DATA PROTECTION ACT 2018 (PART 6, SECTION 155)

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

TO: **INTERSERVE GROUP LIMITED**

OF: CAPITAL TOWER, 91 WATERLOO ROAD, LONDON, ENGLAND SE1 8RT

INTRODUCTION AND SUMMARY

1. This Monetary Penalty Notice is given to Interserve Group Limited ("Interserve"). It relates to infringements of the General Data Protection Regulation (the "GDPR"), which came to the attention of the Information Commissioner ("the Commissioner").[1]

2. The Commissioner has decided to issue Interserve with a Penalty Notice under section 155 of the Data Protection Act 2018 ("the DPA"). This penalty notice imposes an administrative fine on Interserve in accordance with the Commissioner's powers under Article 83 of the GDPR. The amount of the penalty is **£4,400,000**.

3. This penalty has been issued because of contraventions by Interserve of Article 5(1)(f) and Article 32 of the GDPR during the period 18 March

[1] The applicable legislation at the time of the Relevant Period, as defined in paragraph 3, was the General Data Protection Regulation (EU) (2016/679) ("(EU) GDPR"). The Commissioner was at the material time the supervisory authority in respect of the (EU) GDPR. With effect from 1 January 2021 the Commissioner's powers are set out in the UK GDPR, namely the GDPR as it forms part of the law of England and Wales pursuant to section 3 of the European Union (Withdrawal) Act 2018. References to the GDPR are to be construed accordingly.

2019[2] to 1 December 2020[3] (the "Relevant Period"). These contraventions rendered Interserve vulnerable to a cyber-attack which took place in the period 30 March 2020 to 2 May 2020 ("the Incident") which affected the personal data of up to 113,000 employees of Interserve.

4. For the reasons set out in this Monetary Penalty Notice the Commissioner has found that in the Relevant Period Interserve failed to process personal data in a manner that ensured appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures as required by Article 5(1)(f) and Article 32 GDPR.

5. This Monetary Penalty Notice explains the Commissioner's decision, including the Commissioner's reasons for issuing the penalty and for the amount of the penalty. Interserve has had an opportunity to make representations to the Commissioner in response to the Notice of Intent regarding this penalty, and the Commissioner has had regard to those representations in making this final decision.

LEGAL FRAMEWORK

GDPR

6. On 25 May 2018, the GDPR entered into force in the EU, replacing the previous EU law data protection regime that applied under Directive 95/46/EC ("Data Protection Directive")[4]. The GDPR sought to harmonise

[2] The date upon which Interserve Group Limited became the relevant data controller as the successor parent company to Interserve Plc which had been placed in administration and was subject to the obligations in the GDPR.
[3] The date upon which remediation measures were completed.
[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

the protection of fundamental rights in respect of personal data across EU Member States and, unlike the Data Protection Directive, was directly applicable in every Member State[5].

7. The GDPR was developed and enacted in the context of challenges to the protection of personal data posed by, in particular:

   a. the substantial increase in cross-border flows of personal data resulting from the functioning of the internal market[6]; and

   b. the rapid technological developments which have occurred during a period of globalisation[7].

8. Such developments made it necessary for "a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market…"[8].

9. Against that background, the GDPR imposed more stringent duties on controllers and significantly increased the penalties that could be imposed for a breach of the obligations imposed on controllers (amongst others)[9].

10. With effect from 1 January 2021 the GDPR has been retained as part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419).

---

[5] Recital 3.
[6] Recital 5.
[7] Recital 6.
[8] Recital 7.
[9] See, in particular, Recitals 11, 148, 150, and Article 5, Chapter IV and Article 83.

Obligations of the Controller

11. Interserve is a data controller for the purposes of the GDPR and the DPA, because it determines the purposes and means of processing of personal data (GDPR Article 4(7)). While both the Incident and the data security deficiencies addressed in this Monetary Penalty Notice affected numerous companies within the Interserve group of companies, the Commissioner is satisfied that the controller with primary responsibility for these matters is Interserve. This is in particular by reason of the following matters:

    a. Interserve is the parent company for the Interserve group and was responsible for adopting, monitoring and ensuring compliance with the relevant policies relating to data protection and information security.

    b. Interserve was responsible for the security of the IT infrastructure on which the majority of Interserve subsidiaries stored their personal data.

    c. During the Relevant Period, Interserve employed the Chief Information Officer, and the majority of individuals who comprised the Group IT and Group Information Security Teams were employed by Interserve.

    d. Interserve's submissions to the Commissioner appear to accept that it was the controller bearing responsibility for the data security issues relevant to the Incident.

