors, regard

---

[27] 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).

[28] 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.

[29] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd, op. cit,* paragraph 66.

must also be had to the quantity of personal data processed and the sensitivity of that data, as set out by the CJEU.

72. Centric was asked to provide specific information that addressed what measures were in place to comply with Article 32 GDPR and by reference to the principle set down in Article 5(1)(f) GDPR in terms of an assessment of the risks of varying likelihood and severity associated with the forms of data processing activities involved in the notified breach.

73. Centric responded that:

> *"Centric Health undertook a periodic review of the IT infrastructure and network across the organization. Up to the point of the malware incident the last significant review took place in May 2018.*
>
> *"Specifically, and in relation to the Primacare environment, it was identified that the IT Infrastructure and centralized Patient Admin Software (PAS) was deemed high risk as it provided an IT environment for seven Primacare practices."* [30]

74. Centric indicated that the review, which included various Centric activities and work streams, was undertaken in house with the support of an independent technical advisor.

75. The DPC asked Centric what risk assessment it had undertaken on the physical CEN-PRIME system (and hosted virtual systems) prior to the breach to identify any data privacy risks. Centric provided the following comments:

> *"The SQL database that was compromised as part of the incident contained patient data. The SQL database was used by a Patient Admin Software (PAS) called* [redacted] *which is provided by* [redacted] *Health. User access to the PAS is access controlled by individual user credentials. The credentials are not linked to nor controlled by any Centric Health system therefore Centric Health has very limited control over the access to the PAS. All user requests related to user credentials has to be handled by* [redacted] *support.*
>
> *"Prior to the incident Centric Health had undertaken a review of the infrastructure and identified that CEN-PRIME was running on a Windows2008 OS which was subsequently upgraded to Windows2016 OS. The new server had ESET installed, back-ups in place and local patch management configured."*[31]

76. The DPC further queried as to whether Centric carried out any adequate assessment of the risks of varying likelihood and severity for the rights and freedoms of natural persons ('data risk assessment') associated with Centric's processing of personal data on its Patient Administration System, in particular with regard to the fact that the majority of the personal data was clinical health information that was special category personal data pursuant to Article 9 of the GDPR.

---

30 C.3.1 page 3

31 C.3.1 page 7

77. Centric submitted:

> *"Due to the significant passing of time that has resulted in the turnover of staff and resources used to manage our data protection compliance obligations at the time, we are severely restricted in our ability to source further information to supplement our submissions to date. We note that many of our documents would have been stored on the "Smartsheets" platform which is no longer active and from which the data stored has now been deleted. We have attached a copy of a Data Protection Assessment that we commissioned Sytorus, data protection specialists, to undertake between October and December 2017 as part of our ongoing commitment to ensure compliance with data protection laws (See Appendix 12). The findings and learnings from this report were reflected in assessments that we carried out in relation to the processing of personal data on our Patient Administration System to meet our obligations under Articles 6 and 9 of the GDPR.*
>
> *"We are unable to identify any further risk assessments to those already notified to the DPC. In this regard, we would direct the DPC to please refer to our previous responses provided to date and in particular to Queries 1 and 2 in our submission dated 9 April 2021* [DPC Document C.3.1]*."* [32]

78. In its submissions to the DPC of 31 October 2022, Centric stated that it "*acknowledges and accepts that in certain instances, it failed to adequately document accounts of its risk assessments. Since the date of the breach, Centric has made improvements to its processes and procedures in order to ensure that risk assessments are conducted on a regular basis and that they are sufficiently documented*." [33]

79. Centric's failure to maintain documented accounts of its risk assessments is considered further below regarding Article 5(2) GDPR. However, regarding the application of Articles 5(1)(f) and 32 GDPR, in the circumstances, I consider that Centric's processing of personal data presented a high risk in terms of both likelihood and severity to the rights and freedoms of data subjects. The severity of these risks to the rights and freedoms of data subjects was high in circumstances where Centric's processing entailed a significant amount of personal and special category data, access to which ought to have been limited to Centric. The risk arising from this processing of patients' personal data on the server included that an unauthorised person could gain access to patients' data, which would pose a high risk with regard to the fundamental rights and freedoms of data subjects, with the possibility of identity theft, medical identity theft and extortion. An associated risk was that having gained access, the integrity and/or availability of the personal data could be compromised, causing disruption to the medical care of data subjects. Unauthorised deletion of such personal data, for example, could interfere with the provision of medical care to data subjects.

80. Centric stated in its submissions of 31 October 2022 that it did not accept "*the DPC's assertion that unauthorised access of the patients' personal data could result in the disruption of medical*

---

[32] C.7.1 pages 6-7

[33] C.10.1 page 5

care to the data subjects, and/or interfere with the provision of medical care to the data subjects. There is no evidence that this occurred in this case. In any event it is, respectfully, outside the remit of the DPC to opine on matters relating to medical treatment".

81. I disagree with Centric's claim. While it is fortunate that there has been no evidence of any clinical impact on Centric patients, this does not alter the fact that the fundamental rights and freedoms of Centric patients were potentially put at risk due to the loss of availability and absolute loss of personal and special category data.

82. The likelihood of the risks to the rights and freedoms of data subjects was also high. In light of the quantity of the personal data processed and the purposes of that processing, there was a significant risk of ransomware attacks and other attacks. This processing entailed a significant amount of personal and special category data, access to which ought to have been limited to Centric. Therefore, having regard to this high risk, it was incumbent on Centric to implement appropriate technical and organisational measures, as set out in Article 32 (1)(b) and Article 32(1)(c) GDPR.

83. I find that Centric's processing of personal and special category personal data on the server 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 platform was high in the absence of appropriate technical and organisational measures. The severity of that risk was also high in circumstances where the data processed was sensitive in many instances and could result in failure to provide adequate medical care due to a lack of availability of clinical records and other potential harm.

b) Measures Implemented by Centric to Address the Risks

84. 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 assess the risk to data subjects of the particular processing and shall implement *appropriate technical and organisational measures to ensure a level of security appropriate to the risk*, taking into account various factors.

85. 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.

86. Centric'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 in order to ensure the ongoing confidentiality and integrity of the processing of personal data on its patient administration system. These measures can be categorised within the areas of scope specified in the Commencement letter as follows:

a) Data protection governance,
b) Records management,
c) Security of personal data
    (i) Technical measures
    (ii) Organisational measures

(a) Data protection governance

87. Centric outlined that it had a range of policies and procedures in relation to data protection including the following operating procedures-

- Data Protection Policy[34]
- Information Technology Policy[35]
- End User Policy[36]
- Access Security Policy[37]
- IT Security Policy[38]
- IT Change Management Policy[39]

88. Centric's Information Technology Policy was dated June 2018. The Information Technology Policy stated that all software patches were evaluated and tested prior to being applied. Centric stated that the records of such evaluation for all the patches applied to the CEN-PRIME server, its hosted systems, and the firewall for the year 2019 were not available.[40]

89. Centric's Information Technology Policy states:

> "*Centric Health has an annual health check on its Wide Area Network and IT Security Audit and is due to begin annual penetration and social engineering testing as part of the ongoing internal audit schedule, an external gap analysis is scheduled for June 2017*."

