In the matter of the General Data Protection Regulation

DPC Case Reference: IN-19-9-4

In the matter of Health Service Executive
Decision of the Data Protection Commission under Section 111 of the Data Protection Act 2018
Further to an own-volition inquiry under Section 110 of the Data Protection Act 2018

DECISION

Decision-Maker for the Data Protection Commission:

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

10 June 2026

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Protection Commission
6 Pembroke Row
Dublin 2, Ireland

Contents

A. Introduction

1. This document ('**the Decision**') is a decision made by the Data Protection Commission ('**the DPC**') in accordance with section 111 of the Data Protection Act 2018 ('**the 2018 Act**'). The DPC makes this Decision having considered the information obtained in the separate own-volition inquiry ('**the Inquiry**') conducted by authorised officers of the DPC ('**the Inquiry Team**') pursuant to section 110 of the 2018 Act.

2. Reference to 'the **GDPR**' in this Decision is to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

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

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

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

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

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

5. This Decision is provided to the Health Service Executive ('the HSE') pursuant to section 116(1)(a) of the 2018 Act, in order to give notice of the Decision and the reasons for it, and of the DPC's decision in relation to the powers exercised pursuant to Article 58 GDPR.

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

B. Personal data breaches

7. On 16 November 2018, the DPC received a personal data breach notification from the HSE.[1] The breach was stated to have occurred in the Laboratory Information System ('LIS') of the Midland Regional Hospital Tullamore (**'MRHT'**).

8. The HSE stated that the LIS and the associated backup systems at the MRHT had been subjected to a successful cyber-ransomware attack on 14 November 2018 which caused the LIS database server to go offline. The HSE estimated that the breach occurred at 07:29 hours.[2] This triggered a service alert which was reported by their outsourced provider at 08:48 hours to the Senior Medical Scientist with responsibility for IT. The call indicated that a ransomware attack was in progress. The breach notification also stated that the backup devices for the affected servers were connected to the servers and therefore exploited by the attack.[3] The HSE stated in the breach notification that an off-site backup was available at the [redacted], but that this was incomplete.[4] In correspondence on 4 December 2020, the HSE clarified that a full recording of backup data had been created, but that records created between June 2017 and November 2018 had been encrypted during the attack and were not recoverable. The HSE added that paper records of the data in question were available.[5]

9. The HSE immediately investigated the incident internally and also engaged with an external resource ('**External Cybersecurity Consultancy**'), to carry out an analysis of the incident and identify the source and scope of the breach. The External Cybersecurity Consultancy produced its Forensic Analysis Report to the HSE on 6 December 2018.

10. The External Cybersecurity Consultancy forensic report concluded that on 14 November 2018, a bad actor gained access to the LIS environment by means of an unsecured firewall port, exploited a weak administrator password on a server and was able to access other devices on the system. According to the report, a variant of the CrySIS ransomware was deployed, resulting in the encryption of data on several devices on the LIS.

---

1 Breach Notification Form, 16 November 2018.
2 Breach Notification Form, 16 November 2018, 2.
3 Breach Notification Form, 16 November 2018, 5.
4 Breach Notification Form, 16 November 2018, 6.
5 HSE letter to DPC, 4 December 2020, 13.

11. The report concluded that large-scale data exfiltration was unlikely, but it could not conclusively rule out selective records being extracted due to lack of available information. The report was also unable to conclusively state if personal data was viewed by the attackers, also due to a lack of available information.[6]

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

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

13. Based on the information provided by the HSE in its breach notification and otherwise during the course of this inquiry, the DPC is satisfied that:

- the information affected by the incident notified by the HSE on 16 November 2018 was personal data processed by the HSE,
- the incident arose of from a breach of security, and
- the incident led to one or more unauthorised persons having access to that personal data, allowing them to alter it by way of encryption.

The DPC is therefore satisfied that the incident constitutes a personal data breach according to the definition in Article 4(12) GDPR.

a) Data controller

14. In commencing the Inquiry, the DPC considered that the HSE determined the purposes and means of processing the personal data that was the subject of the personal data concerned in the breach notification made by the HSE to the DPC on 16 November 2018, and so was the controller, within the meaning of Article 4(7) GDPR, in respect of that personal data. In this regard, the HSE confirmed in its notification of the personal data breach to the DPC that it was the controller in respect of tests received from within Tullamore Hospital, as well as being a processor on behalf of tests received from GPs in the region.[7]

15. The DPC is satisfied that it is the competent supervisory authority to perform the tasks assigned to it under the GDPR pursuant to Article 55(1) of the GDPR in respect of the HSE's compliance with its obligations under the GDPR.

---

6 External Cybersecurity Consultancy - Forensic Analysis Report, 4.

7 HSE Update Report BN-18-11-244, 30 November 2018, 5.

C. Legal Framework for the Inquiry and the Decision

a) Legal basis for the inquiry

16. The GDPR is the legal regime covering the processing of personal data in the European Union ('**EU**'). 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, under Part 6 of the 2018 Act, the DPC has the power to commence an inquiry on several bases, including on foot of a complaint, or of its own volition.

17. 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.

b) Legal basis for the Decision

18. The decision-making process for the Inquiry is provided for under section 111 of the 2018 Act, and requires the DPC to consider the information obtained during the Inquiry; to decide whether an infringement is occurring or has occurred; and if so, to decide on the corrective powers, if any, to be exercised. In making this Decision, the DPC has carried out an independent assessment of all the materials provided by the Inquiry Team, of any other materials that have been furnished by the HSE, and any other materials that the DPC considers to be relevant.

19. Having considered all of the information obtained in this Inquiry, the DPC is satisfied that the Inquiry was correctly conducted and that fair procedures were followed throughout. The DPC has had regard to submissions made by the HSE in respect of the draft version of this Decision (**'the Draft Decision'**) sent to the HSE on 1 December 2025 before proceeding to make this final Decision under section 111 of the 2018 Act.

D. Factual Background and Material Considered for the Purposes of this Decision

a) Controller overview

20. The HSE was established by the Health Act 2004 to act as a single body with statutory responsibility for the management and delivery of health and personal social services to the population of Ireland.

21. Section 7(1) of the Health Act 2004 states that the object of the HSE is 'to use the resources available to it in the most beneficial, effective and efficient manner to improve, promote and protect the health and welfare of the public.'

22. Nationally, HSE hospitals were organised into seven hospital groups. The MRHT was part of the Dublin Midlands Hospital Group, an organisational division of the HSE.

23. The MRHT provides acute-care hospital services including a 24-hour emergency department and is the regional centre for Orthopaedics, Otolaryngology, Oncology, Haematology, Nephrology and Rheumatology.

24. The Pathology Department at MRHT provides a clinical diagnostic laboratory service for MRHT's Biochemistry, Haematology/Coagulation, Immunology, Endocrinology Blood Transfusion and Microbiology Departments. It also supports some Cellular Pathology services.

25. According to the HSE, it acts as a controller for any tests received from within the hospital and as a processor for any tests received from general practitioners. [8]

26. The LIS is an information processing system for clinical tests and results that was developed in MRHT in the 1990s and extended to cover other hospitals in the Dublin Midland Hospital Group in the early 2000s.[9] The LIS records and retains information in relation to diagnostic test requests. This information includes: patient name, patient address, patient ID, patient DOB, sex, clinical details (date/time of sample collection, date/time of receipt in the laboratory and date/time of report, specimen type, priority, results/reports, requesting clinician details) and a record of communications relating to test results.

27. The DPC is satisfied that the personal data breach outlined in this Inquiry relates to the processing of personal data in the context of the activities of the HSE, a public authority established under the laws of Ireland. The breach is therefore properly a matter for inquiry under the GDPR.

b) Impact of the breach

28. The HSE initially indicated that approximately 50,000 data subjects might have been affected by the attack.[10] In correspondence to the DPC on 30 November 2018, the HSE increased this estimate to 84,000 data subjects after a gap in patient records spanning September 2016 to 12 November 2018 was discovered.[11] However, the HSE maintained

---

8 HSE Update Report BN-18-11-244, 30 November 2018, 5.

9 HSE, 'DPC Enquiry Consolidated responses', 7 November 2019, 3.

10 Breach Notification Form, 16 November 2018, 4.

11 HSE Update Report BN-18-11-244, 30 November 2018, 6.

that, due to the existence of paper records of lab reports, there was no interruption to patient care.[12]

29. The HSE's breach notification stated that the potential consequences of the breach for affected individuals included a loss of control of their personal data and a lack of access to it. It also made clear that the ransomware prevented the staff of the MRHT and other users of the LIS from accessing patient records held on the system.

30. The breach notification identified that the following identifying details relating to individuals were affected by the ransomware attack:

    - Data subject identity (name, surname, birth date)
    - Contact details.

31. The HSE also indicated that the attack impacted health data, a special category of data under the GDPR.

32. In its breach notification, the HSE rated the risk level as 'medium' because, based on its initial assessment, the affected data had been encrypted and the HSE did not have evidence that it had been removed or fallen into unauthorised hands. On that basis, the HSE did not notify affected individuals.

c) Breach response

33. In correspondence with the DPC on 30 November 2018, the HSE said that it became aware of the breach at 08:48 hours on 14 November 2018 when the outsourced provider reported that the remote monitoring service had detected the attack on the laboratory network. The HSE outlined its immediate incident response as follows:

    - MRHT engaged the ICT Business lead and HSE ICT to contain the issue and take preventative actions against contagion of other sites. The firewall connection between the labs and the HSE LAN was blocked and the Tullamore Lab IT officer physically disconnected server equipment from the network,
    - the Lab Manager and Deputy Lab Manager were informed of the situation,
    - LIS downtime contingency plans were activated,
    - the Hospital Management Team and service users (in-patient locations, GP practices) were notified,

[12] Breach Notification Form, 16 November 2018, 6.

- an [outsourced provider] engineer arrived on site and advised on the severity of the ransomware attack, and
- plans to restore systems were put in place.[13]

d) Inquiry IN-19-9-4

34. The DPC issued the Commencement Letter for the Inquiry on 8 October 2019. This informed the HSE that the DPC had commenced an Inquiry under the DPC reference IN-19-9-4 in accordance with section 110(1) of the 2018 Act.[14] The letter included questions with requests for clarification and documentation. The DPC received a response to these on 7 November 2019.[15]

35. Following subsequent queries and responses between 7 November 2020 and 4 December 2020, the DPC issued a draft inquiry report to the HSE on 27 January 2021. The HSE provided submissions on this on 24 February 2021.[16] The DPC considered those submissions before issuing the final inquiry report. The DPC sent a notice of commencement of the decision-making phase of this inquiry to the HSE on 5 December 2022.

36. On 1 December 2025, the DPC provided the HSE a copy of the Draft Decision and invited the HSE to make submissions on it. The HSE responded with submissions on 19 January 2026 and answered further inquiries on 16 March 2026. The DPC has carefully considered all of the HSE's submissions when preparing this Decision.

E. Scope of the Inquiry

37. The Commencement Letter indicated that the general scope of the Inquiry would be to examine whether or not the HSE discharged its obligations in connection with the subject matter of the personal data breach and determine whether or not any provision(s) of the Act and/or the GDPR have/has been contravened by the HSE in that context.

38. The scope of the Inquiry included focus on the HSE's organisational and technical measures in place to ensure security of the personal data involved. In particular the Inquiry examines the ICT security of the HSE laboratory system in MRHT through:
    - examination of the ICT policies in place at the time of the breach,
    - explanations of whether ICT policies were fully implemented on the LIS,

---

13 HSE Update Report BN-18-11-244, 30 November 2018, 2-3.
14 The DPC agreed to a request for an extension to its original deadline of 30 October 2019.
15 HSE, 7 November 2019, 'DPC Enquiry Consolidated responses'.
16 HSE Response to DPC Draft Inquiry Report, 23 February 2021.

- examination of how compliance with ICT policies was achieved,
- examination of intrusion prevention and detection measures in place prior to the breach occurring,
- examination of the technical and organisational measures implemented as a result of the breach.

39. In particular, the Commencement Letter outlined that the Inquiry would involve an analysis of the breach reported to the DPC to determine if any contraventions of data protection legislation had occurred.

F. Issues for Determination

40. Having reviewed the Final Inquiry Report and the other materials provided during the course of this Inquiry, the DPC has determined the issues in respect of which it must make a decision. Those issues are whether the HSE complied with the following obligations in respect of the personal data of patients processed in the LIS and the associated backup systems at the Midlands Regional Hospital, Tullamore ('**the Patient Personal Data**'):

    - Articles 5(1)(f) and 32(1) GDPR, which require controllers to implement appropriate technical and organisational measures to ensure the appropriate security of the personal data;
    - Article 28 GDPR, which requires controllers to engage processors who put in place sufficient guarantees for the protection of personal data, and to put in place with processors a contract or other binding legal act addressing certain matters specified in that Article;
    - Article 30(1) GDPR, which require controllers to ensure that processing is in accordance with the GDPR, and to put in place a record of processing activities that contains the information specified in that Article;
    - Article 34(1) GDPR, which obliges the data controller, in the event of a data breach, to assess the risk to the rights and freedoms of data subjects from that breach and, if the risk is high, to communicate the breach without undue delay to those data subjects.

41. For the first three issues the DPC has determined that the temporal scope is between 25 May 2018 (the date when the GDPR took effect) and 14 November 2018 (the date of the cyber-attack) (the '**Temporal Scope**'). For the final issue, which relates to whether the HSE was obliged to notify data subjects after the cyber-attack, the temporal scope is from 14 November 2018 onwards.

G. Issue 1: Whether the HSE Infringed Articles 5(1)(f) and 32(1) in Relation to Patient Personal Data during the Temporal Scope.

42. Article 5(1)(f) GDPR sets out 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.

43. Article 32(1) GDPR elaborates on the principle of integrity and confidentiality. It sets out criteria for assessing what constitutes 'appropriate technical and organisational measures', stating:

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

44. Thus, Articles 5(1)(f) and 32(1) GDPR oblige controllers and processors to implement a level of security appropriate to the risks presented by their processing of personal data.

a) Assessing risk

45. In determining the appropriate technical and organisational security measures, a controller must assess the risk presented to the rights and freedoms of data subjects by the processing, and then assess what security measures must be implemented.

46. Recital 76 GDPR provides guidance on how this risk can be assessed:

> 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.

47. With respect to the nature, scope and context of processing, all of the processing operations that HSE carries out on the LIS personal data under its controllership relate to the provision of a laboratory diagnostic service for the MRHT and local GPs. As stated in paragraph 25 above, the HSE acts as controller in respect of tests ordered within the hospital and as a processor for those ordered by external GPs.