12. "*Personal data*" is defined by Article 4(1) of the GDPR to mean:

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

13. "*Processing*" is defined by Article 4(2) of the GDPR to mean:

> *"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"*

14. Article 9 GDPR prohibits the processing of "*special categories of personal data*" unless certain conditions are met. The special categories of personal data subject to Article 9 include "*data concerning health or data concerning a natural person's sex life or sexual orientation*".

15. Controllers are subject to various obligations in relation to the processing of personal data, as set out in the GDPR and the DPA. They are obliged by Article 5(2) to adhere to the data processing principles set out in Article 5(1) of the GDPR. Article 5(2) makes clear that the "*controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')".*

16. In particular, controllers are required to implement appropriate technical and organisational measures to ensure that their processing of personal data is secure, and to enable them to demonstrate that their processing is secure. Article 5(1)(f) ("Integrity and Confidentiality") stipulates 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"*

17. Chapter IV, Section 2 addresses security of personal data. Article 32 ("Security of processing") provides, in material part:

> *"1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
>
> > *(a) the pseudonymisation and encryption of personal data;*
> >
> > *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
> >
> > *(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*

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

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

18. Article 32 GDPR applies to both controllers and processors.

The Commissioner's powers of enforcement

19. The Commissioner is the supervisory authority for the UK, as provided for by Article 51 of the GDPR.

20. By Article 57(1) of the GDPR, it is the Commissioner's task to monitor and enforce the application of the GDPR.

21. By Article 58(2)(d) of the GDPR the Commissioner has the power to notify controllers of alleged infringements of GDPR. By Article 58(2)(i) he has the power to impose an administrative fine, in accordance with Article 83, in addition to or instead of the other corrective measures referred to in Article 58(2), depending on the circumstances of each individual case.

22. By Article 83(1), the Commissioner is required to ensure that administrative fines issued in accordance with Article 83 are effective,

proportionate, and dissuasive in each individual case. Article 83(2) goes on to provide that:

> *"When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:*
>
> > *(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;*
> >
> > *(b) the intentional or negligent character of the infringement;*
> >
> > *(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;*
> >
> > *(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;*
> >
> > *(e) any relevant previous infringements by the controller or processor;*
> >
> > *(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;*
> >
> > *(g) the categories of personal data affected by the infringement;*

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

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

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

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

23. Article 83(5) GDPR provides that infringements of the basic principles for processing imposed pursuant to Article 5 GDPR will, in accordance with Article 83(2) GDPR, be subject to administrative fines of up to €20 million or, in the case of an undertaking[10], up to 4% of its total worldwide annual turnover of the preceding financial year, whichever is higher.

24. Article 83(4) GDPR provides, *inter alia*, that infringements of the obligations imposed by Article 32 GDPR on the controller and processor will, in accordance with Article 83(2) GDPR, be subject to administrative

[10] Recital 150 of the GDPR states that where administrative fines are imposed on an undertaking, an 'undertaking' should be understood in accordance with EU competition principles set out in Articles 101 and 102 Treaty on the Functioning of the European Union (TFEU). The Commissioner considers Interserve to be an undertaking comprising Interserve and its subsidiary companies.

fines of up to €10 million or, in the case of an undertaking, up to 2% of its total worldwide annual turnover of the preceding financial year, whichever is higher.

25. Article 83(3) GDPR addresses the circumstances in which the same or linked processing operations give rise to infringements of several provisions of the GDPR. It provides that "*... the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement*".

The DPA

26. Section 115 DPA establishes that the Commissioner is the UK's supervisory authority for the purposes of the GDPR. The DPA contains enforcement provisions in Part 6 which are exercisable by the Commissioner.