90. Centric was asked to furnish records of any health check, security audit, penetration testing and gap analysis carried out in 2017, 2018 and 2019. In response, Centric provided two documents. The first was an ISO27001:2013 *Surveillance and Scope Extension Audit Report.*[41] The audit was carried out in September 2016 to assess the conformity of Centric's Management Systems with the ISO27001:2013 standard. The second document provided was a further ISO27001:2013 *Surveillance, Scope Extension Assessment Report,* which was carried out in March 2017.[42]

---

34 C.1.19
35 C.1.21
36 C.1.22
37 C.3.3
38 C.3.4
39 C.3.5
40 C.3.1 page 27
41 C.3.8
42 C.3.11

91. Centric's Patch Management Policy sets out the need for a Security Impact Assessment and a Technical Impact Assessment that must be documented in relation to each critical patch, software update, hot fix or firmware update.[43] The policy also sets out the requirement for the prior approval before the implementation of all but Critical Patches, and the necessity to document (at operational meetings with the vendor or support provider) any decisions against applying a patch or delaying its deployment.

92. The Forensic Report notes that no security or feature patches were applied to Centric's Windows Operating System for the entirety of 2018. That report shows that patches were applied from January 2016 to September 2017 and then from July 2019 until December 2019.[44] Application of all applicable security patches is essential to ensure an appropriate level of IT security and to guard against cyber and malware attacks. Further to this, that Forensic Report notes that unknown software was installed on 9 January 2018, which may have been a standalone programme or a component of Windows. This software caused various C++ support libraries to be installed. The unknown software is no longer shown as remaining on the system, and although this particular software may have been innocuous, it demonstrates a serious lapse on the part of Centric and an inability to identify all software operating on its system.

93. The DPC identified that a large number of patches were released by Microsoft in 2018 that should have been applied to the Windows Operating System by Centric.[45]

94. Centric stated in its submissions of 31 October 2022, that the failure to implement patches solely related to the "*legacy Primacare server"* and that there was "*no evidence that the 2018 suite of hotfixes released by Microsoft for the Windows Operating System would have prevented the installation of the Phobos ransomware package in the present case*"[46].

95. I find that, regardless of whether the patches in question would have prevented the installation of Phobos ransomware, the failure to implement any security patches from the implementation of GDPR onwards is demonstrative of a failing to ensure the security of the Primacare server and Centric's IT systems as a whole.

96. Centric's failure to implement patches in a systematic manner greatly increased the risk of a cyber or malware attack. Appropriate security measures in the circumstances included technical and organisational measures to ensure that security patching was applied in a timely manner. It is the responsibility of the data controller as owner of the server to ensure that any procedures are in place and the application of patches are applied in a timely manner.

---

43 C.3.4
44 C.5.1 page 2
45 C.8.2
46 C.10.1 page 9

97. When asked to provide findings of a May 2019 ICT review with respect to the CEN-PRIME server, its hosted systems, backups and the security of the associated ICT systems, Centric's response to the query did not contain this information. [47] Centric stated that the purpose of the review conducted in May 2019 was to achieve the ISO270001 certification.

98. In its submissions of 31 October 2022, Centric stated that immediately following the data breach an incident report was prepared on 16 December 2019, which was in accordance with the policies that were in place. [48] However, I note that later in Centric's submissions references is made to the fact that the report was not previously provided to the DPC on the grounds that it could not be located and that "*the custodians of the report [had] left the company*. [49] I find that this falls some way short of the best practices to ensure that the incident is comprehensively dealt with and that any possible repeat of the incident may be avoided.

99. As noted above, Centric had identified a high risk in its processing of the sensitive patient personal data. As it was processing such high risk data, it was appropriate for Centric "*to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services*" pursuant to Article 32(1)(b) GDPR. Centric had a range of Data Protection Governance policies and procedures in place to ensure the accuracy and security of patients' personal data. However, these policies were not adhered to and the steps within them were not carried out at the determined intervals.

(b) Records management

100. Centric outlined to the DPC its records management policies such as its Retention Periods for Healthcare and Other Records. [50]

101. Centric provided details to the DPC of its backup system, which I find highlights a number of issues not consistent with an appropriate level of security.

> *"The backup software was Altero. It is believed that a SQL backup was taken and a daily Altero backup of the VM's snap was taken and stored on the physical server and not off-site.*
>
> *"It is also believed that the backup was infected at the time of the incident.*
>
> *"This server was in the process of moving to a new infrastructure solution and was not configured as per the standard solution. Therefore, no processes where in place to test data fail-safes including the restoration from backup.*
>
> *"We are unable to confirm the date of the last restore process prior to the breach for this server.*

47 C.1.7 page 10
48 C.10.5
49 C.10.1 page 12
50 C.3.2

"We understand that the backup that was in place was to a local drive on the server which is not consist with the advice highlighted on the Malwarebytes Guide."[51]

102. In its submissions of 31 October 2022, Centric acknowledged that the "*daily backup of data on the CEN-Prime server should have been stored off site and not on a local drive on the server*".[52]

103. Centric indicated that it had records management oversight measures in place to ensure the accuracy and security of patients' personal data. However, the deviation from the standard practice of off-site storage, incomplete data migration of personal data, a failure to have a proper failsafe backup of systems available and a failure to document the reasons behind the decision to save backups locally to the server show that the oversight measures were not sufficient to prevent the breach. Again, in circumstances where the data being processed gave rise to a high risk to the data subjects, it was appropriate to implement measures referred to in Article 32(1)(d) 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) Security of personal data

(i) Technical measures

104. Centric provided the following description of its physical and virtual operating system environments prior to the 2019 breach which included:

- Up-to-date ESET antivirus software on all virtual servers;
- Routine patching of virtual servers;
- Physical access controls to data centres overseen by [redacted];
- Use of firewall and Windows Directory passwords.[53]

105. Centric outlined that access to the Patient Administration System was controlled by way of individual user credentials, which were handled by [redacted] Support. Centric also confirmed that the data at rest in the PAS were not encrypted.[54]

106. As stated above, the Forensic Report noted that the host server was fully exposed to the internet with a password that "*could have been brute forced without too much difficulty*" and that many unsuccessful attempts were made to log in to the [redacted] account prior to successful log in, which was consistent with this approach.[55] [redacted] further noted in the Forensic Report that the passwords to administrator accounts "*appeared to follow a common*