48. MRHT is the largest hospital in in the Midlands, with over 180 beds, out-patient facilities and a busy Emergency Department. It serves counties Westmeath, Laois, Offaly and Longford, with a combined population in 2018 of more than 292,000 persons. [17]

49. The LIS records and retains information in relation to diagnostic test requests. This information includes: patient name, patient address, patient ID, patient DOB, sex, clinical details: date/time of sample collection, date/time of receipt in the laboratory and date/time of report, specimen type, priority, results/reports, requesting clinician details and a record of communications relating to test results.[18] The nature of the personal data encompasses clinical data, which is special category health data, and commonly includes data of vulnerable individuals.[19]

50. The aggregate effect of these is to make clear that the processing for which appropriate technical and organisational measures were required in MRHT was extensive in terms the number of persons potentially affected and the types of activities that it served. The purposes served by the processing and the types of personal data processed were of high sensitivity and importance to the welfare of the persons concerned.

b) Likelihood of risk

51. The types of risk posed by the HSE's processing on the LIS system include delay or loss of access to personal data, as well as unauthorised access to or disclosure of it. The likelihood of these risks crystallising must vary according to the manner in which they occur.

52. Loss of access to data can occur where systems degrade or break down, as can happen when they are not properly maintained and kept up to date, or where an external event such as a power failure or disruption of a network takes place. The likelihood of these

---

17 See Midlands Regional Hospital Tullamore, HSE information page, available at https://www.hse.ie/eng/about/who/acute-hospitals-division/hospital-groups/dublin-midlands-hospital-group/our-hospitals/mrht/ (accessed 18 February 2025). See also, *Statistical Yearbook of Ireland, 2018*, Central Statistics Office.

18 HSE Update Report BN-18-11-244, 30 November 2018, 5.

19 Breach Notification Form, 16 November 2018, 4-5.

can range from a medium degree of probability to a remote one, but will generally increase in line with the complexity of a system and the interdependence of its components. Related to this, the likelihood of risk affecting one part of a system will increase where another component on which it depends becomes more vulnerable. Technical and organisational measures to address such risks must therefore take account of not only the performance and operation of individual components, but of the entire system used in the data processing. The data controller should foresee and address a range of scenarios ranging from delays or inconvenience arising from maintenance tasks, to more serious losses of access caused by failure of or disruption to one or more central components.

53. Unauthorised access to or disclosure of personal data is a particular concern in systems such as the LIS, which processes large amounts of sensitive data that is critical for the health and wellbeing of data subjects. The likelihood of this risk varies from everyday mistakes, such as inadvertently mistyping the address for a message, to less common (though still foreseeable) risks such as deliberate intrusion by unauthorised persons, whether physically or online. Measures to address these risks, such as access controls, backup procedures and management protocols, must be periodically reviewed to identify patterns of events that may indicate vulnerabilities, as well as external sources that can give information on emerging threats or developments in best practices.

54. The DPC notes in this regard that, since at least 2016, ransomware attacks on healthcare facilities had significantly increased in frequency and severity. This trend was widely publicised in both health and IT publications.[20] The increased likelihood of this risk to the LIS system should therefore have been known to the HSE. The DPC finds that the likelihood of the risk was high.

c) Severity of risk

55. The personal data processed included special category data, including that of vulnerable persons. The risk arising from this processing of patients' personal data on the LIS included that an unauthorised person could gain access to patients' personal data, which would pose a high risk to the fundamental rights and freedoms of data subjects, including the possibility of identity theft and extortion.

---

[20] Healthcare IT News, 17 February 2016, 'Hollywood Presbyterian hack signals more ransomware attacks to come', https://www.healthcareitnews.com/news/hollywood-presbyterian-hack-signals-more-ransomware-attacks-come (accessed 20 February 2025). See also McCoy TH, Perlis RH. 'Temporal Trends and Characteristics of Reportable Health Data Breaches, 2010-2017', Journal of the American Medical Association. 2018;320(12):1282–1284.

56. A further risk was that having gained access, an unauthorised person could compromise the integrity or availability of patients' personal data, causing disruption to or interference with the medical care of data subjects, with potentially severe consequences.

57. Similarly, failure of or disruption to the operation of some or all components of the LIS system could interfere with patients' care and treatment.

58. Based on this analysis, the DPC assesses the severity of the risk to be addressed by the HSE's technical and organisational measures concerning the LIS to be high.

d) Technical and organisational security measures implemented by the HSE

59. The HSE provided details of the technical and organisational measures in place in the MRHT at the time of the breach.[21]

60. The HSE outlined the laboratory local area network ('**LAN**') infrastructure in MRHT as comprising:

- two relational database servers – one live ('**Primary DB Server**') and one failover ('**Secondary DB Server**');
- four client desktops which hosted the LIS-related analyser interface applications. The software for these applications was provided by an external software provider (**'the Software Provider'**);
- a Firewall; and
- a Network-attached storage (NAS) device and three external hard drives for backup storage.

61. The HSE outlined the technical and organisational measures in place at the time of the breach as follows:

- the physical server hardware was housed in secure locations with access restricted to authorised persons;
- access to the Laboratory servers and PCs on the domains involved was controlled by username and password restrictions. User access rights were managed using different levels of access within the domains. A secondary level of authentication was in place for the relational databases;

[21] HSE submission 22 October 2020, 2-3.

- An Anti-Virus ('AV') solution was deployed on the systems in the LIS. Physical access to the servers was restricted to authorised persons. Logging systems were in place to record logins to the system.
- Username and password restrictions were in place for access to the LIS applications.

62. The HSE provided details of several business continuity measures in place to maintain availability and resilience of their processing systems:

    - 'T-PATH-IT-011 .03- Procedure for Processing Samples in Biochemistry - Haematology - Coagulation - Microbiology and Histopathology during Planned & Unplanned Computer Down Time': This laid down a set of procedures to revert to a largely paper-based process to maintain service provision at times when computer systems were not available and
    - 'T-PATH-IT-019 .03 Laboratory System-Server-Database- Backup and Restoration Procedures': This detailed procedures for backing up the servers and databases to storage devices physically attached to the servers.

63. In relation to regular testing, assessment and evaluation of the effectiveness of the technical and organisation measures for ensuring the security of the processing, the HSE provided the following internal audit documents:

    - 'PPPG-T-QA-LP-006.06 – Internal Audit in the Pathology Department'; and
    - 'LIS Audit 2017 HAUD-PATH-2017-002'.

    These documents made reference to the two Standard Operating Procedure documents mentioned in paragraph 62 above, as well as 'T-PATH-IT-003.05 Procedure for Controlling Access to the [redacted] LIS and associated IT Infrastructure'.

64. None of the above documents mentioned any procedures for penetration testing or vulnerability scanning. With regard to business continuity, the risk of having backup devices directly attached to the servers (thus exposing them to malware infection and other lateral attacks) was not flagged as a concern.

65. In its submissions of 29 March 2019, the HSE stated that the LIS infrastructure

    > was not under the management of the HSE OoCIO. A third-party supplier [referred to in this Decision as **'the Infrastructure Provider'**] provided management and support of the LIS infrastructure from early 2000s. This operating model resulted

in no active oversight of compliance with HSE IT security policies as they evolved over the years.[22]

66. In relation to the technical measures in place in the LIS environment at the time of the breach, the DPC notes that in its breach notification, the HSE mentioned that the backup devices were directly attached to the servers and were exploited by the attack.[23] This hindered the HSE's ability to effectively and efficiently restore the data.

67. The notification also stated that, while there was a firewall in place, external connections on an unsecure port were still possible. The subsequent forensic analysis carried out by the External Cybersecurity Consultancy confirmed that this was the vector used by the attackers to gain access to the LIS. The report said:

> This incident occurred due to the fact that it was possible to connect to a server in the HSE lab over a Remote Desktop Connection from the internet. Attackers frequently spider and search for available remote desktop connections and attempt to access these. Remote Desktop is not considered safe to have accessible from outside of a secure network.
>
> A firewall or gateway protection should be setup to ensure remote desktop connections are not accessible to the internet. Remote Desktop should only be available for internal connections only.[24]

68. In correspondence with the DPC on 29 March 2019, the HSE relayed a response from the Infrastructure Provider which stated that it 'is not aware of any other measures such as multi-factor authentication'.[25] The absence of such controls would be a contributing factor to the attackers' ability to access the LIS network.

69. The External Cybersecurity Consultancy report also revealed that a weak and obvious password was configured for an administrator account on the Secondary DB Server, through which the ransomware was deployed. This account was used to access other devices on the network, including the Primary DB Server.[26] While the Infrastructure Provider monitored whether or not the Primary DB server was operational, there was no Intrusion Detection System (IDS) in place.[27] Therefore the Infrastructure Provider, and consequently the HSE, became aware of the attack only after the Primary DB Server went offline as a result of the encryption.

---

22 HSE submission 29 March 2019, 12.
23 Breach Notification Form, 16 November 2018, 3 and 5.
24 External Cybersecurity Consultancy - Forensic Analysis Report, 22.
25 HSE submission 29 March 2019, 12.
26 External Cybersecurity Consultancy - Forensic Analysis Report, 12.
27 HSE Update Report BN-18-11-244, 30 November 2018 7.

70. The HSE also stated in its breach notification that anti-virus /anti malware software was not up to date on the devices in the LIS. The External Cybersecurity Consultancy report also noted that one of the affected devices was running a Microsoft operating system that had not been supported July 2010. Devices running unsupported versions of operating system have been directly targeted in numerous high-profile cyberattacks such as the WannaCry attack in 2017.[28] The existence of such devices on the LIS network greatly increased the vulnerability of the system to attacks and consequently the risks to the rights and freedoms of data subjects.

e) Assessment of technical and organisational measures for security

71. Having considered the technical and organisational measures in place at the time of the breach, and taking into account the state of the art and the likelihood and severity of the risk posed by processing on the LIS, it is clear that the implemented measures were not appropriate to the risk.

72. Endpoint security flaws in the LIS placed the confidentiality of Patient Personal Data at risk. While the HSE stated that a firewall was in place, the absence of an intrusion detection and prevention system meant that the HSE had no knowledge of malicious activity until after the attackers chose to deploy the ransomware. An unsecured firewall port was enabled without any additional security feature such as multi-factor authentication (MFA).

73. Lack of adherence to strong administrator password policies presented an opportunity for the attackers to not only view and alter the state of the relational database (irrespective of whether or not secondary authentication was configured) but also to move laterally to and exploit several other devices on the network.

74. With regard to the volume and category of data processed by the HSE and the high level of risk, the DPC considers that a more secure method such as Agentless backup would have been more appropriate. The devices storing the database backups were not separated from the other devices. This architecture allowed the ransomware to infect the backup devices as well as the server, resulting in an inability to fully restore the database following the attack. The offsite backups to the facility in [redacted] were not maintained, resulting in loss of data.

75. In addition to lack of separation of the backup devices from the servers, the HSE failed to implement network segmentation separating the database from the client devices running the application used to access data. There also appears to have been no user-

[28] See Europol 'Wannacry Ransomware' (6 November 2017), at https://www.europol.europa.eu/wannacry-ransomware (accessed 13 January 2025).

right restrictions on the remote access account, thus allowing the attackers to infiltrate multiple devices on the LIS with a single set of credentials.

76. The DPC also noted that encryption at rest was not implemented on the LIS devices. Recital 51 GDPR states that personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection, as the context of their processing could create significant risks to the fundamental rights and freedoms to the data subjects. Both the European Union Agency for Cybersecurity (ENISA)[29] and the US-based Health Insurance Portability and Accountability Act (HIPAA)[30] recommend encryption at rest to protect health data from unauthorised access.

77. Furthermore, notwithstanding the lack of such measures, the volume and sensitive nature of the data should have warranted a more robust 'defence in depth' approach. The LIS environment was not subject to regular security oversight for some time prior to the breach.

78. To summarise, the inadequacies of the technical and organisational measures in place at the time of the breach included:

- ineffective intrusion detection and prevention systems;
- an unsecured remote access port enabled on the firewall without MFA;
- a weak and obvious administrator password on the Secondary DB Server through which the ransomware attack was initiated, which was then used to move to other devices on the network, including the Primary DB Server;
- a device with an unsupported operating present on the network;
- Anti-Virus not updated on some of the affected devices;
- sensitive data not encrypted at rest;
- a lack of adequate security testing, such as vulnerability scanning and penetration testing on the LIS environment;
- an absence of up-to-date off-site backups to successfully restore the data;
- a lack of effective centralised governance with regard to ongoing security audits.

---

29 ENISA Procurement Guidelines for Cybersecurity in Hospitals.

30 The HIPAA Journal, 'HIPAA Encryption Requirements - 2025 Update', available at https://www.hipaajournal.com/hipaa-encryption-requirements/ (accessed 13 January 2025).

Conclusion on Issue 1: The DPC finds that the HSE 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 operations carried out on the LIS. In correspondence to the DPC on 19 January 2026, the HSE concurred with the DPC's provisional conclusions to this effect as set out in the Draft Decision.

H. Issue 2: Whether the HSE Infringed Article 28 GDPR in Relation to the Patient Personal Data During the Temporal Scope.

79. Article 28 GDPR sets out obligations of the controller and processor concerning the data processing relationship between them. These include the following requirements:

- The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures to implement GDPR and protect the rights of the data subjects;[31]
- Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor;[32] and
- The parties have an agreement in writing that clearly establishes the relationship between the parties and includes provisions requiring the processor to process peronal data only in accordance with the controller's instructions, to ensure the confidentiality and security of the personal data, and related matters ensuring that processing complies with the standards mandated by the GDPR.[33]

80. The HSE outsourced maintenance of key components of the LIS to two external companies: the Infrastructure Provider, which provided and monitored the status of the system hardware and operating systems, and the Software Provider, which provided the client software interface. The DPC asked the HSE to provide details of its arrangements with these companies.

81. On 30 November 2019, in response to the DPC's request to identify 'any third-party contractor or processor with respect to [the HSE's] Lab System solution', the HSE identified the Infrastructure Provider and the Software Provider. In response to the DPC's question asking whether 'a written data processing agreement/contract or

---

31 GDPR, Article 28(1).
32 GDPR, Article 28(3)
33 GDPR, Article 28(9)

equivalent in place', the HSE stated 'Service Level Agreement in Place - Confidentiality Agreement in Place.'[34]

82. Having examined all information and materials submitted over the course of the inquiry, the DPC finds that the relationship between the HSE and those two companies was that of controller and processor. The DPC is of the view that normal maintenance of hardware and software would require engineers to log into systems that store personal data and move datasets from place to place during backups. This is clearly 'processing' as defined in Article 4(2) GDPR, and is done on behalf of the controller, bringing the relationship into the scope of Article 28 GDPR. A review of the HSE's contracts with the Infrastructure Provider and the Software Provider, and the conduct of the parties in relation to the LIS, indicates that those relationships were not governed in such a way as to demonstrate compliance with Article 28 GDPR.

a) The Infrastructure Provider

83. The HSE signed an 'On Site Hardware Maintenance Contract' with the Infrastructure Provider on 13 October 2017. The HSE identified this as 'the Service Level Agreement (SLA) between the MRHT Pathology Department and [the Infrastructure Provider]'.[35] The contract outlined the following maintenance services which the Infrastructure Provider would provide in relation to the equipment specified in the contract:

- call-outs between 8.30am and 5.30pm from Monday to Friday (excluding public holidays);
- response within 4 hours for Servers;
- on-site operating system support in the event of corruption;
- management of warranty support with [redacted]
- temporary replacement equipment in the event of machine failure;
- call track reporting via [redacted];
- telephone support for Windows Operating Systems; and
- Remote Managed Service Inclusive.

84. Specifically referring to viruses, the contract stated that the Infrastructure Provider:

> shall have no obligation to maintain or repair any Equipment which is affect [sic] by viruses, worms, Trojan horses, cancelbots, or other contaminants or any codes or instructions that may or shall be used to access, modify, delete, corrupt,

---

34 HSE Submission 30 November 2019, 6-7.

35 HSE submission 27 February 2019, 17.

> deteriorate, alter or damage any data, files or other computer programs used by the Customer.[36]

85. While the firewall is listed as one of the items of equipment covered by the contract, there is no evidence that the Infrastructure Provider's obligations in relation to the ongoing management of the device extended beyond those of a standard 'break and fix' agreement. In other words, the Infrastructure Provider's responsibilities included repairing or replacing defective elements of the system as the need arose, but did not extend to updating or enhancing security in line with changing standards or circumstances. In particular, there was no provision for updating and maintaining firewall rules or implementing effective intrusion detection and prevention systems.

86. On 24 April 2019, the HSE submitted a response from the Infrastructure Provider on this matter which stated that the Infrastructure Provider:

> do[es] not have policies/procedures for the management of MHRT infrastructure (including firewalls) as the support agreement is a break/fix contract rather than pro-active management and monitoring of the infrastructure.[37]

87. In relation to the technical measures in place to provide alerts on sign-in behaviour for the LIS environment, the Infrastructure Provider stated that there

> was no pro-active alerting on the MHRT infrastructure sign-in behaviour. [The Infrastructure Provider does] not monitor the MHRT infrastructure.[38]

88. The HSE issued a response to the Infrastructure Provider's claim on 24 February 2021:

> The HSE concede that the SLA and documentation surrounding the support arrangements in place were ill defined however it is not entirely accurate to contend that monitoring and management arrangements for the MRHT lab infrastructure were totally absent.
>
> Domain changes, firewall config, AV licensing, hardware purchasing and repair were handled via competent [Infrastructure Provider] engineers. Works not covered under the terms of the SLA were chargeable items and invoiced separate to the annual maintenance contract.
>
> The ransomware attack under investigation occurred on the 14th of November at 7:20 a.m. Immediately after the attack the HSE was notified by [the Infrastructure Provider] of the attack by way of phone calls to the designated laboratory IT Lead. They also notified the HSE that a service engineer from [the Infrastructure

---

36 HSE submission 27 February 2019, 21.
37 HSE submission 29 March 2019, 10.
38 HSE submission 29 March 2019, 12.

> Provider] had been dispatched to MRHT to assist. They were able to do this because they had monitoring software installed on the HSE servers which returned alerts to them regarding login behaviour. From the HSE perspective this call was 'normal' and fitted within the remit and responsibilities of [the Infrastructure Provider].
>
> It is beyond comprehension how [the Infrastructure Provider] can state that there was '…no proactive alerting on the MRHT infrastructure sign in behaviour…' when it was this exact process that discovered the attack. A process which the HSE contends [the Infrastructure Provider] were contracted to provide despite our inability to find contractual documentation explicitly referring to this function.[39]

89. It is clear that there were differences between the HSE's and the Infrastructure Provider's opinions on the level of support that was in place. While the Infrastructure Provider claimed that it did not monitor the LIS infrastructure, it was that company which alerted the HSE to the breach. The HSE stated that this constituted pro-active alerting of unusual sign-in behaviour. However, as noted in the original breach notification, the Infrastructure Provider became aware of the breach only when the Primary DB Server went offline. As was later discovered during the forensic investigation, the Primary DB Server was accessed by means of remote access from the Secondary DB Server. There did not appear to be any pro-active alerting of sign-in behaviour on the Secondary DB Server. In any event, the HSE refers only to monitoring software on the servers, but not to any preventative measures or technologies that could have repelled the attack before it moved laterally through the LIS network.

90. On 27 February 2019, the HSE submitted a letter from the Infrastructure Provider dated 24 May 2018 which outlined how the Infrastructure Provider proposed to ensure adherence to GDPR. Among other things, this stated that the Infrastructure Provider had 'prepared a Data Processor Agreement for customers where our role is as Data Processor.'[40] The DPC notes that:

    - the letter clearly stated that the Infrastructure Provider's 'adherence to GDPR is not sufficient for other organisations to meet their GDPR obligations';
    - it was a general letter sent to all the Infrastructure Provider's customers and it did not specifically identify the Infrastructure Provider acting as a Data Processor for the MRHT Pathology Department;

---

39 HSE Response to DPC Draft Inquiry Report, 23 February 2021, 4.

40 HSE submission 27 February 2019, 25-27.

- the purpose of the letter was to 'outline details of the customer data we have, what the nature of the data is, what purpose it is used for and how it is securely protected';
- the letter listed the data held and this data pertained to customer data, contract data and IT data of which the Infrastructure Provider itself would be a controller; and
- the letter made no references to the clauses required to be included in contracts between controllers and processors under Article 28(3) GDPR.

91. The DPC is of the view that the letter dealt only with the Infrastructure Provider's processing of personal data on its own systems and that there was a lack of sufficient guarantees in place around the maintenance role concerning server access and the storage and security of personal data on the HSE servers. The difference of opinion between the HSE and the Infrastructure Provider as outlined above highlights the absence of clarity and the need for robust documented processing agreements.

92. Although the Infrastructure Provider's letter of 24 May 2018 stated that the Infrastructure Provider had prepared a data processor agreement for customers where its role was that of a data processor, the HSE did not demonstrate that it had entered into such an agreement identifying the Infrastructure Provider as a Data Processor for the services it provided for the MRHT Pathology Department.

b) The Software Provider

93. The HSE provided the DPC with a copy of a software maintenance agreement dated 16 January 2018 between the MRHT Pathology Department and the Software Provider.[41] This describes the maintenance services that the Software Provider provided 'in relation to its Laboratory Information System'. It also provides that the Software Provider would review 'hardware requirements on an annual basis and provide advisory services to laboratory personnel in relation to recommended hardware requirements'.[42] The agreement stated that the Software Provider would 'strive to fix most problems by remote access to the customer site, where it [the Software Provider]'s policy was to abide by the customer's agreed remote access procedures'.[43]

94. The Final Inquiry Report concluded that this agreement was limited to the provision and maintenance of the three client desktop applications utilised by MRHT and did not make any provision for the security of personal data that might be accessed or otherwise

---

41 HSE submission 27 February 2019, 11.
42 HSE submission 27 February 2019, 11 and 12.
43 HSE submission 27 February 2019, 11 and 13.

processed during maintenance operations. The Final Inquiry Report also concluded that the three client software applications processed a significant amount of personal data including special category data by way of collection, recording, organisation, storage, consultation and disclosure by transmission of patients' laboratory results.

c) Assessment

95. The DPC finds that the HSE's agreements with the Infrastructure Provider and the Software Provider did not provide sufficient guarantees to implement appropriate technical and organisational measures to meet the requirements of the GDPR and ensure protection of the rights of data subjects. Therefore, the agreements did not meet the requirements of Article 28(1) GDPR.

96. The DPC finds that the HSE's agreement with the Infrastructure Provider predated the entry into effect of the GDPR on 25 May 2018 and was not subsequently updated to reflect the standards required after that date. It did not offer any guarantees relating to any appropriate technical or organisational measures in place at MRHT. It did not include any of the clauses required by Articles 28(3)(a) to (h) GDPR.

97. With regard to the agreement with the Infrastructure Provider, processing activities that should have been governed by a contract or other binding legal act included access to, operation and system-level protection of databases and information; operation, design and protection of backup architecture and protocols, disaster recovery procedures in the event of security incidents and the updating of anti-virus software on the HSE servers. The DPC finds that the lack of a written contract governing these activities contravened Article 28(9) GDPR.

Conclusion on Issue 2: The DPC finds that the HSE infringed Articles 28(1), (3) and (9) GDPR by failing to use only processors providing guarantees to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its processing of Patient Personal Data and by the lack of sufficient binding written agreements and procedure documentation relating to their processing arrangements.

I. Issue 3: Whether the HSE Infringed Article 30 GDPR in Relation to Patient Personal Data During the Temporal Scope.

98. Article 30 GDPR requires controllers to maintain a Record of Processing Activities under its responsibility. While neither specifically include the words 'Record of Processing Activities' in their title, the HSE submitted two documents[44] which, it claimed,

[44] MRHT Laboratory Data Protection SOP and Procedure for Controlling Access to the [redacted] LIS and associated IT Infrastructure.

constituted a 'clear record... of who had access to what data and how that data was further processed'.[45]

99. The DPC noted during the inquiry that the formal approval date for these documents was 23 November 2018,[46] which post-dated not only the introduction of the GDPR but also the breach itself, though the HSE stated that the documents 'existed in draft format prior to the breach'.[47] In addition, while the documents contained some of the information required under Article 30(1) GDPR, other required information was absent, specifically contact information for the Data Protection Officer, retention periods and categories of recipients to whom personal data may be disclosed.

100. The DPC concurs with the findings of the inquiry that there was no formal Article 30 Record of Processing Activity in place at the time that the breach occurred on 14 November 2018, and that the lack of a GDPR-compliant Record of Processing Activity that was contemporaneous with the processing activities undertaken by MRHT at the time of the breach was an infringement of Article 30(1) GDPR.

Conclusion on Issue 3: the DPC finds that the HSE infringed Article 30(1) GDPR by failing to have in place a Record of Processing Activity compliant with the requirements of that Article at the time of the breach.

J. Issue 4: Whether the HSE Infringed Article 34 GDPR in Relation to Patient Personal Data During the Temporal Scope.

101. Article 34(1) GDPR provides:

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

102. In its initial notification of the breach,[48] the HSE assigned a medium risk to the breach and maintained this position throughout the Inquiry and in its submissions on the Draft Inquiry Report.[49] In the breach notification submitted on 16 November 2018, the HSE stated that

---

45 HSE Response to DPC Draft Inquiry Report, 23 February 2021, 3.
46 MRHT Laboratory Data Protection SOP, 2.
47 HSE Response to DPC Draft Inquiry Report, 23 February 2021, 3.
48 Breach Notification Form, 16 November 2018, 3.
49 HSE Response to DPC Draft Inquiry Report, 23 Feb 2021.

there is no evidence that data was removed or has fallen into unauthorised hands. The data has been encrypted by the ransomware virus only.[50]

103. In its reply to the Commencement Notice on 7 November 2019,[51] the HSE listed the following as reasons for its decision to rate the risk posed by the breach as 'Medium':

- The nature of the breach (ransomware attack). Typically in this type of scenario, the attacker is not stealing the data, they are rendering it unusable.
- The type of information held on the lab (which included special category data).
- The number of individuals affected.
- The fact that there were some viable backups of the lab data which were unaffected.
- The fact that hard copy reports are sent to requesting clinician.
- There was no evidence at the time that the data was removed.
- The steps taken on confirmation of the attack which included:
    - Unplugging all the servers and workstation on the lab network;
    - Blocking the lab systems access to the HSE LAN via the firewall;
    - Isolating the HSE server that was connected to the lab system network;
    - Running a manual virus scan on the HSE server which was connected to the lab system network; and
    - Running a virus scan on the Tullamore network.

104. The conclusion of the Final Inquiry Report was that

> given the nature and scope of the processing of the special category data, and the malicious nature of the personal data breach, the HSE should have reassessed the potential risks to the rights and freedoms of the affected individuals as 'high' and that as a result this would have created an additional obligation on the HSE to communicate the circumstances of the breach as required by Article 34(1) of the GDPR.

---

50 Breach Notification Form, 16 November 2018, 3.

51 HSE, 7 November 2019, 'DPC Enquiry Consolidated responses', 5.

105. As notification of data subjects under Article 34 GDPR is required where a breach is likely to result in a high risk to data subjects, this section will assess whether the HSE's assessment of the risk as 'medium' was correct. If the risk was medium, then the requirement to notify data subjects would not have been triggered. If the risk was high, then the HSE should have notified data subjects.

106. Where the notification obligation is triggered, the notification must be made 'without undue delay.' An assessment of the risk must therefore be carried out promptly after the breach, in order to determine whether the notification obligation arises. The European Data Protection Board ("EDPB")'s guidelines on personal data breach notification say that

> immediately upon becoming aware of a breach, it is vitally important that the controller should not only seek to contain the incident but it should also assess the risk that could result from it. There are two important reasons for this: firstly, knowing the likelihood and the potential severity of the impact on the individual will help the controller to take effective steps to contain and address the breach; secondly, it will help it to determine whether notification is required to the supervisory authority and, if necessary, to the individuals concerned.[52]

a) Analysis of whether the HSE's risk assessment was appropriate in the circumstances of the breach

107. This section sets out the DPC's analysis of whether the HSE's risk assessment was appropriate, having regard to the nature of risk of adverse effects to data subjects, and the testing that was conducted to assess the risks that actually occurred.

i. Nature of risks

108. First, it is necessary to consider the nature of the risks to data subjects that could have arisen from the incident. The analysis below considers the risk of the lack of availability of data and the risks to the confidentiality of patient data arising from the breach.

109. In relation to the availability of data, the HSE stated that paper-based records are the primary source of information for clinicians using the LIS, and that the electronic copies served as a supplementary source. In its submission of 23 February 2021, the HSE elaborated on this:

> Samples arrive into the laboratory reception together with a written (paper based) form, filled in and signed by a relevant person with authority to request a test

[52] EDPB 'Guidelines 9/2022 on personal data breach notification under GDPR', para 101.