51 C.3.1 page 17
52 C.10.1 page 9
53 C.3.1 page 16
54 C.3.1 page 11
55 C.1.29 page 4

organizational format and would not meet password security standards for internet-facing services".[56]

107. The Forensic Report outlined that the "*network firewall was fully exposed, allowing all inbound and outbound traffic through*".[57] However, Centric claimed that:

> *"The performance of the firewall would not impact the effectiveness or appropriate security in respect of the security of data held on the system."*[58]

A properly configured firewall as part of an IDS (Intrusion Detection System) is the frontline of defence for an organisation against external cyber threats. It is clear that a non-functioning firewall would reduce security. The European Union Agency for Cyber Security (ENISA) has provided guidance on data security since before GDPR came into application and states:

> "*Traffic to and from the IT system should be monitored and controlled through Firewalls and Intrusion Detection Systems*."[59]

108. The Cybersecurity risk assessment carried out by Auxilion 18 months prior to the breach recommended that Centric needed to be "*proactive in avoiding the risks associated with privacy, security and related cyber threats*". The Remote Desktop Protocol was running on Centric's server and was fully exposed to the internet, but could have been blocked by a properly implemented firewall. Security settings could have been configured to restrict access to a known IP address range (whitelisting), thus excluding that of the bad actor. Therefore, I reject Centric's assertion the performance of the firewall would not affect the security of the data held by Centric.

109. Centric provided details of its hosting arrangements and the proposed data migration at the time of the personal data breach. Although Centric had planned to introduce a new distributed localized environment, migration had not been completed by the time of the breach. Moreover, with respect to the CEN-PRIME server, migration had not yet begun.

> *"In June 2019, Centric Health initiated a project to replace the remote desktop service centralized environment with a distributed localized environment. The distributed localized environment was aligned to the Centric Health model whereby a local server containing a local patient administration system would be provided to each PrimaCare practice. However, at the time of the Incident on 3 December 2019, the Centric Health project was still in progress and had not initiated migration with respect to the CEN-PRIME host server.*
>
> *"The following virtual machines were hosted on the CEN-PRIME host server:*
>
> • *PC-RS02 – Session Host*

[56] C.1.29 page 10
[57] C.1.29 page 4
[58] C.7.1 page 11
[59] C.8.3 p. 62 Enisa Handbook on Security of Personal Data Processing, December 2017

• *DC01 – Network Domain Controller*
• *PC-AS02 – Application Server*
• *PC-AS01 – SQL Database"*[60]

"This project was a very significant undertaking as is evident in what is defined above and is not possible to achieve in a short amount of time. At the time of breach circa 40% of the plan had been implemented and we had planned to decommission the [redacted] *data centre on 8 December 2019, but the malware attack forced us to postpone this and implement alternative measures."* [61]

110. Centric's submissions demonstrate that the CEN-Prime server had not been migrated at the time of the personal data breach, nor had it been appropriately secured. As such, the data contained on the CEN-PRIME server was unprotected and particularly vulnerable to attack. Centric indicated that it was "*satisfied that the appropriate measures were implemented to secure the processing of personal data at the time of the breach*"[62], however with reference to the measures detailed above, I find that there is very little basis for this assertion.

111. Centric's failure to implement industry standard measures such as complete patch application, encryption of data at rest, appropriate levels of server security and failure to ensure an appropriate level of security of passwords and log in credentials demonstrates that adequate technical security measures were not in place to ensure the ongoing integrity and confidentiality of personal data held by Centric. Therefore, I consider that the technical security measures in place at the time of the breach did not meet the standard required by the Article 5(1)(f) GDPR or Article 32(1).

(ii) Organisational measures

112. The DPC asked Centric to provide details of the backup software, hardware, backup methods and processes in place, including:

- information on how often backups were copied/moved off the live system in such a manner that they were no longer exposed to access or alteration;
- the extent to which the backups were exposed to the same attack vector;
- what the processes were to test data fail-safes, restoration from backup/disaster recovery;
- when the restore process had last been tested prior to the data breach; and
- if Centric, or its service provider, had followed the advice highlighted on Malwarebytes' Guide to Backups that "*It is also recommended that you do not keep*

60 C.4.13 page 12
61 C.3.1 page 6
62 C.7.1 page 10

the backup drive connected to the system all the time. It should only be connected to do the backup and then once the backup has completed disconnect the drive"[63]

113. Centric responded that:

> *"The backup software was Altero. It is believed that a SQL backup was taken and a daily Altero backup of the VM's snap was taken and stored on the physical server and not off-site.*
>
> *"It is also believed that the backup was infected at the time of the incident.*
>
> *"This server was in the process of moving to a new infrastructure solution and was not configured as per the standard solution. Therefore, no processes where in place to test data fail-safes including the restoration from backup.*
>
> *"We are unable to confirm the date of the last restore process prior to the breach for this server.*
>
> *"We understand that the backup that was in place was to a local drive on the server which is not consist with the advice highlighted on the Malwarebytes Guide."*[64]

114. The DPC sought details of appropriate technical and organisational measures put in place prior to the personal data breach. Centric stated that:

> *"It is not viable for Centric Health to have all of the required expertise in house, so part of our control environment requires the use of third-party specialists to ensure best Practices are identified and kept up to date.*
>
> *"Specifically, and in relation to the Primacare environment, in June 2019 Centric IT initiated a project to move from the Primacare RDS centralized environment to a distributed localized environment. The distributed localized environment was aligned to the Centric Health model whereby a local server containing a local PAS would be provided to each of the seven Primacare practices. This initiative would remove the risk of both centralized IT infrastructure and a centralized PAS."*[65]

115. The fact that Centric did not have a functioning business continuity plan demonstrates that adequate organisational measures were not in place to ensure the ongoing accuracy and integrity of personal data held by Centric. This is evidenced by the fact that the backups were stored on the physical server as opposed to offsite so that the backup itself was vulnerable and infected at the time of the data breach. I note that there were no records to document processes for testing of restores from the backup systems and that testing of restoration did not occur at regular intervals. As such, Centric was not in a position to know the integrity of the backup data or whether any backup restoration attempt would be successful at the time of the

---

63 https://forums.malwarebytes.com/topic/136226-backup-software/
64 C.3.1 page 17
65 C.3.1 page 4

breach. Therefore, I find that the organisational measures in place at the time of the breach did not meet the standard required by the GDPR.

c) Processes to test, assess and evaluate effectiveness of measures

116. The severity of the risk to the rights and freedoms of natural persons increased due to the quantity and sensitivity of personal and special category data processing undertaken by Centric. The technical and organisational measures that Centric 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. Centric had an obligation to run tests on its 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

117. 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. 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 records management

118. Centric outlined that it had a range of oversight and quality assurance measures in place. Oversight and quality assurance measures, including applying minimum password complexity rules and limited log on attempts to systems or applications processing personal data, must be sufficiently robust and appropriately designed in order to identify issues before they result in a breach.