(consultant, house doctor, general practitioner etc.). The form is a traditional paper form with a main sheet and four carbon copies. Each copy is used for the different laboratory disciplines involved in the tests requested (as a single request may be for multiple tests in different disciplines of the laboratory).

Once the relevant data is transcribed from the form into the LIS, the sample is taken and processed by an operator/medical scientist in accordance with the relevant protocol for the tests requested. Most tests involve the use of automated analysers which use either internal processors or else externally attached processors to control the operation of the analyser and communicate with the operator of the analyser, finally reporting the result of the test as a numeric value either directly or through an independent computer. Once the LIS flags that a test is complete and a result available, it is reviewed by the relevant Lab personnel before being authorised and returned by way of a printed test result report to the requesting clinician.

In addition to the printed report, results are returned electronically to a general practitioner who has their own practice management system. In that case the test result is returned electronically to the GP practice and stored in their practice management system by the HSE's Healthlink system. A paper report is also returned in these cases.[53]

110. From this description, it appears that the LIS plays a significant role in the efficiency of returning sample tests, particularly in relation to the role played by the automated analysers. Therefore, the impairment of this function caused by the breach is likely to have had at least some detrimental effects on patient services.

111. In correspondence to the DPC on 25 January 2023 responding to the final report of the inquiry, the HSE added:

> An important element of the risk assessment carried out was that, in normal circumstances, the electronic record was only available for a limited period of time (90 days) after which it was not available to clinicians.[54]

112. Irrespective of whether the data on the LIS system was intended to be available to clinicians after 90 days, the data gap in the offsite backup referred to in paragraphs 8 and 74 above referenced data more than 90 days old. This indicates that the data remained on the database and was thus accessible by anyone, including unauthorised persons, with access to the database.

---

53 HSE Response to DPC Draft Inquiry Report, 23 Feb 2021, 2-3.

54 HSE email to DPC, 23 January 2023.

113. In its initial assessment of the breach, the HSE was of the opinion that viable backups of the affected data were available. Ultimately however, the HSE was unable to fully restore the database to its original state, as electronic records from June 2017 to November 2018 had not been backed up and so were not recoverable.

114. The DPC considered the risk that confidential information could have been accessed or extracted in the incident. In its submissions dated 23 February 2021 on the Draft Inquiry Report, the HSE maintained that the configuration of the SQL database mitigated this risk:

> The MRHT LIS is designed around a SQL Database structure. This SQL databases back-boning the LIS were protected by strong username and password restrictions (secondary to the domain account credentials the hacker exploited to instigate the breach). The structure of the SQL relational databases is highly complex consisting of multiple tables that need to be linked together to make sense. This is highlighted by the Database Schema.

115. In the context of the specific incident, SQL Server authentication would have been effective only as an extra line of defence if the attackers did not gain administrator level privileges on the Primary DB Server. It was clear from the outset that the attackers had administrator level privileges, as they were able to log into and run executables on the server (in this case, the encryption program). This was later confirmed by the forensic report. Therefore, the DPC does not consider that secondary SQL authentication provided a safeguard to the confidentiality of patient data in respect of the incident.

116. The DPC does not agree with the HSE's assertion that the structure of the SQL database is 'highly complex', and that this helped to prevent the risk posed by the breach being high. The HSE submitted a sample of the relational database schema on 24 February 2021. This showed that the database included a table called '[redacted] containing data capable of identifying individuals, such as patient name, age, and date of birth. The Primary Key of this table is a field named '[redacted], which acts as a Foreign Key for several other tables (referred to as [redacted]') such as '[redacted] and '[redacted][55] Other fields in this table are named '[redacted], '[redacted] and '[redacted]. These are commonly used acronyms for [redacted]', [redacted]' and '[redacted]'

117. Having viewed the schema, the DPC is of the opinion that it would not take a great deal of time or proficiency in relational database administration to combine and view these

[55] HSE Response to Draft Inquiry Report, 23 February 2021, Appendix 1 - LIMS database schema

tables using basic 'Join' commands.[56] The DPC is therefore of the view that fields containing personal data capable of identifying individuals, such as those stored in the [redacted] table and numeric data stored in the [redacted] tables, are linkable with reasonable facility.

118. In correspondence to the DPC on 25 January 2023, the HSE stated:

> the data itself whilst special category was not sensitive in nature as the majority of clinical data in a laboratory information system is numeric in nature and has no meaning until associated with the discipline involved and the patient.

119. Although the data were alphanumeric, they do not appear to have been particularly difficult to read. For example, in the schema provided to the DPC, one of the tables linked to the [redacted] table through the [redacted] field is named '[redacted]. In addition to the [redacted] foreign key, other fields in this table are named '[redacted], '[redacted] and '[redacted]. These are commonly used acronyms for [redacted]', [redacted]' and '[redacted]' Therefore, the alphanumeric nature of this data would not have pseudonymised that data sufficiently, as a motivated attacker could link it to identifiable data fields with only moderate effort.

120. As outlined in paragraphs 114 to 115 above, this avenue was open to the attackers once they had obtained administrator access to the server.

121. The EDPB Guidelines on breach notifications provide guidance on the circumstances under which data subjects should be notified:

> [N]otification of a breach is required unless it is unlikely to result in a risk to the rights and freedoms of individuals, and the key trigger requiring communication of a breach to data subjects is where it is likely to result in a high risk to the rights and freedoms of individuals. This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data have been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach involves personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, **data concerning health** or data concerning sex life, or criminal convictions and offences or related security measures, such damage should be considered likely to occur.[57]

---

[56] Microsoft.com, 'Joins (SQL Server)', available at https://learn.microsoft.com/en-us/sql/relational-databases/performance/joins (accessed 15 December 2024).

[57] EDPB 'Guidelines 9/2022 on personal data breach notification under GDPR', at paragraph 102. (Emphasis added).

122. Based on the preceding analysis, the DPC considers that the actual risks to data subjects arising from the incident included a risk that special category data – in this case health data – may have been viewed, altered, deleted or exfiltrated. This clearly comes within the ambit of high risk.

123. The HSE asserted that there was limited risk to patient services because of the existence of paper records. (The HSE did not quantify the reduction in risk that it considered that the paper records provided.) The HSE submitted that the purpose of the LIS system is to provide 'ease of access' for clinicians, who could still access all relevant data on the paper records. However, as noted in paragraph 110, automated tasks performed on the electronic data played a significant role in returning test results. It is the DPC's view that the LIS system being offline removed a more quick and convenient means of location and retrieval, which would have affected clinicians' ability to access patient data and, consequently had a potential adverse effect on the efficiency of patient services.

124. The HSE was also unable to restore all of the data due to the backup devices also being encrypted. Therefore, the DPC is of the opinion that there was a partial loss of availability of patient personal data as a result the breach. The fact that the database was not encrypted and not ultimately restored to its original state points to loss of integrity of the patient data.

125. In the light of these findings, the risks arising from the incident pertain to the confidentiality, integrity and availability of the patient data processed on the LIS.

ii. Post-incident testing and risk analysis

126. The HSE's risk assessment took into account risks to special category personal data and the risk of extraction. The HSE's breach notification stated 'Typically in this type of scenario, the attacker is not stealing the data, they are rendering it unusable'. The DPC cannot see how there was sufficient empirical evidence to arrive at this conclusion immediately after the breach was discovered. Due to the LIS devices being encrypted, the HSE was unable to sufficiently triage the breach to estimate how long the attackers had access to its network. The DPC also bears in mind that in May 2021, the HSE was subjected to another ransomware attack. A report on that incident confirmed an eight-week interval between the network being compromised and deployment of ransomware.[58] The report also confirmed that data was extracted in that time. This indicates that it is entirely possible in an incident of this nature that hackers could have

[58] HSE, 'HSE – Independent Post Incident Review', 3 December 2021, 2.

access to a system and engage in malicious activity long before they deploy ransomware.

127. In its response to the Draft Inquiry Report dated 24 February 2021, the HSE provided further information about its immediate response to and assessment of the breach:

> One of the immediate post shutdown actions was to check the possibility that data had been removed from the HSE environment. To do this our own network people checked network usage…... the HSE had conducted its own investigations and on the 15th of November, prior to issuing the breach notification on the 16th had determined that there was no evidence to show that a 150 Gb+ database file had been copied out of the Hospital network.

128. The HSE also provided internal email correspondence on the day of the breach, which stated:

> From our [redacted] (network management software) there is no real change in baseline traffic and actual traffic up to the time of the event on NHN thus giving credibility to us saying that the DB was not copied over NHN anywhere.[59]

129. While this offers some assurance that large-scale extraction of data did not occur, it does not rule out the possibility that unauthorised viewing of the data took place. Additionally, the correspondence quoted above gives no details of the duration of time during which the network traffic was monitored.

130. It was apparent at the time of discovery of the breach that the attackers had obtained administrator access to the database servers. As a result, they could query the database directly. It would also have been feasible for them to export and extract data into smaller file types such as .xls or .csv. Transmission of these files would be harder to detect solely by monitoring network traffic. These are plausible possibilities because, at the time when it first assessed the breach, the HSE had no way to accurately estimate how long the attackers had access to the LIS environment.

131. The absence of an intrusion detection system, coupled with the enabling of a remote access port on the firewall, meant that the attackers were able to act without being detected until they deployed the ransomware, causing the server to cease operation. In correspondence to the DPC on 29 March 2019, the HSE stated that firewall logs were not reviewed by the Infrastructure Provider in the immediate post-incident investigation.[60]

---

59 HSE internal email 'Potential Major Incident - i31733 - Ransomware issue with Tullamore LAB server', 22 February 2021.

60 HSE submission 29 March 2019, 14.

132. The External Cybersecurity Consultancy's investigation into the incident sought to establish further facts on the attack, particularly in relation to the vector employed and the scope of the attackers' activities. However, the DPC notes that, of the five devices encrypted in the attack, only four were examined by the External Cybersecurity Consultancy. The encrypted device that was not examined has been identified as the Primary DB Server. Examination of this server could have shown whether it had been affected by malicious activity. It is also possible that the event logs were erased from this server, but in the absence of an examination, it is impossible to know. The failure to forensically examine this server is thus a material omission from the post-incident investigation.

133. The External Cybersecurity Consultancy was specifically asked to confirm if HSE data was viewed or extracted during the attack.[61] Its response was:

> It is difficult to state conclusively whether HSE data was viewed by the hackers or not. Many records have been lost by the encryption process… no evidence of file viewing was found, but the number of records available to check this was minimal.
>
> While no evidence of data exfiltration was found, it cannot be conclusively ruled out due to lack of available evidence.

134. The External Cybersecurity Consultancy report also stated that the device operating system does not record files copied over the unsecured remote access protocol, which was the vector employed by the attackers. The report noted that the attackers regularly cleared the logs of all devices during their operation, thus obscuring much of their footprint. The encryption process purged most of the log files, which would give a clearer picture of file-viewing activity.

135. The External Cybersecurity Consultancy also endeavoured to estimate a timeline of the attackers' activities. As previously stated, much of the logging information was purged during the incident. The surviving logging information was used to estimate the timeline. A summary of the remaining logs for 14 November 2018 are detailed in the table below:

---

[61] External Cybersecurity Consultancy- Forensic Analysis Report, 4-5.

Time	Device	Log type	Activity
07:20:30	[redacted]	Registry	Outbound remote desktop connection made to [redacted] ([redacted] using username [redacted]
07:25:02	[redacted]	Registry	Outbound remote desktop connection made to DSKML06071 (MK01) using username [redacted]
07:25:03	[redacted]	Registry	Outbound remote desktop connection made to ([redacted] using username [redacted]
07:29:36	[redacted]	Registry	Outbound remote desktop connection made to [redacted] using username [redacted]
07:36:39	[redacted]	Registry	[redacted] file for [redacted] indicates inbound Remote Desktop Connection using the clipboard
07:37	[redacted]	Registry	[redacted] shows the Remote Desktop executable mstsc.exe was last run at this time
07:37:46	[redacted]	Registry	Incoming remote desktop connection from [redacted] ([redacted] using username [redacted]
07:40:34	[redacted]	Registry	Remote desktop session disconnected
07:41:22	[redacted]	Registry	Outbound remote desktop connection made to [redacted] using username [redacted]
07:43:26	[redacted]	Event Log	Remote Desktop session from Panama IP of [redacted] disconnects

136. The earliest available information was a registry log describing an outbound RDP connection from the Secondary DB Server (referred to in the above table as MK04) at 07:20, implying that the LIS network was breached prior to that point in time. It is important to note that the majority of remaining logs are in the form of Registry key modification dates. These record only the most recent modification of the key or sub-part of the key. They are not the most reliable records for determining in full the attackers' activity in the LIS environment, as they do not show intervening modifications or access to the files. The External Cybersecurity Consultancy alluded to this fact in their

report.[62] As the record of each modification is overwritten by any subsequent modification to the file, there is no way of determining from these records when the attackers first gained access to the LIS network or for how long they were active.

137. The DPC also notes that the time of disconnection from the remote session from the Panama IP address was recorded, but the time of the initial connection was not. It is likely that this record was purged when the attackers cleared the event logs after deploying the ransomware. This raises a reasonable doubt to the HSE's assertion that 23 minutes was indicative of the length of time during which the attackers were active in the LIS environment.

b) Summary and conclusion on risks arising from these measures

138. Article 34 GDPR requires notification to data subjects where a personal data breach is likely to result in a risk to their rights and freedoms.

139. As set out above, the DPC considers that the incident gave rise to risks to the confidentiality, integrity and availability of patient personal data. The lack of reliable evidence of the duration of the incident and the possibility that selective extraction took place mean that it is not possible for the HSE to demonstrably determine from the evidence collected in the Inquiry whether or not the confidentiality of patient data was compromised. While this lack of evidence is due in part to the attackers deleting, overwriting and encrypting data, the HSE must share responsibility for this lack of information. It did not have an intrusion detection system in place and firewall logs were not examined, which meant that it did not know that attackers had access to the system until it went offline.

140. Some aspects of the HSE's risk assessment do not stand up to scrutiny. The HSE concluded that ransomware was the sole purpose of the attack despite having insufficient knowledge of how long its network had been compromised and the attack vector employed. Therefore, on the basis of the facts available, the DPC sees no basis to conclude that that the HSE fully assessed the implications of the attackers acquiring administrator privileges on its devices, particularly the relational database servers, and the associated risk that special category personal data could have been viewed or extracted from that database.