(c) Testing security of personal data

(i) Technical measures

119. An appropriate level of security includes **technical measures** that may have, inter alia as appropriate, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. The personal data being processed was health data that required suitable and specific measures to safeguard the fundamental rights and the interests of the data subjects. In those circumstances, it was appropriate that technical measures should have ensured confidentiality, integrity, availability and resilience. Centric did not have adequate protections in the form of passwords and encryption of data at rest, nor was there any testing of these technical measures, which would have highlighted the risks to the integrity of data processed by Centric. Similarly, it was appropriate for Centric to have appropriate technical measures implemented to create adequate, secure backups of the personal data or effective and comprehensive measures to restore all the personal data from backups in the event of an incident. The lack of testing along with lack of robust backup and recovery measures led to a failure to ensure availability and resilience of the processing systems and services. Centric took insufficient steps to identify and mitigate the risks present in its system.

(ii) Organisational measures

120. 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, where appropriate pursuant to Article 32(1)(d) GDPR, controllers must take the initiative to test, assess, and evaluate their organisational and technical security measures.

121. As noted above, the processing of sensitive personal health data requires suitable and specific measures to protect the interests of the data subjects and this should involve appropriate processes to test the effectiveness of the measures implemented pursuant to Article 32(1). Centric did not regularly test the security of its servers, attempt to restore its systems from the backup solution in place, or assess the risks to patient data from only having partially completed a server migration. Therefore, I consider that the organisational security measures in place at the time of the breach did not meet the standard required by the GDPR.

122. An appropriate level of security includes organisational measures to ensure at least that there is:

- Documentation of the security policy of the controller and the procedures to be followed by staff;
- Adequate training of all staff in those policies and procedures;
- Oversight of ongoing implementation of those policies and procedures.

H. Findings Regarding Article 5(1)(f) and 32(1)

123. I consider that the root cause of the personal data breach was that ransomware was executed on Centric's system, which held sensitive health data. The processing by Centric 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 ransomware bad actor was **unauthorised and unlawful**. The processing by Centric itself in the immediate aftermath of the ransomware attack resulted in **processing** causing permanent **accidental loss** of some personal data. In the circumstances as outlined above, I find that the lack of appropriate measures to prevent the placement and execution of ransomware on this system and the subsequent steps taken by Centric that permanently deleted some of the personal data amounted to an infringement of Article 5(1)(f) GDPR.

124. There was a significant **loss of availability** of sensitive personal data that was subsequently reconstructed from other sources. There was an **inability to restore the availability** for a subset of the data. There was a failure to appropriately address the identified risks and ensure ongoing integrity and availability, amounting to an infringement of Article 32(1) GDPR.

125. For the reasons set out above, I find that Centric 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 its Patient Administration System.

I. Accountability Principle

126. Article 5(2) GDPR provides that "*[t]he controller shall be responsible for, and be able to demonstrate compliance with, [Article 5(1)] ('accountability')*". This includes accountability in respect of the 'integrity and confidentiality' principle in Article 5(1)(f) GDPR.

127. Recital 74 GDPR states that:

> *"The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons."*

128. I have set out above how Centric failed to implement appropriate technical and organisational measures pursuant to its obligations under Articles 5(1)(f) and 32(1) GDPR. Regarding the measures that Centric did implement, the obligation in Article 5(2) GDPR to demonstrate compliance with Article 5(1) GDPR required Centric to maintain documentation to demonstrate that such measures were in place.

129. In the circumstances, Article 5(2) GDPR obliged Centric to retain appropriate documentation to demonstrate whether risks or vulnerabilities had previously been identified, and to demonstrate any planning for mitigation of such risks. Centric claims to have undertaken relevant assessments of such risks. The documentation of the progression from risk assessment to implementation of appropriate measures forms part of the requirements to satisfy the principle of accountability of Article 5(2) GDPR. As such, Centric's failure to maintain such records amounts to a contravention of Article 5(2) GDPR.

130. As set out above, Centric's Patch Management Policy required documented Security Impact Assessments and Technical Impact Assessments for each critical patch. Despite this, Centric was not able to produce any such documents to the DPC. Centric stated that it was not in a position to demonstrate adherence to the patch management policy due to the unintentional deletion of log files.

> *"As explained as part of our letter of 9 April 2021, the relevant log files were unintentionally deleted arising from attempts to restore the affected systems. Unfortunately this means that we have no available patch records, security impact assessments or implementation reports.*
>
> *"The CEN-PRIME host server resided within the PrimaCare environment/domain and was the only server in that environment/domain. The Centric IT Patch Management Policy*

would have applied to the CEN-PRIME host server. We believe that if we had not attempted to patch the CEN-PRIME host server at the time of the Incident, this would have been queried by the independent forensic specialist. We have requested the forensic investigators to check whether any logs are still available."[66]

131. In the circumstances, I consider that Centric's obligation to demonstrate compliance under Article 5(2) GDPR required it to be in a position to produce, amongst other things, documented Security Impact Assessments and Technical Impact Assessments for each critical patch during the temporal scope. As set out above, the Forensic Report states that patches were applied from July 2019 until December 2019. However, Centric failed to maintain relevant documentation for the patches applied during the temporal scope. In circumstances where Centric has failed to do so, I find that it has infringed Article 5(2) GDPR in the circumstances.

132. As Centric's processing included special category personal data, I consider that appropriate measures ought to have included processes to regularly test, assess and evaluate that the security measures were effective. This may have, among other things, included a review of the IT systems in place particularly in circumstances where the server operating system had not been upgraded for some considerable time. Documents which may have been relevant to same are no longer accessible. Centric has failed to furnish documentation to demonstrate that the security measures were subject to testing, assessment or evaluation to determine their effectiveness. Therefore, Centric has infringed Article 5(2) by failing to demonstrate that such tests, assessments and evaluations were undertaken during the temporal scope.

J. Finding Regarding Article 5(2)GDPR

133. For the purpose of Article 5(2) GDPR in respect of Article 5(1)(f) GDPR, I consider that Centric's failure to document the matters referred to above resulted in its failure to demonstrate compliance with the integrity and confidentiality principle in respect of those relevant measures. Therefore, I find that Centric infringed Article 5(2) GDPR.

K. Decision on Corrective Powers

134. I have set out above, pursuant to section 111(1)(a) of the 2018 Act, my decision to the effect that Centric has infringed Articles 5(1)(f), 5(2) and 32(1) GDPR.

135. Under section 111(2) of the 2018 Act, where the DPC makes a decision (under section 111(1)(a)), it must, in addition, make a decision as to whether a corrective power should be exercised in respect of the controller or processor concerned and, if so, the corrective power to be exercised. The remaining question for determination in this Decision is whether 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.

[66] C.4.13 page 11

136. 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…*

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

b. Administrative fines for the infringements of Articles 5(1)(f), 5(2) and 32(1).

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

L. Reprimand

139. 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*

140. I issue Centric with a reprimand in respect of its infringements of Article 5(1)(f) GDPR, Article 5(2) GDPR and Article 32(1) GDPR identified in this Decision. The purpose of the reprimand is to dissuade non-compliance with the GDPR. The infringements contributed to a higher risk of unavailability of patient data and a possible lack of progression of medical appointments with an ongoing risk to patient health. Furthermore, there was a risk of disclosure of patient data to unauthorised third parties. I consider that a reprimand is necessary and appropriate in respect of such non-compliance in order to recognise formally the serious nature of the infringements and to dissuade such non-compliance. The reprimand will contribute to ensuring that Centric 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.

M. Administrative Fines

141. 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*

142. This makes clear that the DPC may impose administrative fines in addition to, or instead of, the 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.

143. Article 83(1) GDPR provides:

> *Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.*

144. 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.*

145. 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 each of the individual infringements identified in this Decision respectively.

146. In applying the Article 83(2)(a)-(k) GDPR factors to the infringements, I have set out below my analysis of the infringements collectively, where it is possible to do so. Regardless of whether the analysis below is individual or collective in respect of a particular factor or infringement, I have considered the infringement of Article 5(1)(f) GDPR, Article 5(2) GDPR and the infringement of Article 32(1) GDPR separately when deciding whether to impose an administrative fine in respect of each infringement. I have made a separate decision on each infringement, and I have made each decision without prejudice to any factors arising in respect of the other infringement.

147. For the avoidance of doubt, my decision as to whether to impose an administrative fine in respect of each infringement, and the amount of that fine where applicable, is independent and specific to the circumstances of each particular infringement. Having considered whether to impose a fine for each infringement and the indicative amount of that fine where applicable, I have at that point considered whether there should be a reduction in light of the cumulative impact of the fines, such that the overall fines in this decision remain proportionate.

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;

148. In considering the nature, gravity and duration of Centric'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 have due regard to the nature, gravity and duration of the infringement. Article 83(2)(a) GDPR also requires me to have due regard to 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.

149. Approximately 2,500 data subjects were permanently affected by the personal data breach considered in this Decision in circumstances where their personal and special category data was deleted with no backup available. However, over 70,000 data subjects, including the aforementioned 2,500, were affected by access to, unauthorised alteration of, and loss of availability to their personal and special category data when the ransomware programme was activated.

150. Centric's infringement of Articles 5(1)(f) and 32(1) GDPR includes the failure to implement technical and organisational measures appropriate to the level of risk as a result of Centric's processing of data subjects' personal and special category data on its server. The failure to implement the necessary safeguards in an effective manner at the appropriate time led to the possibility that patients' personal data being erroneously disclosed to unauthorised people.

151. In Centric's submissions of 31 October 2022 it stated that there is no evidence of unauthorised disclosure of the personal data, no evidence of material loss, nor evidence of further exploitation. Centric maintain that no evidence of exfiltration of data was found.[67] Nonetheless, the circumstances of the breach mean that the possibility existed for the disclosure and unauthorised use of the personal data.

152. In assessing the level of damage suffered by the data subjects, I have had regard to the loss of control suffered by them over their personal data. The personal data affected by the breaches included health data relating to private matters kept strictly confidential by most people and a lack of availability may have serious consequences to the wellbeing of an affected individual.

The nature of the infringement

153. The nature of Centric's infringements of Articles 5(1)(f) and 32(1) GDPR comprises a failure to comply with its obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk in respect of its processing operations concerning the handling of health data and patient appointment data. The objective of Articles 5(1)(f) and 32(1) GDPR is to protect the rights and freedoms of natural persons by ensuring that their personal data are processed in a manner that ensures appropriate security. A failure to implement an appropriate level of security increases the risk of personal data breaches. This, in turn, poses a threat to the rights and freedoms of data subjects because of the potential for damage to data subjects where personal data breaches occur, leading to, inter alia, destruction of essential personal data or unauthorised access, alteration or disclosure of that personal data. Therefore, compliance with Articles 5(1)(f) and 32(1) is central to the protection of the rights and freedoms of natural persons pursuant to the GDPR. As such, non-compliance with this obligation has serious consequences in that it has the potential to result in damage to data subjects.

154. The infringement of Article 5(2) GDPR concerns the failure to be able to demonstrate compliance with the principle of integrity and confidentiality in Article 5(1)(f) GDPR. This includes the obligation to demonstrate the process of risk assessment and the implementation of technical and organisational measures to address the risks appropriately. I consider the inability to demonstrate compliance to be serious.

The gravity of the infringement

155. The gravity of the infringement of Articles 5(1)(f) and 32(1) of the GDPR is serious in circumstances where the infringement resulted in the personal data breach. Centric's lack of technical and organisational measures at the time of the breach contributed to the unauthorised processing of personal and special category data of 70,000 data subjects including the irretrievable loss of personal and special category data of 2,500 of those data subjects. There is a lack of certainty around whether there has been unauthorised disclosure of the personal data as a result of the ransomware attack and, if so, the extent of that disclosure. The infringement of Article 5(2) GDPR includes the failure to document adequately the events surrounding the actual breach, such that there is lack of certainty about the full

[67] C.10.1 page 12

nature of the attack. Notwithstanding this, I consider that the gravity of Centric's failure to implement sufficient and appropriate technical and organisational measures *to ensure the confidentiality, integrity availability and resilience of its processing systems* to be serious.

156. In its submissions of 31 October 2022, Centric provided the DPC a copy of the initial incident report following the data breach.[68]

The duration of the infringement

157. The duration of Centric's infringement of Articles 5(1)(f) and 32(1) GDPR regarding the processing and the infringement of Article 5(2) GDPR commenced at the application of the GDPR on 25 May 2018. The obligation to implement and be able to demonstrate the appropriate organisational and technical measures applied from 25 May 2018. The infringement was ongoing for the entirety of 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 of Articles 5(1)(f), 5(2) and 32(1) GDPR lasted at least from 25 May 2018 until 1 March 2021.