141. Over the course of the Inquiry, the HSE referred to the External Cybersecurity Consultancy's report to support its assessment of the risks posed by the breach. However, as outlined above, that report specifically stated that the External Cybersecurity Consultancy could not rule out the possibility that patient data was

---

[62] External Cybersecurity Consultancy- Forensic Analysis Report, 19.

viewed or extracted. The External Cybersecurity Consultancy did not examine the Primary DB server and could not establish a complete timeline of the attackers' activities due to incomplete logging information.

142. In its response to the Inquiry Report on 24 February 2021, the HSE stated:

> in the short time the attack happened, later confirmed to be 23 minutes, there is no evidence to show that the database management system itself was breached in such a way as to make the database schema available to an attacker.[63]

143. As outlined in paragraphs 137-139, the External Cybersecurity Consultancy report does not support the conclusion that the timeframe of the incident was limited to 23 minutes. Having examined that report, and noting that the Primary DB server was not forensically examined, the DPC is of the opinion that the lack of evidence to which the HSE refers was caused by the attackers purging logging information that might have provided a clearer picture of their activity.

144. The HSE also stated:

> The modus operandi of the ransomware variant involved in the breach is encrypts files – [the External Cybersecurity Consultancy] testing confirmed no network activity or attempts to store or export data were associated with this variant.[64]

145. While this is true in relation to the behaviour of the ransomware variant, this was only one of three methods of data viewing or extraction that the External Cybersecurity Consultancy considered in its report. As outlined earlier, in the absence of records that were purged or overwritten during the attack, the report concluded that it could not conclusively rule out file viewing or extraction.

146. The DPC acknowledges that there is no direct evidence that the attackers viewed or extracted data, and that the deletion of the Event logs prevented the HSE from easily establishing whether that had occurred. The DPC also acknowledges that testing for selective extraction in the absence of these logs would be very difficult, and that the HSE conducted tests for bulk extraction, which ruled out the possibility that a large single file was copied.

147. Nevertheless, the absence of clear evidence ruling out viewing or extraction of data leaves a significant residual doubt as to whether confidentiality of patient data was compromised. The DPC therefore must consider the actual likelihood of confidentiality

---

63 HSE Response to DPC Draft Inquiry Report, 23 February 2021, 5.

64 HSE Response to DPC Draft Inquiry Report, 23 February 2021, 8.

being compromised. If it is likely that confidentiality was compromised, this would indicate a high risk to data subjects and require notification under Article 34(1) GDPR.

148. The EDPB guidelines 9/2022 on personal data breach notification under GDPR point out that, in line with Recitals 75 and 76 GDPR, controllers must consider the likelihood and severity of risk to determine whether the risk posed by a breach is high. Where it is found to be high, data subjects must accordingly be notified.

149. The severity of the risk to data subjects arising from access to the data was high. The attackers had access to a relational database from which it was possible within reasonable means to view and extract special category personal data such as clinical test results.

150. Controllers must assess the likelihood of the risks on the basis of the information available at the time of, or shortly after, the breach. In this case, while subsequent investigations by the External Cybersecurity Consultancy and the HSE do not indicate that patient personal data was viewed or extracted during the attack, it is important to bear in mind the purpose of the requirement to notify under Article 34 GDPR. That purpose is to enable data subjects to respond and protect their rights and freedoms to the fullest extent possible. This necessarily requires the notification to be made at the earliest opportunity. Controllers must notify data subjects 'without undue delay', so the likelihood of risk should have been assessed at the time of the breach on the basis of the evidence then available.

151. Anyone with administrator access to the entire database would have been able to retrieve details of test results about any particular patient. Retrieving such details would have involved a number of steps to link the data across different tables, but it would have been possible, within reasonable means, for the attackers to do this while they were in the system. It also would have been possible to do this if data were extracted in bulk.

152. The HSE took prompt action to check for significant spikes in network traffic preceding the incident. While this goes some way to reassuring that bulk extraction of the database did not take place, it does not, as outlined in paragraph 141, rule out the possibility that exfiltration or viewing of data of any kind did not occur.

153. The HSE also did not recognise that the attack resulted in reduced availability of patient data. The HSE claimed that the existence of paper records negated concerns about the availability of patient data despite stating that the purpose of the LIS was to provide

'ease of access' for clinicians. In this regard, the DPC notes that in January 2023, a senior HSE official stated to an Oireachtas Committee that paper records were 'inefficient'.[65]

154. While it cannot be conclusively stated that individual records were amended while the attackers had access to the LIS environment, the very nature of a ransomware attack is to alter the state of the database so as to render it unusable. This signifies a risk to the integrity of patient data.

155. ENISA has provided a recommended methodology on assigning level of severity to data breaches.[66] The severity level (SE) is determined by the formula:

Data Processing Context × Ease of Identification + Circumstances of the breach

Where SE is between 3 and 4, the guidelines recommend that a high severity be assigned and a 'very high' risk for any rating greater than 4.

156. For Data Processing Context, ENISA recommend that a base score of 4 be assigned to special category personal data such as health data. Additional details such as the volume of data affected and special characteristics of the data controller are seen as increasing factors for this score.[67]

157. A score of 1 is assigned to Ease of Identification if the data subject can be easily identified. In the case of this breach, a data subject's full name, address and date of birth were viewable in the Demographics table of the LIS database as per the schema provided by the HSE.

158. Circumstances of the breach is calculated on four factors: Loss of confidentiality, Loss of integrity, Loss of availability, and whether malicious intent was involved. Loss of confidentiality is scored at 0 if data is exposed to confidentiality risks but without evidence that illegal processing has occurred. In the circumstances of this breach a score of 0 is therefore appropriate.

159. Loss of integrity carries an additional score of 0.5 if the original data cannot be recovered. In the DPC's view, this is the appropriate weight in this case irrespective of whether paper records existed. The HSE ultimately could not restore the electronic data to its original state.

---

65 Irish Independent, 'Healthcare is held back by paper-based records as funding yet to be approved for switch to electronic system', 25 January 2023.

66 ENISA, 'Recommendations for a methodology of the assessment of severity of personal data breaches', v.1.0, December 2013.

67 ENISA, 'Recommendations for a methodology of the assessment of severity of personal data breaches', v.1.0, December 2013, Annex 1.

160. Loss of availability carries an additional score of 0.25 in the case of temporal unavailability, i.e. where the information can be retrieved from other sources. In this case, the existence of paper records is relevant. Finally, an extra score of 0.5 is applied if malicious intent was involved, which is clearly the case for this breach.

161. Applying this methodology, the overall score is 6.25, which is above the threshold for a high severity breach. Taking this into account, as well as the DPC's evaluation of the HSE's reasoning for their classification of the breach, the DPC does not accept that 'medium' was an appropriate risk rating for this breach. Taking into account the scale of the risk, in terms of the number of affected data subjects, and the special category personal data affected, the DPC is of the view that the HSE should have assigned a high risk rating to the breach.

c) Assessment of the HSE's Media Communication

162. Article 34(2) GDPR states

> The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

163. The measures in Article 33(3) referred to above require that the notification should at least:

> communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
>
> describe the likely consequences of the personal data breach;
>
> describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

164. Article 34(3) GDPR provides three limited exceptions to the requirement to communicate details of a breach assessed to pose a high risk:

> The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
>
> (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

165. The exception in Article 34(3)(a) GDPR does not apply because the personal data accessible (and so potentially disclosed to the attackers) were not encrypted by the HSE or otherwise rendered unintelligible to unauthorised persons.

166. Similarly, the exception in Article 34(3)(b) GDPR does not apply. As noted in paragraph 133 above, the External Cybersecurity Consultancy's forensic analysis could not exclude the possibility that the attackers exfiltrated data from the LIS before encrypting it and cutting off contact. As the attackers, and their conduct with any personal data they may have exfiltrated, were entirely outside the control of the HSE, nothing that the HSE could have done would have reduced the risks posed by such possible exfiltration, or rendered them unlikely to materialise.

167. Article 34(3)(c) applies where communicating the breach directly to data subjects 'would involve disproportionate effort'. The DPC notes in this regard that the records of approximately 84,000 persons were affected by the breach. Given the large number of data subjects, and the need to communicate 'without undue delay', the DPC accepts that individual communication would have involved disproportionate effort in this case. As prescribed by Article 34(3)(c), 'a public communication or similar measure whereby the data subjects are informed in an equally effective manner' was therefore required.

168. The DPC notes the efforts made by the HSE to publicise the breach. In its submission on 23 February 2021, the HSE stated:

> [T]he HSE took part in numerous public communications events, both print and radio, in order to explain and assure the people affected. Appendix 2 gives further details of these interactions.[68]

169. The 'Appendix 2' referred to by the HSE ('Media Communications' for the purposes of this document) includes articles and segments from print and broadcast media outlets on Thursday 15 November 2018,[69] the day after discovery of the breach. The HSE is quoted as describing the incident as an 'isolated Windows ransomware attack'. Extracts from the statement, as quoted by numerous print media outlets state:

---

68 HSE Response to DPC Draft Inquiry Report, 23 February 2021, 2.

69 The HSE did not submit to the DPC the press release that it provided to media outlets.

The hospital has been assured that this is an isolated incident and there is no evidence of contagion in the wider health service beyond the initial attack. The hospital has been working in conjunction with the HSE Office of the Chief Information Officer to restore the system and re-instate a functional Laboratory Information System within a re-configured secure HSE environment. There has been no impact on patient care and business continuity plans are in operation until the full system is restored. The HSE have informed the Data Protection Commission on a precautionary basis.

170. The HSE submitted to the Inquiry that, during the week after discovery of the breach, a HSE spokesperson also granted an interview to the radio station Midlands 103 **('M103').** The spokesperson stated that the fall back to paper-based records meant that there was no interruption to patient care. M103 asked for further clarity on the security of patient data. The following is a transcript from that segment of the interview:[70]

M103: ...to confirm, there is no threat to any patient's information, their date of birth, emails that may have been hijacked or hacked?

HSE: Not that we are aware of at this point in time.

M103: But you can't give 100% certainty that that has not happened.

HSE: At this point in time I have no information to state that that has happened. It is important to point out that at this point in time, our Laboratory Information System is 80% fully recovered and with ongoing works that will happen throughout today, it is expected that we will have our Laboratory Information System fully restored by the afternoon.

M103: And when do you expect to be able to tell patients that their information is 100% secure?

HSE: I will rely on the Office of the Chief Information Officer to provide me with that assurance.

Later in the interview the following exchange took place:

M103: And when will you issue a statement or update to reassure patients?

HSE: We can issue statements throughout the day but at this point in time, I can assure our patients and the public that there has been absolutely no impact on patient care and we will continue to maintain that.

---

70 Recording of interview available at https://soundcloud.com/benfinnegannews/manager-of-tullamore-hospital-on-ransomware-attack. The quoted extract is at 1:30 to 2:24 of the recording.

171. While it is commendable that the HSE took prompt action to publicise the breach and inform the public of its efforts to address the breach and mitigate the adverse effects, there was no attempt to communicate the name and contact details of the data protection officer or other contact point for the public to get further information.

172. The DPC understands that the incident was still under investigation at the time of these media statements and that the public should have been informed of updates as more information was made available. The HSE did not make any further statements on the incident. This is concerning for the following reasons:

- Despite the assurances given in the M103 interview, the LIS data was not fully restored, i.e. that personal data had been irrecoverably lost.
- The forensic report did not conclusively rule out the possibility that data was viewed and/or extracted.

173. As concluded by the Inquiry Report, a high-risk rating requires the HSE to communicate the circumstances of the breach pursuant to Article 34(1) GDPR. The DPC finds that, following a proper assessment of the breach, a high risk to the rights and freedoms of 84,000 data subjects should have been identified and that the HSE's failure to communicate fully all required information relating to the breach to those affected data subjects is a contravention of the provisions of Article 34(1) of the GDPR.

d) Conclusion on Issue 4:

174. The DPC finds that the HSE infringed Article 34 GDPR by failing to fully communicate to the affected data subjects without undue delay the following information relating to the breach:

- that patients' personal data had been irrecoverably lost,
- that a forensic examination of the breach could not rule out that patients' personal data had been accessed or exfiltrated, and
- the name and contact details of the HSE's data protection officer.

K. Decision on Corrective Powers

175. The DPC has set out above, pursuant to section 111(1)(a) of the 2018 Act, its decision that the HSE has infringed Articles 5(1)(f), 28(1), 28(3), 28(9), 30(1), 32(1) and 34 GDPR. Section 111(2) of the 2018 Act provides that, where the DPC makes a decision under section 111(1)(a), it must, in addition, make a decision as to whether a corrective power should be exercised in respect of the controller or processor concerned and, if so, the corrective power to be exercised. The remaining question for determination in this Decision is whether those findings merit the exercise of any of the corrective powers set out in Article 58(2) GDPR and, if so, which corrective powers.

176. Recital 129 GDPR assists in the interpretation of Article 58. It says in respect of the corrective powers exercised by supervisory authorities:

> … 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 ….

177. In the circumstances of this Inquiry, and with particular reference to the findings of infringements set out above, the DPC finds that the exercise of one or more corrective powers is appropriate, necessary and proportionate for the purpose of ensuring compliance with the GDPR.

178. Having carefully considered the infringements identified in this Decision, the DPC has decided to exercise the following corrective powers in accordance with section 115 of the 2018 Act and Article 58(2) GDPR:

- An order to bring its processing into compliance fine in respect of the infringements of Articles 5(1)(f) and 32(1) GDPR.
- A reprimand to the HSE in respect of its infringements of Articles 5(1)(f), 28(1), 28(3), 28(9), 30(1), 32(1) and 34 GDPR.
- An administrative fine in respect of the infringements of Articles 5(1)(f) and 32(1) GDPR. The reasons for this are outlined below.

179. The DPC sets out below further detail in respect of each of these corrective powers that it has decided to exercise and the reasons why it has decided to exercise them.

L. Order for Compliance

180. Article 58(2)(d) GDPR provides that a supervisory authority shall have the power to 'order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period.' The DPC orders the HSE to bring its processing into compliance with the GDPR in the terms set out in paragraphs 182 to 186 below.

181. The DPC's decision to impose this order is to ensure that full effect is given to the HSE's obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk posed by the HSE's processing. In deciding that an order is appropriate to achieve this end, the DPC has had particular regard to the high quantity of highly sensitive personal data processed by the HSE. The HSE must perform the necessary risk assessment to inform the measures that it must implement.

182. The HSE is required to ensure that appropriate technical and organisational measures are in place to protect the personal data processed in the LIS to satisfy Articles 5(1)(f) and 32(1) GDPR, with specific regard to the elements of its National Cybersecurity Plan not yet implemented as at the date of this decision.