158. In its submissions of 31 October 2022, Centric stated that the period of the temporal scope is excessive. As stated previously, the relevant vulnerabilities existed in the Centric system from the implementation of the GDPR up until the date of the breach and could have been exploited at any time during this period. I therefore reject this submission.[69]

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

159. 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."*[70]

160. 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.*[71]

68 C.10.5 4 Incident report 3.12.2019
69 C.10.1 page 9
70 C.8.1 page 11.
71 Ibid at page 12.

161. 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.

162. 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.

163. In its submissions of 31 October 2022, Centric stated that:

> *"In circumstances where the relevant GDPR and EDBP guidance notes provide little guidance on how negligence is to be assessed / determined, it is submitted that the appropriate test to be applied is under Irish law for tortious negligence. In order to establish negligence, the test for tortious negligence requires that there be actual loss or damage to the recognised interests of the plaintiff. In the present case, there has been no evidence of actual loss being suffered by the impacted data subjects and no claims have been brought against Centric."*[72]

164. I do not find Centric's above submissions persuasive. In the first instance, Centric's assertion that there has been "*no evidence of actual loss being suffered by the impacted data subjects"* is incorrect. As previously stated,70,000 data subjects suffered temporary loss of personal data and of these 2,500 data subjects had their medical records deleted.

165. In the second instance, as the GDPR is an instrument of European Law that is to be applied with equal effect across all of the EEA, its provisions should not be interpreted solely within an Irish legal rubric.

166. As compliance with the GDPR Articles is measured in terms of compliance with clear obligations on controllers and processors, to find any infringement there must have been either an intentional or a negligent failure to meet those obligations. If the infringement has an intentional character then it indicates a more serious infringement and if it has a negligent character then it has a lower severity.

167. Centric's infringement of Articles 5(1)(f) and 32(1) GDPR regarding the processing, concerns its failure to implement appropriate measures to protect the rights and freedoms of natural persons by ensuring that their personal data are processed in a manner that ensures appropriate security 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 this infringement as intentional, I must be satisfied that (i) Centric 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 Articles 5(1)(f) and 32(1) GDPR.

[72] C.10.1 page 13

168. Centric submitted that it carried out *a "periodic review of the IT infrastructure and network across the organization"* and that

> "*…the last significant review took place in May 2018. Specifically, and in relation to the Primacare environment, it was identified that the IT Infrastructure and centralized Patient Admin Software (PAS) was deemed high risk as it provided an IT environment for seven Primacare practices*." [73]

169. Despite Centric's assessment that the processing was high risk, Centric failed to implement appropriate measures to secure this processing. While Centric's attempts to implement appropriate measures were not sufficient for the purposes of Articles 5(1)(f) and 32(1) GDPR), I do not consider that Centric knew that the measures implemented were not sufficient at the time. However, in the circumstances, Centric ought to have been aware that it was falling short of the duty owed under Article 5(1)(f) and 32(1). For example, Centric ought to have been aware that its failure to implement patches in a systematic manner greatly increased the risk of a cyber or malware attack, that its Data Protection Governance policies and procedures were not being adhered to, and its password security standards did not meet the standard required. The infringement was negligent because Centric ought to have been aware that it was falling short of the duty owed under Articles 5(1)(f) and 32(1) GDPR in the circumstances.

170. Similarly, Centric's infringement of Article 5(2) GDPR concerns its failure to be able to demonstrate compliance with Article 5(1)(f) GDPR. The principle of accountability in Article 5(2) GDPR places a positive obligation upon a controller to be able to demonstrate the manner in which it has ensured that processing is in compliance with the principles in Article 5(1) GDPR. This includes accountability in respect of the '*integrity and confidentiality*' principle in Article 5(1)(f) GDPR. In respect of the necessary documentation to show the application of the processes needed to ensure basic cybersecurity, such as application of security patches in a timely manner, I do not consider that this lack of documentation was as a result of a wilful act. However, I consider that Centric's unintentional deletion of the patch records and its general failure to maintain documented records of to demonstrate that the security measures were subject to testing, assessment or evaluation to determine their effectiveness 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;

171. Centric put in place various mitigation measures after it discovered the data breach. Once appropriate measures were fully implemented, a recurrence of the particular breach vector was prevented. However, it is not always possible to correct a past lack of control retrospectively, and these actions did not mitigate the loss of availability and risk to the confidentiality of the data belonging to the affected data subjects. The erasure of the information from the hard drive prior to analysis by the Forensic Analysts removed some information that may have been helpful in assessing the extent of the breach. Having regard to the actions taken by Centric for the purpose of mitigating the damage suffered by data

[73] C.3.1 page 3

subjects, I am of the view that they aggravated the damage suffered by the data subjects. I have had regard to this factor when calculating the administrative fine below.

172. In Centric's submissions of 31 October 2022, it stated:

> *"It is noted that the DPC considers the actions taken by Centric with a view to mitigating the damage suffered by the data subjects to have actually aggravated the damage suffered by the data subjects, and that regard has been had to this factor when calculating the proposed administrative fine. This is a surprising approach to take in circumstances where Centric acted in good faith, and attempted to follow industry best practice, in its attempts to recover the relevant data from the impacted server."*[74]

173. I do not find Centric's above submissions persuasive. While the attempt to recover the data from the affected server may have been envisaged to follow industry best practices, the execution of same fell considerably short of the standard required. In such circumstances, I cannot agree with the contention that the deletion of the patient data should not be considered an aggravating factor.

174. Centric further stated that:

> *"Arguably, if the DPC adopts this approach in this case, it could have a dissuasive effect on other similar cases as data controllers would be faced with the impossible choice of following best practice but with the risk that they will be punished for a human error or take no action at all so as to avoid any potential human error risk and thus be punished for inaction. Accordingly, it is submitted that the impact of Centric's actions in attempting to address the breach, albeit those actions inadvertently resulted in the deletion of data, should not be considered an aggravating factor when determining the appropriate sanction.* [75]

175. I find that there is little basis for Centric's claim that the classification of this action as aggravating will have a dissuasive effect on data controllers who seek to mitigate damage following a data breach. Actions taken by controllers that go some way towards mitigating the damage will be viewed favourably by the DPC and taken into consideration when calculating administrative fines.

176. Finally, Centric stated "*Centric itself was the victim of a crime in this matter and was making best efforts to minimise the impact on data subjects once the breach was identified*."[76] I understand Centric's position and do have sympathy for the attack that it suffered. However, it is incumbent on data controllers to employ the necessary technical and organisational measures to ensure that their security systems are able to deal with such attacks, particularly

[74] C.10.1 page 14
[75] Ibid
[76] Ibid

in circumstances where the controller is dealing with sensitive personal and special category data.