183. The HSE has outlined measures implemented since 2021 as part of its National Cybersecurity Plan (NCSP) which have rectified many of the cybersecurity deficiencies which led to the Breach. The LIS environment has now been incorporated into the HSE's National Data Centre. Unsecured firewall ports have been disabled and MFA has been applied for remote access. A new Backup policy has been implemented.[71]

184. In correspondence with the DPC on 16 March 2026, the HSE provided details on the timeline for the remaining action points of its National Cybersecurity Plan. These are

- Migrating the LIS into the National MedLIS solution (2026)
- Managed Threat Detection & Response Service (2026)
- Extended Detection & Response Service (2026)
- Digital Risk Protection Service (2027)
- Unified Cyber Incident Response Service (2027)
- Cyber Governance, Risk, Compliance and Resilience Capability (2027)
- Third Party Risk Management Service (2027)
- Cyber Awareness and Training Platform (2027).

185. To ensure compliance with the GDPR, the HSE must keep the DPC informed of the progress of these projects. It must be noted that implementing these measures does not relieve the HSE of its obligation to continually evaluate the effectiveness of the measures that it puts in place to ensure compliance with the GDPR.

186. The DPC imposes a deadline of 31 December 2027 for the HSE to comply with the measures specified above. The DPC further requires the HSE, on the expiry of that deadline, to submit a report to the DPC outlining the steps it has taken to comply with those measures.

M. Reprimand

187. 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.

[71] HSE response to DPC queries, 16 March 2026.

188. The DPC issues a reprimand to the HSE in respect of all the infringements identified in this Decision. The purpose of the reprimand is to dissuade non-compliance with the GDPR:

- The infringements of Articles 5(1)(f) and 32(1) GDPR contributed to a higher risk of unavailability of patient data and a possible lack of progression of medical care, with an ongoing risk to patient health. There was also a risk of disclosure of patient data to unauthorised third parties.
- The infringements of Article 28 GDPR demonstrate a failure on the part of the HSE to properly assess and, where required, adapt its processing arrangements to comply with the heightened standards imposed by the GDPR.
- The infringement of Article 30 GDPR similarly reflects a failure by the HSE to fully assess and document its processes and procedures to ensure that it could demonstrate compliance with the GDPR.
- The failure to fully communicate all information required under Article 34(1) may have distressed or inconvenienced data subjects affected by the breach.
- The DPC considers 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 contributes to ensuring that the HSE 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, the proper management of processing contracts and communication of information about breaches to data subjects.

N. Decision on Administrative Fines

189. 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.

190. The purpose of administrative fines is to strengthen the enforcement of the rules of the GDPR.[72] Fines sanction non-compliance and seek to re-establish compliance with the GDPR.

---

[72] GDPR, Recital 148.

191. As the DPC has identified infringements of the GDPR above, the DPC will decide whether to impose administrative fines in respect of those infringements. In conducting this assessment, the DPC has had regard to Article 83 GDPR, which sets out 'General conditions for imposing administrative fines.' The DPC has also had regard to EDPB guidelines, which are designed to ensure a harmonised approach to fining. These include the EDPB's Guidelines on the calculation of administrative fines (the EDPB Fining Guidelines), and the Article 29 Working Party's Guidelines on the application and setting of administrative fines (the A29WP Fining Guidelines), which have been endorsed by the EDPB. [73]

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

a) Whether to impose an administrative fine

193. Article 83(2) GDPR states,

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

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

---

[73] EDPB, 'Guidelines 04/2022 on the calculation of administrative fines under the GDPR', Version 2.1, adopted 24 May 2023; Article 29 Data Protection Working Party, 'Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679', WP 253, adopted on 3 October 2017, endorsed by the EDPB on 25 July 2018.

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

195. Article 83(2)(a) requires consideration of the identified criteria by reference to 'the infringement' as well as 'the processing concerned.' The phrase '**the processing concerned**' in this Article 83(2) analysis should be understood as meaning all of the processing operations that HSE carries out on the LIS personal data under its controllership.

196. Considering next the meaning of 'infringement', it is clear from Articles 83(3)-(5), that 'infringement' means an infringement of a provision of the GDPR. Above, HSE was found to have infringed Articles 5(1)(f) and 32(1) GDPR, Article 28 GDPR, Article 30 GDPR and Article 34 GDPR. Thus, '**the infringement**', for the purpose of the DPC's assessment of the Article 83(2) criteria, should be understood (depending on the context in which the term is used) as meaning an infringement of Articles 5(1)(f), 28(1), 28(3), 28(9), 30(1), 32(1) and 34 GDPR. While each is an individual 'infringement' of the relevant provision, they all concern the processing concerned and, by reason of their common nature and purpose, are likely to generate the same, or similar, outcomes in the context of some of the Article 83(2) assessment criteria. Accordingly, and for ease of review, the DPC will assess all of these infringements simultaneously, by reference to the collective term '**infringements**' unless otherwise indicated.

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

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

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

199. The **nature** of the processing can include:

> the context in which the processing is functionally based (e.g. business activity, non-profit, political party, etc.) and all the characteristics of the processing."[74]

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

> where the purpose is to monitor, evaluate personal aspects or to take decisions or measures with negative effects for data subjects, where there is a clear imbalance between the controller and data subjects or where the processing involves children or other vulnerable data subjects.[75]

201. The nature of the processing relating to the infringements identified herein is the recording and retaining of information in relation to diagnostic test requests on a hospital laboratory information system.

202. The **scope** of the processing is assessed

> with reference to the local, national or cross-border scope of the processing carried out and the relationship between this information and the actual extent of the processing in terms of the allocation of resources by the data controller… The larger the scope of the processing, the more weight the supervisory authority may attribute to this factor.[76]

203. The scope of the processing in this case is regional, and localised to patients of the MRHT LIS. The MRHT provides acute-care hospital services including a 24-hour emergency department and is the regional centre for Orthopaedics, Otolaryngology, Oncology, Haematology, Nephrology and Rheumatology. In turn, the LIS retains information including Patient Name, Patient Address, Patient ID, Patient DOB, Sex, Clinical Details (date/time of sample collection, date/time of receipt in the laboratory and date/time of report, specimen type, priority, results/reports, requesting clinician details) and a record of communications relating to test results.

204. The EDPB Fining Guidelines state that the **purpose** of the processing

> will lead the supervisory authority to attribute more weight to this factor. The supervisory authority may also consider whether the processing of personal data falls within the so-called core activities of the controller. The more central the processing is to the controller's or processor's core activities, the more severe irregularities in this processing will be. The supervisory authority may attribute

---

74 EDPB Fining Guidelines, para 53.b.i.
75 EDPB Fining Guidelines, para 53.b.i.
76 EDPB Fining Guidelines, para 53.b.ii.

more weight to this factor in these circumstances. There may be circumstances though, in which the processing of personal data is further removed from the core activities of the controller or processor, but significantly impacts the evaluation nonetheless (this is the case, for example, of processing concerning personal data of workers where the infringement significantly affects those workers' dignity).[77]

205. The purpose of the processing relating to the infringements identified herein is to provide health services to data subjects and retain and process test results. This is a core activity of the controller.

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

> The higher the number of data subjects involved, the more weight the supervisory authority may attribute to this factor. In many cases, it may also be considered that the infringement takes on "systemic" connotations and can therefore affect, even at different times, additional data subjects who have not submitted complaints or reports to the supervisory authority. The supervisory authority may, depending on the circumstances of the case, consider the ratio between the number of data subjects affected and the total number of data subjects in that context (e.g. the number of citizens, customers or employees) in order to assess whether the infringement is of a systemic nature.[78]

207. Some 84,000 data subjects were impacted by the personal data breach. This is a significant number of data subjects.

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

> The reference to the 'level' of damage suffered, therefore, is intended to draw the attention of the supervisory authorities to the damage suffered, or likely to have been suffered as a further, separate parameter with respect to the number of data subjects involved (for example, in cases where the number of individuals affected by the unlawful processing is high but the damage suffered by them is marginal). Following Recital 75 GDPR, the level of damage suffered refers to physical, material or non-material damage. The assessment of the damage, in any case, be limited [sic] to what is functionally necessary to achieve correct evaluation of the level of seriousness of the infringement as indicated in

---

77 EDPB Fining Guidelines, para 53.b.iii.

78 EDPB Fining Guidelines, para 53.b.iv.

paragraph 60 below, without overlapping with the activities of judicial authorities as tasked with ascertaining the different forms of individual harm.[79]

209. The level of damage suffered as a result of the infringements of Articles 5(1)(f) and 32(1) is high. The personal data affected by the HSE's failure to adopt and maintain appropriate security measures included health data of some 84,000 persons relating to sensitive matters kept strictly confidential by most people. While there is no direct evidence that the data was subsequently misused or disclosed by the attackers, the fact that it had been accessed, and the uncertainty as to whether it might be misused or disclosed must have caused distress at least to affected persons. Further, the reduced availability of data caused by the need to revert to a paper-based system is likely to have delayed communication of information needed to diagnose, treat or reassure patients.

210. The level of damage suffered as a result of the infringements of Articles 28 is medium. While the HSE had some documented agreements and details of its processing activities, these did not fully meet the requirements of the GDPR and had not been updated to comply with it. Appropriate documentation that complied with the requirements of those Articles would have helped to identify and highlight deficiencies in the HSE's technical and organisational measures for security that contributed to the vulnerabilities exploited in the breach, and the risks posed by it.

211. The level of damage suffered as a result of the infringements of Article 30 GDPR is low. The record produced to the DPC by the HSE recorded most of the information required by Article 30(1) GDPR, and the information not included in it was readily accessible. Although the record was created after date of the breach, it appears to have existed in draft form before, indicating an awareness of the obligation to maintain such a record and a motivation to comply with that requirement.

212. The level of damage suffered as a result of the infringement of Article 34 GDPR is low in circumstances where, notwithstanding the HSE's failure to assess the risk posed by the breach to be high, it nevertheless promptly took steps to inform the public of the breach and its efforts to remediate it. While, as detailed in paragraph 174, the HSE's Media Communications did not include all information required by Article 34 GDPR, the DPC is not aware of any person having suffered any loss, inconvenience or detriment as a result.

---

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

The nature of the infringements

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

> review the interest that the infringed provision seeks to protect and the place of this provision in the data protection framework. In addition, the supervisory authority may consider the degree to which the infringement prohibited the effective application of the provision and the fulfilment of the objective it sought to protect.[80]

214. In line with the text of the GDPR, the nature, gravity and duration of the infringements are all assessed by taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them.[81]

215. The nature of the infringements of Articles 5(1)(f) and 32(1) GDPR identified herein is the failure by the HSE to implement technical and organisational measures appropriate to the level of risk arising from its processing of data subjects' personal and special category personal data on the LIS. The nature of the infringements of Article 28 GDPR identified herein is a failure by the HSE to ensure that its agreements with the Infrastructure Provider and the Software Provider included sufficient guarantees to ensure that all relevant requirements of the GDPR were met and to ensure the protections of data subjects' rights. The HSE failed to ensure that binding agreements were up to date at the time of the breach, and the policies and procedures for implementing these agreements were not fully documented. This resulted in a contravention of the provisions of Articles 28 (1), (3) and (9) GDPR.

216. The nature of the infringement of Article 30 GDPR identified herein is the failure by the HSE to create and maintain a formal Record of Processing Activities containing all the information required by that Article.

217. The nature of the infringement of Article 34 GDPR identified herein was the HSE's failure to appropriately assess the risk to posed patients as a result of the breach to be high, and its failure in its Media Communications to include all information required by that provision.

---

80 EDPB Fining Guidelines, para 53.a.

81 Article 83(2)(a) GDPR.

The gravity of the infringements

218. The gravity (as well as the nature and duration of the infringements) is assessed taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them.[82]

219. 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 vulnerabilities that allowed the personal data breach to occur and contributed to the risks that the breach created. The HSE's lack of technical and organisational measures at the time of the breach contributed to the potential unauthorised disclosure of personal and special category data of 84,000 data subjects, including the irretrievable loss of electronic records of personal and special category data. There also was an adverse effect on availability of patient's health information, as the LIS provided ease of access for clinicians. As noted at paragraph 143, it is not possible to know how long the attackers had access to the system. Lastly, while there is no clear evidence that the attackers viewed or exfiltrated clinical data, the [redacted] forensic report makes it clear that such action cannot be excluded.

220. In relation to the gravity of the infringement of Article 28 GDPR, while there was a failure by the HSE to adhere to that provision of the GDPR in respect of its processors, the underlying level of damage to data subjects caused by those infringements has been identified as medium. Thus, the gravity of this infringement is moderate.

221. The gravity of the infringement of Article 30 GDPR is low. There was no Record of Processing Activity compliant with Article 30(1) in place at the time when the breach occurred, and some required information was not included in the record formally approved after the breach. However, the DPC is satisfied that the record existed with some of the relevant information.

222. The gravity of the infringement of Article 34 GDPR is moderate. The circumstances of the breach, including the fact that special category personal data of large number of data subjects was affected, clearly indicated a high risk, which the HSE failed to assess properly. However, the DPC takes account of the HSE's steps to publicise the breach – albeit incompletely – as outlined above, and considers these a mitigating factor of medium weight.

---

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

The duration of the infringements

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

> a supervisory authority may generally attribute more weight to an infringement with longer duration. The longer the duration of the infringement, the more weight the supervisory authority may attribute to this factor.[83]

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

- wilful conduct on the data controller's part, or
- failure to take appropriate preventive measures, or
- inability to put in place the required technical and organisational measures.[84]

225. For the purposes of this Decision, the HSE's infringements of Articles 5(1)(f) and 32(1) GDPR commenced on 25 May 2018, when the GDPR took effect. The obligation to comply with Articles 5(1)(f) and 32 GDPR applied from then, and the information and materials provided to the DPC during the course of this inquiry make clear that the deficiencies giving rise to the infringement of those Articles were in existence from at least that date. In its submission of 7 November 2019, the HSE stated:

> The MRHT LIS infrastructure has been fully migrated to the HSE OoCIO environment within a week of the breach occurring. The Laboratory quality management policies have been updated to reflect this. SLAs have been drafted to describe the new arrangements within the OoCIO environment.
>
> The Lab server infrastructure is now managed in line with group policies. Lab desktops are built per HSE National standards, including AV and the infrastructure support is aligned with National Standards.[85]

226. The DPC accepts this as evidence that the deficiencies in the HSE's technical and organisational measures for security of personal data processed on the LIS have been partially recognised and addressed. Therefore, for the purposes of deciding whether to impose an administrative fine, and for calculating the appropriate amount if applicable,

---

83 EDPB Fining Guidelines, para 53.c.

84 A29WP Fining Guidelines, 11.

85 HSE Submission, 'DPC Enquiry Consolidated responses', 7 November 2019, response to Q. 4 'Please provide a detailed overview of the technical and organisational measures in place for the Tullamore Laboratory System as a result of this breach.'

the DPC proceeds on the basis that the infringements of Articles 5(1)(f) and 32(1) GDPR lasted from 25 May 2018 until no later than 7 November 2019.