177. Centric compiled a list of *Learnings As a Result of a Data Breach*.[77] This included considerations of prevention plans, security and response plans, consideration of changes to policies and procedures, revision of staff training, and a project plan for the implementation of data protection by design and default. Having regard to the actions taken by Centric for the purpose of mitigating the damage suffered by data subjects, I am of the view that this somewhat mitigated the damage suffered by the data subjects. I have had regard to this factor when calculating the administrative fine below.

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;

178. In the submissions in relation to the Issues Paper, Centric outlined the measures that it had in place to prevent any potential breach of data protection.[78] I have had full regard to those measures in part G of this Decision. This Decision assesses whether Centric complied with its obligations under Articles 5(1)(f) and 32(1) GDPR by implementing appropriate technical and organisational measures to ensure appropriate security of the personal data of patient processed in the patient administration system. In addition, I have considered whether Centric complied with its obligation under Article 5(2) to be able to demonstrate compliance with Article 5(1)(f) GDPR. As stated above, I find that Centric infringed those three provisions.

179. I consider that Centric holds a high degree of responsibility for this failure 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 Articles 5(1)(f), 5(2) and 32(1) against Centric, this factor cannot be considered aggravating in respect of those infringements.

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

180. 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;

181. I acknowledge Centric's cooperation with the DPC during the course of the Inquiry. However, I note that Centric was, in any event, under a duty, in light of Article 31 GDPR, to cooperate, on request, with the supervisory authority in the performance of its tasks. I wish to note that while (as Centric has submitted[79]) the production of a Learnings Review following the commencement of the Inquiry may be viewed as a step towards remedying the infringement of Article 5(2) GDPR described in this Decision and to mitigating its possible adverse effects, the initiation of the Learnings Review has separately been taken into account as a mitigating factor under Article 83(2)(c) above. Furthermore, while I appreciate that Centric took action

[77] C.7.3
[78] C.7.1 pages 7-8, 11-12; C.7.6; C.7.8 - C.7.12
[79] C.7.3

to locate the incident report and comply fully with the request of the DPC, I find that the provision of the report almost three years following the data breach cannot be deemed to be of mitigating effect in this regard.

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

182. The personal data affected by the infringement included personal and sensitive category clinical health personal data. These types of personal data, by their nature, carry a high risk to the rights and freedoms of the affected data subjects with the risk suffering from lack of adequate care arising from the loss of health data. While it is not known whether there was unauthorised disclosure of this personal data, the inadequate security measures implemented related to this sensitive personal data. I find that the sensitivity of these categories of personal data aggravates the infringement of Articles 5(1)(f) and 32(1) in circumstances where there was a loss of availability of health records to 70,000 data subjects for two days and where the personal data of 2,500 of these data subjects were permanently deleted.

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;

183. The DPC received notification of a personal data breach from Centric on 5 December 2019.[80] Controllers are obliged to notify personal data breaches in certain circumstances and Centric's notification of the personal data breach was the manner in which the infringement became known to the DPC.

184. 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."*[81]

185. Centric's compliance with its obligation to notify personal data breaches under Article 33(1) cannot be considered mitigating in respect of the infringement of Articles 5(1)(f), Article 5(2) and 32(1) GDPR.

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

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

---

80 C.1.1

81 ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on the application and setting of administrative fines, op. cit., page 15

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

187. 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.

188. I am of the view that there are no other aggravating or mitigating factors in respect of the infringements of Articles 5(1)(f), 5(2) and 32(1) GDPR.

N. Decisions on Whether to Impose Administrative Fines

189. In deciding whether to impose an administrative fine in respect of each infringement, 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 when deciding the amount of each administrative fine. I find that administrative fines in respect of each infringement are appropriate, necessary and proportionate in view of ensuring compliance with the GDPR.

190. 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.*

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

1) Each infringement is serious in nature and gravity as set out pursuant to Article 83(2)(a) GDPR. Infringements that are of a serious nature and gravity must be strongly dissuaded both in respect of the individual controller and in respect of other entities carrying out similar processing. Regarding the infringement of Articles 5(1)(f) and 32(1) GDPR, where data subjects' personal health data was unavailable and permanently lost resulting in a risk to appropriate medical care, I consider that Centric'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 infringements, I also consider that administrative fines are proportionate in the circumstances in view of ensuring compliance. Centric's infringements of Articles 5(1)(f), 5(2) and 32(1) GDPR caused the permanent loss of personal and special category data of 2,500 data subjects and loss of availability to the personal and special category data of 70,000 data subjects. I consider that the unauthorised access to and alteration of sensitive health data constitutes significant damage in the circumstances. In light of this damage, I consider that administrative fines are proportionate to responding to Centric's infringement of Articles 5(1)(f), 5(2) and 32(1) GDPR with a view to ensuring future compliance. I consider that administrative fines do not exceed what is necessary to enforce compliance in respect of the infringement identified in this Decision.

3) I consider that the negligent character of Centric's infringement of Articles 5(1)(f), 5(2) and 32(1) GDPR carries weight when considering whether to impose administrative fines, and if so, the amount of those fines. This negligence suggests that administrative fines are necessary to ensure that Centric directs sufficient attention to its obligations under Articles 5(1)(f), 5(2) and 32(1) GDPR in the future.

4) I consider that administrative fines would help to ensure that Centric 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 the particular circumstances where the categories of user's data affected by Centric's infringement carry a high risk with regard to the fundamental rights and freedoms of data subjects, in particular in relation to the provision of necessary healthcare, I consider that administrative fines are appropriate.

5) I have had regard to the lack of previous relevant infringements by Centric, which is a slightly mitigating factor. I have also had regard to the actions taken by Centric to bring the data breach to the attention of a minority of the affected data subjects. In light of the negligent character of the infringements, and Centric's failure to comply with its obligations with regard to data protection, I consider that dissuasive administrative fines are necessary in the circumstances to ensure future compliance.

192. Based on the analysis I have set out above, I impose the following administrative fines:

(1) In respect of Centric's infringement of Article 5(1)(f) GDPR, I impose a fine of €275,000.

(2) In respect of Centric's infringement of Article 5(2) GDPR, I impose a fine of between €50,000.

(3) In respect of Centric's infringement of Article 32(1) GDPR, I impose a fine of €135,000.

193. In having determined the quantum of the fines above, I have taken account of the requirement, set out in Article 83(1) GDPR, for fines imposed to be *effective, proportionate and dissuasive* in each individual case. My view is that, in order for any fine to be *effective*, it must reflect the circumstances of the individual case. As outlined above, the infringement is serious in nature and in gravity. The infringement concerns the personal and special category data and increased the risks posed by the processing to the rights and freedoms of those data subjects, in particular in relation to the provision of appropriate medical care to the affected data subjects. I have therefore considered this aggravating factor when calculating the administrative fines. I consider that administrative fines are appropriate, necessary and proportionate in respect of the infringements 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.