227. The infringement of Article 28 GDPR identified herein similarly commenced on 25 May 2018, when the GDPR took effect. As described in Section H of this Decision, the HSE's agreements and arrangements with the Software Provider and the Infrastructure Provider relating to the LIS pre-dated the entry into force of the GDPR, did not provide for the matters required in that Article, and were not updated to do so when the GDPR took effect. The HSE's arrangements with the Infrastructure Provider in respect of the LIS terminated when the LIS infrastructure was migrated to the OoCIO environment during November 2018, and the HSE and the Software Provider entered into a new 'Service Provider and Data Processing Agreement' compliant with Article 28 GDPR on 8 April 2019. The duration of the infringements of Article 28 GDPR identified herein is therefore from 25 May 2018 until 1 December 2018 in the case of the HSE's arrangements with the Infrastructure Provider, and from 25 May 2018 until 8 April 2019 in relation to the Software Provider.

228. The infringement of Article 30 GDPR similarly commenced on 25 May 2018, when the GDPR took effect. As outlined in Section I above, the HSE's document dated 23 November 2018[86] contained most, but not all, of the required information. However, the DPC is satisfied that the information not included was readily accessible and that the infringement did not persist beyond that date. The duration of the infringement is therefore from 25 May 2018 to 23 November 2018.

229. The HSE's infringement of Article 34 GDPR identified herein commenced when the HSE submitted its breach notification on 16 November 2018 showing an incorrect assessment of the risk posed by the breach as 'medium' rather than 'high'. As detailed in Section J of this Decision, the nature of the breach, the type and quantity of the personal data affected, the failure of backup procedures and the potential harms that unauthorised third parties might commit with the data all gave an unambiguous indication of a high risk. The HSE should have identified notification of data subjects under Article 34 GDPR as a priority at the time of notifying the breach on 16 November 2018.

230. Notwithstanding its incorrect assessment of the risk posed by breach, the HSE acted promptly to bring information about the breach to public attention through the press and broadcast media. This action commenced even before the HSE lodged its breach notification with the DPC. However, as noted previously, the HSE did not publicly

---

86 MRHT Laboratory Data Protection SOP.

identify its Data Protection Officer or other contact point for more information, and did not make clear that – as the External Cybersecurity Consultancy report pointed out in December 2018 – the possibility that personal data might have been exfiltrated could not be ruled out. While the contact details of the HSE's Data Protection Officer are easily available to concerned members of the public, the DPC is not aware that the HSE has to date made any public statement about the possibility that personal data affected by the breach may have been exfiltrated.

231. The duration of the infringement of Article 34 GDPR identified herein is therefore ongoing from 16 November 2018.

Assessment of Article 83(2)(a)

232. Taking account of all of the factors considered in this section, the DPC assesses the infringements of Articles 5(1)(f) and 32(1) to be of a high seriousness. This conclusion is made having regard to the assessment above that these infringements were of a high gravity. It also takes into consideration the nature of the infringements, which amounted to a failure to put in place appropriate technical and organisational measures to protect the personal data on the LIS. It recognises that the level of damage that may be suffered from a failure to put technical and organisational measures in place to protect this data is high. While the scope of the processing was localised to the systems of the MRHT, the large number of data subjects affected is also relevant to the overall conclusion that the infringements were of a high seriousness.

233. Taking account of all of the factors assessed above, the DPC considers the infringements of Article 28 GDPR to be of moderate seriousness. This takes account of the fact that the infringements were of a moderate gravity and of a relatively short duration.

234. Taking account of all the factors assessed above, the infringement of Article 30 GDPR was of low seriousness. This takes account of the short duration of the infringement and the ready availability of the information not included in the version of the record of processing activities submitted to the DPC.

235. Taking account of all the factors assessed above, the infringement of Article 34 GDPR was of moderate seriousness. The HSE's assessment of the risk posed by the breach should have concluded that, in circumstances where unauthorised access to large amounts of special category data had occurred, and where exfiltration could not be ruled out, that the risk posed by the breach was high. A correct assessment of a high risk would have likely prompted the HSE to consider and address all requirements of Article 34 GDPR. Against that, the DPC takes account of the HSE's prompt action to inform data subjects through public media channels of the breach and actions being

taken to remedy it. While this action did not convey all the information required by Article 34 GDPR, it reduces the seriousness of the infringement.

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

236. The A29WP Fining Guidelines state:

> in general, intent includes both knowledge and willfulness in relation to the characteristics of an offence, whereas 'unintentional' means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law.[87]

237. The EDPB Fining Guidelines state:

> The intentional or negligent character of the infringement (Article 83(2)(b) GDPR) should be assessed taking into account the objective elements of conduct gathered from the facts of the case. The EDPB highlighted that it is generally admitted that intentional infringements, 'demonstrating contempt for the provisions of the law, are more severe than unintentional ones'.[88] In case of an intentional infringement, the supervisory authority is likely to attribute more weight to this factor. Depending on the circumstances of the case, the supervisory authority may also attach weight to the degree of negligence. At best, negligence could be regarded as neutral.

238. In this case, the DPC finds that the infringements were not intentional. The DPC therefore does not consider there was 'intent' on the part of the HSE in the sense that there was no knowledge or wilfulness on their part in respect of their failures to ensure compliance with the relevant provisions of the GDPR.

239. In the Article 29 Working Party Guidelines, the following examples and guidance are given in relation to negligence:

> Other circumstances, such as failure to read and abide by existing policies, human error, failure to check for personal data in information published, failure to apply technical updates in a timely manner, failure to adopt policies (rather than simply failure to apply them) may be indicative of negligence.
>
> Enterprises should be responsible for adopting structures and resources adequate to the nature and complexity of their business. As such, controllers and processors

---

87 A29WP Fining Guidelines, 11.

88 EDPB Fining Guidelines, paragraph 56.

cannot legitimise breaches of data protection law by claiming a shortage of resources.

240. On the basis of the guidelines outlined above, the DPC finds that the HSE's infringements of Articles 5(1)(f) and 32(1) GDPR were of a negligent character for the purposes of Article 83(2)(b). The HSE is a well-funded public body processing large amounts of sensitive and special category personal data. It was aware that it had obligations under the GDPR in relation to its processing of that data. The HSE failed to identify all of its processing operations, or ensure that they were carried out in a manner that complied with the GDPR. There was a failure to implement adequate technical and organisational measures, which created vulnerabilities that allowed the breach to occur.

241. The DPC finds that the HSE's infringements of Article 28 GDPR were of a negligent character for the purposes of Article 83(2)(b). Sufficient guarantees to implement appropriate technical and organisational measures were not in place and there was a failure to produce formal processing agreements during the period from the entry into effect of the GDPR to the time of the breach. The HSE's agreements and arrangements with the Infrastructure Provider and the Software Provider pre-dated the entry into effect of the GDPR, but a controller with the technical and organisational resources of the HSE could and should have recognised that its arrangements with its processors did not comply with the standards introduced by Article 28, and should have acted to bring them into compliance.

242. The DPC finds that the HSE's infringement of Article 30 GDPR was of a negligent character for the purposes of Article 83(2)(b). There was no formal Record of Processing Activity in the form required by Article 30 GDPR in place during the period from the entry in to effect of the GDPR until 23 November 2018 and that the lack of any adequate Record of Processing Activity that was contemporaneous with the processing activities undertaken by MRHT at the time of the incident. The resources available to the HSE should have enabled it to foresee the need for such records well before the GDPR took effect, and to ensure that they were duly created and maintained. The HSE's failure to do so must be attributed to a lack of diligence and care.

243. The DPC finds that the HSE's infringement of Article 34 was negligent in character for the purposes of Article 83(2)(b) GDPR. Although the HSE rejected the DPC's assessment of the risk posed by the breach as being high, the HSE did so on the basis of a genuine but, in the DPC's considered view, misconceived assessment of the risk. The DPC is of the view that, to justify a finding that an infringement is of an intentional character, it must be caused by a deliberate or wilful action that knowingly or recklessly disregards a legal obligation. The DPC does not find that the HSE's assessment of the risk posed by the breach reached that threshold, and therefore finds this infringement to be negligent in character.

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

244. According to the A29WP Fining Guidelines:

> This provision acts as an assessment of the degree of responsibility of the controller after the infringement has occurred. It may cover cases where the controller has clearly not taken a negligent approach but where they have done all they can to correct their actions when they became aware of the infringement.[89]

245. In this case, HSE took measures to mitigate the damage suffered by data subjects. Regarding the infringements of Articles 5(1)(f) and 32(1) GDPR, the HSE acted promptly after becoming aware of the breach to physically isolate the affected environment from the wider HSE network.

246. The DPC also acknowledges the considerable improvements made by HSE in the intervening period of time since the breach and its commitment to ongoing improvements. The HSE has outlined measures implemented since 2021 as part of its National Cybersecurity Plan (NCSP) which have rectified many of the cybersecurity deficiencies which led to the Breach. The LIS environment has now been incorporated into the HSE's National Data Centre. Unsecured firewall ports have been disabled and MFA has been applied for remote access. A new Backup policy has been implemented.[90]

247. The HSE has demonstrated a commitment to implementing further improvements to its Cybersecurity posture. Details of these have been outlined in the Order for Compliance in paragraphs 180-186. In light of this, the DPC considers these mitigating factors to be of moderate value.

248. The infringement of Article 28 GDPR identified in this Decision arose in large part from a failure by the HSE to recognise that maintenance, servicing and support services provided under agreements with third parties involved processing of personal data of which the HSE was the controller. In correspondence with the DPC, the HSE indicated that, in the time since the breach, it has adopted new procurement and review procedures, impact assessments, and standard contract templates, which are designed to ensure compliance with Article 28 and other provisions of the GDPR. The HSE stated that:

> In summary we have a written contract which has been validated by our legal advisors with supporting documentation for each vendor, validate the

---

89 A29WP Fining Guidelines, 12-13.

90 HSE response to DPC queries, 16 March 2026.

documentation at the point of the contract, ensure that Data Processing elements comply with the GDPR act [sic] as a minimum. In addition we have review meetings with vendors on a regular basis to ensure that there is contract and support compliance. [91]

249. The DPC recognises that these measures demonstrate a significant improvement in the HSE's awareness of potential non-compliance and are an essential step in remedying the deficiencies that led to the infringements of Article 28 GDPR in this case. The DPC therefore considers this a mitigating factor of medium value.

250. In relation to Article 30 GDPR, the DPC notes that a compliant record of processing activity was created after the breach.[92] The DPC considers this a mitigating factor of medium value.

251. In relation to the infringement of Article 34, the DPC considers HSE's engagement with numerous media outlets as a mitigating factor to the infringement of Article 34. The DPC notes that, after the HSE's initial efforts to inform the public of the breach and efforts to remediate it, there were no significant public updates on the breach. Further, as noted in paragraph 174, not all required information was communicated to the public, including that personal data had been irretrievably lost, that test results would have to be processed from manual records, and that unauthorised viewing and exfiltration could not be ruled out. Accordingly, the DPC finds that this mitigating factor to be of medium value.

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

252. The key question in relation to this provision is whether the HSE 'did what it could be expected to do given the nature, the purposes or the size of the processing, seen in light of the obligations imposed on them by the Regulation.'[93]

253. In its submissions, HSE outlined the measures that it had in place to prevent potential data breaches. The DPC has had full regard to those measures in this Decision. This Decision assesses whether HSE complied with its obligations under Articles 5(1)(f) and 32(1) by implementing appropriate technical and organisational measures to ensure the

---

91 HSE response to DPC queries, 16 March 2026.

92 MRGT Laboratory Data Protection SOP, 2.

93 EDPB Fining Guidelines, 77.

requisite level of security of the Personal Data processed on the LIS environment. As outlined earlier, the DPC finds that HSE infringed those provisions.

254. In relation to the infringements of Articles 28 and 30(1), the HSE implemented measures to ensure compliance with those provisions in some contexts. It updated processor contracts to bring them in line with the requirements of Article 28(3), and adapted its organisational procedures to mitigate the risk of a recurrence of the infringement. In relation to Articles 30(1) it formally approved documents relating to processing activity. The DPC acknowledges that the HSE's revised RoPA meets the requirements of Article 30 GDPR.

255. In relation to Article 34 GDPR, the DPC notes that the HSE's media engagement following the breach partially complied with the requirement to notify data subjects. Whereas the HSE initially argued that the risk posed by the breach was medium rather than high, in response to the Draft Decision, the HSE revised their stance on this issue and conceded that high risk was the appropriate rating. The DPC acknowledges this response.

256. The DPC considers that the HSE holds a high degree of responsibility for all infringements identified in this Decision. All of these infringements arose from responsibilities that were clearly those of the HSE as the controller. However, in circumstances where this factor forms the basis for the finding of the infringement of Article 32 GDPR against HSE, this factor cannot be considered aggravating in respect of the infringements. Therefore, the DPC considers that this factor is neither aggravating nor mitigating in the circumstances.

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

257. In line with the EDPB Fining Guidelines, prior infringements are those already established before the draft decision (in the sense of Article 60 GDPR) is issued.[94]

258. According to the A29WP Fining Guidelines, '[t]his criterion is meant to assess the track record of the entity committing the infringement.'[95]

259. The DPC has concluded other inquiries into the HSE's processing of personal data, and has made findings of infringement in those inquiries. On 18 August 2020 and 29 September 2020, Inquiries IN-19-9-1 and IN-19-9-2 respectively made findings of infringements of Article 5(1)(f) and 32(1) GDPR for the HSE's failure to implement appropriate technical and organisational measures to ensure a level of security

---

94 EDPB Fining Guidelines, para 82.

95 A20WP Fining Guidelines, 14.

appropriate to the risk. However, the DPC does not consider them to be either an aggravating or mitigating factor in this Decision.

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

260. The extent to which HSE has cooperated with the inquiry is relevant to consider under this heading.[96] The DPC acknowledges the HSE's cooperation with the DPC during the course of the Inquiry. However, the DPC notes that the HSE 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. Subsequent measures taken with regard to the infringements of Article 5(1)(f), 28, 30 and 32(1) have been separately taken into account as mitigating factors under Article 83(2)(c) above.

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

261. By way of example of the categories that may be relevant to consider here, the A29WP Fining Guidelines suggest considering whether the infringements concern special category personal data under Articles 9 or 10 GDPR, whether the data are directly or indirectly identifiable, whether the data are encrypted, or whether the processing involves data whose dissemination would cause immediate damage or distress to the individual.[97]

262. The processing in this case involved special category data in the form of health data. This type of personal data, by its nature, carries a high risk to the rights and freedoms of the affected data subjects with the risk of 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 as a result of the personal data breach reported to the DPC, the inadequate security measures identified in this Decision related to this special category of personal data. The DPC finds that the sensitivity of this category of personal data aggravates the infringement of Articles 5(1)(f) and 32(1) in circumstances where there was a loss of confidentiality of and access to health records of 84,000 data subjects.

---

96 A29WP Fining Guidelines, 14.

97 A29WP Fining Guidelines, 14.

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

263. According to the A29WP Fining Guidelines, this section can be used to consider whether the DPC became aware of the infringement 'as a result of investigation, complaints, articles in the press, anonymous tips or notification by the data controller.'[98]

264. The A29WP Fining Guidelines also note that,

> The controller has an obligation according to the Regulation to notify the supervisory authority about personal data breaches. Where the controller merely fulfils this obligation, compliance with the obligation cannot be interpreted as an attenuating/ mitigating factor. Similarly, a data controller/processor who acted carelessly without notifying, or at least not notifying all of the details of the infringement due to a failure to adequately assess the extent of the infringement may also be considered by the supervisory authority to merit a more serious penalty i.e. it is unlikely to be classified as a minor infringement.[99]

265. In this case, the DPC became aware of the infringements as a result of a personal data breach notification from the HSE on 16 November 2018. The HSE's compliance with its obligation to notify personal data breaches under Article 33(1) cannot be considered mitigating in respect of the infringements of Articles 5(1)(f), 28, 30, 32(1) and 34 GDPR.

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

266. The A29WP Fining Guidelines state

> As opposed to the criteria in (e), this assessment criteria only seeks to remind supervisory authorities to refer to measures that they themselves have previously issued to the same controller or processors "with regard to the same subject matter".[100]

267. As noted above, the DPC does not consider previous infringements by the HSE are to be relevant to this Decision.

---

98 A29WP Fining Guidelines, 15.
99 A29WP Fining Guidelines, 15.
100 A29WP Fining Guidelines, 15.

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

268. Such considerations do not arise in this case.

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

269. The DPC considers that the matters considered under Article 83(2)(a) – (j) reflect an exhaustive account of both the aggravating and mitigating factors applicable in the circumstances of the case.

xii. Decision as to whether to impose a fine

270. The decision to impose an administrative fine 'needs to be taken on a case-by-case basis, in light of the circumstances of each individual case.'[101]

271. 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.

---

[101] EDPB, Binding Decision 1/2023.

272. Taking into account the assessment of the criteria at (ii) to (xi) above, the DPC has decided to impose an administrative fine for the infringements of Articles 5(1)(f) and 32(1) GDPR. This takes into account as aggravating factors the high level of seriousness of those infringements, their negligent nature, the degree of the responsibility of the HSE, and the fact that they impacted special category personal data. In view of the nature and seriousness of these aggravating factors, the DPC considers that it is appropriate to issue a fine. Although mitigating factors were identified in relation to Article 83(2)(c) GDPR, these did not eliminate the risk to data subjects. The DPC considers that the factors assessed in relation to Articles 83(2)(e), (f), (h), (i), (j) and (k) are neither mitigating nor aggravating.

273. While the Order to bring the HSE's data processing into GDPR compliance in respect of the infringements of Articles 5(1)(f) and 32(1) GDPR will bring the HSE into compliance and while the reprimand will assist in dissuading the HSE and other entities from similar future non-compliance, in light of the seriousness of the infringement, the DPC does not consider that the Order or reprimand, either taken severally or together, are proportionate or effective alone. The DPC finds that an administrative fine is necessary in respect of the infringements of Articles 5(1)(f) and 32(1) GDPR to deter other future serious non-compliance on the part of HSE and other controllers or processors carrying out similar processing operations. The reasons for this finding include

    - The infringements of Articles 5(1)(f) and 32(1) GDPR are serious in nature and gravity as set out pursuant to Article 83(2)(a) GDPR. Infringements that are of a serious nature and gravity must be dissuaded both in respect of the individual controller and in respect of other entities carrying out similar processing.

    - Regarding the infringements of Articles 5(1)(f) and 32(1) GDPR, the DPC considers that the HSE's non-compliance with its obligations under these Articles must be strongly dissuaded. Such dissuasive effect is crucial for protecting the rights and freedoms of those data subjects by implementing appropriate measures.

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

274. Having regard to the nature, gravity and duration of the infringements of Articles 5(1)(f) and 32(1) GDPR, the DPC also considers that an administrative fine is proportionate for ensuring compliance. The HSE's infringements of those Articles were a primary cause of the data breach. In light of this damage, the DPC considers that an administrative fine is proportionate in response to the HSE's infringement of Articles 5(1)(f) and 32(1) GDPR with a view to ensuring future compliance. The DPC considers that an administrative fine does not exceed what is necessary to enforce compliance in respect of the infringements identified in this Decision.

275. The DPC considers that the negligent character of the HSE's infringements of Articles 5(1)(f) 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 an administrative fine is necessary to ensure that HSE directs sufficient attention to its obligations under Articles 5(1)(f) and 32(1) GDPR in the future.

276. The DPC considers that an administrative fine would help to ensure that the HSE and other similar controllers take the utmost care to avoid infringements of the GDPR in respect of users' data.

277. Regarding the HSE's infringement of Articles 28, 30 and 34 GDPR, the DPC has taken account of all of the factors above, and particularly the fact that the seriousness of the infringements was moderate. The DPC has decided that in all of the circumstances, the reprimand is are sufficient to address those infringements.

b) Decision on the amount of the administrative fine

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

i. Article 83(3) GDPR

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

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

280. As outlined previously, the infringements identified herein all relate to the processing concerned, i.e. the personal data processed on the LIS.

281. In respect of the interpretation of Article 83(3) GDPR, the DPC is mindful of its obligations of cooperation and consistency in, *inter alia*, Articles 60(1) and 63 GDPR. Accordingly, it is necessary to follow the EDPB's interpretation of Article 83(3) GDPR which was set out in the EDPB's binding decision 1/2021, which was made in relation to an inquiry conducted by the DPC.[102] In summary, the view of the EDPB is that the correct approach to the interpretation of Article 83(3) requires that:

---

[102] DPC Inquiry IN-18-12-2.

> 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.

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

283. In this case, the DPC has decided to impose a fine for the identified infringements of Articles 5(1)(f) and 32(1) GDPR. The gravest infringement is that of Article 5(1)(f) GDPR as it is an infringement of a core principle of the GDPR.

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

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

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

The categorisation of the infringements under Articles 83(4) or (5) is a relevant consideration in assessing the seriousness of the infringements in this case. The infringement of Article 5(1)(f) found in this case relates to the basic principles of processing and is ascribed considerably greater significance, with the legislator providing for, in general, maximum administrative fines double those applicable to the infringements of Articles 32(1), 28 and 33(1).

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

285. The EDPB Guidelines state that the factors assessed in relation to Articles 83(2)(a), (b) and (g) GDPR indicate the seriousness of the infringement.[103] These factors were assessed in paragraphs 213 to 240 and 261 to 262 above. The guidelines also state that

> This assessment is no mathematical calculation in which the abovementioned factors are considered individually, but rather a thorough evaluation of the concrete circumstances of the case, in which all of the abovementioned factors are interlinked. Therefore, in reviewing the seriousness of the infringement, regard should be given to the infringement as a whole.[104]

286. Having regard to these factors as a whole, the infringements are of a medium to high level of seriousness. Under Article 83(2)(a) the infringements of Articles 5(1)(f) and 32(1) were found to be of a serious nature and have a high degree of gravity. The infringements affected special category personal data relating to health which, by their nature, carry a risk with regard to the fundamental rights and freedoms of 84,000 data subjects, as assessed under Article 83(2)(g). The infringements were also of a negligent character, as assessed under Article 83(2)(b). The infringements are found to have been of moderate duration. Therefore, balancing these factors, the DPC considers that the infringements were of high seriousness.

iv. Imposing an effective, dissuasive and proportionate fine

287. Article 83(1) GDPR requires a fine to be effective, proportionate and dissuasive in each individual case. As the guidelines also say that this doesn't 'dismiss a supervisory authority from the responsibility to carry out a review of the effectiveness, dissuasiveness and proportionality at the end of the calculation.'[105] Article 83(1) will be considered again at the end of this calculation.

v. Aggravating and mitigating circumstances

288. Articles 83(2)(a), (b) and (g) GDPR were considered above in relation to the starting point for the calculation of the fine. In line with the approach suggested in the EDPB Fining Guidelines,[106] this section considers the aggravating or mitigating impact of the remaining criteria in Article 83(2) GDPR.

---

103 EDPB Fining Guidelines, paragraph 51.
104 EDPB Fining Guidelines, paragraph 59.
105 EDPB Fining Guidelines, paragraph 64.
106 EDPB Fining Guidelines, paragraph 70.

289. In relation to Article 83(2)(c), the DPC notes that the HSE adopted measures to mitigate the damage to data subjects. The DPC considers this a mitigating factor of moderate weight, as there remain concerns regarding the HSE's ability to safeguard against future attacks.

290. In relation to Article 83(2)(d), the DPC notes that the HSE had a high degree of responsibility for the infringements. The DPC consider this factor to be aggravating, as the HSE did not do what could be expected to be done in the circumstances. The failure to adopt technical and organisational measures is not in itself, aggravating, as this forms the basis for the infringements identified.

291. In relation to Article 83(2)(e), the DPC notes that the HSE has had previous infringements, but that these were neither mitigating nor aggravating in the circumstances.

292. In relation to Article 83(2)(f), the DPC notes that the HSE cooperated with the DPC. As the HSE has a general obligation to cooperate under Article 31 GDPR, this factor is considered to be neither mitigating nor aggravating.

293. In relation to Article 83(2)(h), the DPC notes that the manner in which the infringement became known to the DPC was through a notification of a personal data breach from the HSE on 16 November 2018. This factor is considered to be neither mitigating nor aggravating.

294. In relation to Article 83(2)(i), the DPC notes that no measures had previously been made by the DPC with regard to the same subject matter. [107]

295. In relation to Article 83(2)(j), the DPC has found no relevant approved codes of conduct or approved certification mechanisms. This factor is therefore not applicable.

296. In relation to Article 83(2)(k), the DPC notes that there were no additional aggravating or mitigating factors for consideration. This is factor is therefore not applicable.

---

[107] Paragraph 101 of the EDPB Fining Guidelines says in relation to this provision: '…as opposed to Article 83(2)(e) GDPR, this assessment only refers to measures that supervisory authorities themselves have previously issued to the same controller or processor with regard to the same subject matter.' In its Decision on inquiry IN-19-9-1 (issued on 18 August 2020) the DPC imposed administrative fines and issued a reprimand to the HSE for infringements of Articles 5(1)(f) and 32 GDPR. However, the processing concerned in that case related to hard copy records and the DPC does not consider that it concerns the same subject matter.

297. Taking into account all of the matters arising for consideration as part of the individual assessments required to be carried out pursuant to Article 83(2), together with the recommendations in the Fining Guidelines as detailed above, the DPC imposes an administrative fine of €300,000 in respect of the infringement of Articles 5(1)(f) and 32(1) GDPR.

298. This fine is at the lower end of the range proposed in the Draft Decision. The DPC's choice of this level of administrative fine reflects the mitigation occasioned by the HSE in acknowledging flaws in its technical and organisations measures, indicating its commitment to compliance and protecting data protection rights and promptly making significant improvements in order to reduce the likelihood of similar breaches occurring in the future.

vi. The relevant legal maximums for the different processing operations

The relevant undertaking for the purposes of the fine calculation

299. The DPC notes that the State has exercised its right under Article 83(7) GDPR to lay down rules on the extent to which administrative fines may be imposed on public authorities and bodies, and enacted section 141 of the Act of 2018 setting the maximum fine on such authorities and bodies at €1,000,000.

300. The DPC notes that the HSE is a public authority (as defined in section 2(1) of the 2018 Act), having been established under the Health Act 2004. Section 141(4) of the 2018 Act provides that any administrative fine that the DPC decides to impose on a public authority or public body shall not exceed €1,000,000 unless that authority or body acts as an undertaking within the meaning of the Competition Act 2002. As the administrative fine imposed in this Decision does not exceed that amount, it is not necessary for the DPC to determine whether the HSE acts as an undertaking for the purpose of the processing concerned.

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

Effectiveness

301. It is the DPC's view that for a fine to be effective, it must be large enough to have a significant effect on the controller or processor such that GDPR compliance, motivated by avoiding such fines in the future, becomes a factor in the entity's governance and management decision-making at the highest level. Furthermore, a sufficiently large fine is necessary to ensure that the fine is not just an insignificant expense for the controller or processor concerned, and to ensure that the controller or processor does not enjoy

an unfair advantage by reason of its ability to absorb even large fines for its infringements of the GDPR.

302. In the DPC's view, the levels of the fine imposed in this Decision ensure a sufficiently effective fine, and no further adjustment is required.

Dissuasiveness

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

304. In coming to this conclusion, the DPC has considered that the fine imposed is dissuasive having regard to the severity of the infringements and the resources of the HSE. The DPC considers that the fine will be dissuasive for the HSE and other controllers in similar positions.

Proportionality

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

306. The DPC is satisfied that the fine imposed above does not exceed the minimum necessary to enforce compliance with the GDPR. The infringements relate to the security measures applicable to health data, were negligent, and the HSE had a high degree of responsibility for them. Overall, the DPC is satisfied that the imposed fine complies with the principle of proportionality.

O. Summary of Envisaged Action

307. In summary, the corrective powers that the DPC has decided to exercise are:

- an Order to bring processing into compliance in respect of the HSE's infringement of Articles 5(1)(f) and 32(1) GDPR;
- a Reprimand to the HSE pursuant to Article 58(2)(b) GDPR regarding the infringements identified in this Decision
- and an administrative fine in respect of the HSE's infringement of Articles 5(1)f and 32(1) GDPR of €300,000.

P. Right of Appeal

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

This Decision is addressed to
The Health Service Executive
Dr. Steevens' Hospital, Steeven's Lane,
Dublin 8, D08 W2A8
Ireland

_____ _____

Dr. Des Hogan
Commissioner for Data Protection
Chairperson

Dale Sunderland
Commissioner for Data Protection