194. 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.

195. 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 fines above do not exceed what is necessary to enforce compliance with the GDPR taking into account the number of data subjects using Centric 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.

196. I am satisfied that the three ranges for the fines specified above, if imposed on Centric, would be effective, proportionate and dissuasive, taking into account all of the circumstances covered by the Inquiry.

Article 83(3) GDPR

197. Having completed my assessment of whether or not to impose a fine (and of the amount of any such fine), I must now consider the remaining provisions of Article 83 GDPR, with a view to ascertaining if there are any factors that might require the adjustment of the fines.

198. 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.*

199. The European Data Protection Board ('**the EDPB**') adopted a binding decision ('**the EDPB Decision**')[82] relating to IN-18-12-2, an Inquiry conducted by the DPC into WhatsApp Ireland Limited's compliance with Articles 12, 13 and 14 GDPR. The EDPB Decision arose out of a dispute resolution procedure pursuant to Article 65 GDPR, and was adopted by the DPC in conjunction with the DPC's final decision on 2 September 2021.

200. In light of the DPC's obligations of cooperation and consistency in, *inter alia*, Articles 60(1) and 63 GDPR, it is necessary for me to follow the EDPB's interpretation of Article 83(3) GDPR in inquiries given that it is a matter of general interpretation that is not specific to the facts of the case in which it arose.

201. The relevant passages of the EDPB decision are as follows:

> *"315. All CSAs argued in their respective objections that not taking into account infringements other than the "gravest infringement" is not in line with their interpretation of Article 83(3) GDPR, as this would result in a situation where WhatsApp IE is fined in the same way for one infringement as it would be for several infringements. On the other hand, as explained above, the IE SA argued that the assessment of whether to impose a fine, and of the amount thereof, must be carried out in respect of each individual infringement found and the assessment of the gravity of the infringement should be done by taking into account the individual circumstances of the case. The IE SA decided to impose only a fine for the infringement of Article 14 GDPR, considering it to be the gravest of the three infringements.*
>
> *316. The EDPB notes that the IE SA identified several infringements in the Draft Decision for which it specified fines, namely infringements of Article 12, 13 and 14 GDPR, and then applied Article 83(3) GDPR.*
>
> *317. Furthermore, the EDPB notes that WhatsApp IE agreed with the approach of the IE SA concerning the interpretation of Article 83(3) GDPR. In its submissions on the objections, WhatsApp IE also raised that the approach of the IE SA did not lead to a restriction of the IE SA's ability to find other infringements of other provisions of the GDPR or of its ability to impose a very significant fine. WhatsApp IE argued that the alternative interpretation of Article 83(3) GDPR suggested by the CSAs is not consistent with the text and structure of Article 83 GDPR and expressed support for the IE SA's literal and purposive interpretation of the provision.*

[82] https://edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_en.pdf

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

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

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

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

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

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

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

possibility for the SA to apply the corrective measure within the limit set out for the gravest infringement, i.e. in the example the limits of Article 83(5) GDPR.

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

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

*327. In light of the above, the EDPB instructs the IE SA to amend its Draft Decision on the basis of the objections raised by the DE SA, FR SA and PT SA with respect to Article 83(3) GDPR and to also take into account the other infringements – in addition to the gravest infringement – when calculating the fine, subject to the criteria of Article 83(1) GDPR of effectiveness, proportionality and dissuasive*ness."

202. The impact of this interpretation would be that administrative fine(s) would be imposed cumulatively, as opposed to imposing only the fine for the gravest infringement. The only applicable limit for the total fine imposed, under this interpretation, would be the overall "cap". By way of example, in a case of multiple infringements, if the gravest infringement was one which carried a maximum administrative fine of 2% of the turnover of the undertaking, the cumulative fine imposed could also not exceed 2% of the turnover of the undertaking.

203. I consider that Centric's infringement of Article 5(1)(f) GDPR is the gravest infringement. I further note that the associated maximum possible fine for that infringement under Article 83(4) GDPR is 4% of the turnover of Centric. I have also had regard to Centric's turnover in the calculation of the fine amounts.[83] When the imposed fines for the individual infringements are added together, a fine of €460,000 arises. The imposed fine is below 4% of the turnover of Centric, as considered below.

Articles 83(4) and 83(5) GDPR

204. Turning, finally, to Articles 83(4) and 83(5) GDPR, I note that these provisions operate to limit the maximum amount of any fine that may be imposed in respect of certain types of infringement.

[83] Centric provided the Annual Financial Statement for the period ending June 2021 that stated the Group turnover was EUR [redacted]

205. Article 83(4) GDPR provides as follows:

> *Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher:*
>
> > *(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;*

206. 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;*

207. 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.*[84]

208. 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"*[85]

209. 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

---

84 Treaty on the Functioning of the European Union

85 *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.[86]

210. 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.

211. 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 that tie the subsidiary to the parent company, which may vary from case to case.[87]

212. The CJEU has, however, established[88] 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.

213. 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.[89]

214. 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[90]. 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*

---

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

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

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

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

90 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 …"[91]

215. 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.

216. 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.

217. I calculate the administrative fine on the basis that Centric had a reported group total turnover of € [redacted] million for the year ended 30 June 2021.

218. Applying the above to Article 83(4) GDPR, I first note that, in circumstances where the fine is being imposed on an *'undertaking'* in respect of an infringement of Article 32(1) GDPR, a fine of up to 2% of the undertaking's total worldwide annual turnover of the preceding financial year may be imposed. I further note that the imposed fine is less than 1% of Centric's total worldwide annual turnover for the year 2021.

219. Similarly, applying the above to Article 83(5), in circumstances where the fine is being imposed on an undertaking in respect of each infringement of Article 5 GDPR, each fine may be up to 4% of the undertaking's total worldwide annual turnover of the preceding financial year. I further note the imposed fines are each less than 4% of Centric's total worldwide annual turnover for the year 2021.

220. That being the case, the total of the fines imposed at paragraph 171 does not exceed the overall applicable fining "cap" of 4% prescribed or the gravest infringement by Article 83(3) GDPR.

[91] 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).

O. Summary of Envisaged Action

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

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

1. In respect of Centric's infringement of Article 5(1)(f) GDPR, I impose a fine of €275,000.
2. In respect of Centric's infringement of Article 5(2) GDPR, I impose a fine of €50,000.
3. In respect of Centric's infringement of Article 32(1) GDPR, I impose a fine of €135,000.

P. Right of Appeal

222. This Decision is issued in accordance with section 111 of the 2018 Act. Pursuant to section 150(5) of the 2018 Act, Centric 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, Centric 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.