27. Section 155 of the DPA sets out the matters to which the Commissioner must have regard when deciding whether to issue a penalty notice and when determining the amount of the penalty and provides that:

> *"(1) If the Commissioner is satisfied that a person—*
>
> *(a) has failed or is failing as described in section 149(2) …,*
>
> *the Commissioner may, by written notice (a "penalty notice"), require the person to pay to the Commissioner an amount in sterling specified in the notice.*
>
> *(2) Subject to subsection (4), when deciding whether to give a penalty notice to a person and determining the amount of the*

penalty, the Commissioner must have regard to the following, so far as relevant—

> *(a) to the extent that the notice concerns a matter to which the GDPR applies, the matters listed in Article 83(1) and (2) of the GDPR."*

28. The failures identified in section 149(2) DPA are, insofar as relevant here:

> *"(2) The first type of failure is where a controller or processor has failed, or is failing, to comply with any of the following—*
>
> > *(a) a provision of Chapter II of the GDPR or Chapter 2 of Part 3 or Chapter 2 of Part 4 of this Act (principles of processing);*
> >
> > *…;*
> >
> > *(c) a provision of Articles 25 to 39 of the GDPR or section 64 or 65 of this Act (obligations of controllers and processors) […]"*

29. Schedule 16 includes provisions relevant to the imposition of penalties. Paragraph 2 makes provision for the issuing of notices of intent to impose a penalty, as follows:

> *"(1) Before giving a person a penalty notice, the Commissioner must, by written notice (a "notice of intent") inform the person that the Commissioner intends to give a penalty notice."*

The Commissioner's Regulatory Action Policy

30. Pursuant to section 160(1) DPA, the Commissioner published his Regulatory Action Policy ("RAP") on 7 November 2018. The RAP was published following a consultation exercise and was submitted to the Secretary of State and laid before Parliament for approval.

31. Under the hearing "Aims", the RAP explains that it seeks to:

- "Set out the nature of the Commissioner's various powers in one place and to be clear and consistent about when and how we use them"

- "Ensure that we take fair, proportionate and timely regulatory action with a view to guaranteeing that individuals' information rights are properly protected"

- "Guide the Commissioner and our staff in ensuring that any regulatory action is targeted, proportionate and effective ..."[11]

32. The objectives of regulatory action are set out at page 6 of the RAP, including:

- "To respond swiftly and effectively to breaches of legislation which fall within the ICO's remit, focusing on [inter alia] those adversely affecting large groups of individuals.

- "To be effective, proportionate, dissuasive and consistent in our application of sanctions", using the Commissioner's most significant powers on, inter alia, "organisations and individuals

[11] RAP page 5.

suspected of repeated or willful misconduct or serious failures to take proper steps to protect personal data".

33. The RAP explains that the Commissioner will adopt a selective approach to regulatory action. When deciding whether and how to respond to breaches of information rights obligations he will consider criteria which include the following:

- "the nature and seriousness of the breach or potential breach";
- "where relevant, the categories of personal data affected (including whether any special categories of personal data are involved) and the level of any privacy intrusion";
- "the number of individuals affected, the extent of any exposure to physical, financial or psychological harm, and, where it is an issue, the degree of intrusion into their privacy;
- "whether the issue raises new or repeated issues, or concerns that technological security measures are not protecting the personal data";
- "the cost of measures to mitigate any risk, issue or harm";
- "the public interest in regulatory action being taken (for example, to provide an effective deterrent against future breaches or clarify or test an issue in dispute."[12]

[12] RAP, pages 10 – 11.

34. The RAP explains that, as a general principle, "more serious, high-impact, intentional, willful, neglectful or repeated breaches can expect stronger regulatory action".[13]

35. The process the Commissioner will follow in deciding the appropriate amount of penalty to be imposed is described in the RAP from page 27 onwards. In particular, the RAP sets out the following five-step process:

    a. Step 1. An 'initial element' removing any financial gain from the breach.

    b. Step 2. Adding in an element to censure the breach based on its scale and severity, taking into account the considerations identified at section 155(2) - (4) DPA and adopting as a starting point the relevant percentage of revenue figures in accordance with Article 83(5) GDPR.

    c. Step 3. Adding in an element to reflect any aggravating factors. A list of aggravating factors which the Commissioner would take into account, where relevant, is provided at page 11 of the RAP. This list is intended to be indicative, not exhaustive.

    d. Step 4. Adding in an amount for deterrent effect to others.

    e. Step 5. Reducing the amount (save that in the initial element) to reflect any mitigating factors, including ability to pay (financial hardship). A list of mitigating factors which the Commissioner would take into account, where relevant, is provided at page 11-12 of the RAP. This list is intended to be indicative, not exhaustive.

[13] RAP, page 12.

CIRCUMSTANCES OF THE CONTRAVENTION: FACTS

General Background

36. This Monetary Penalty Notice does not purport to identify exhaustively each and every circumstance and document relevant to the Commissioner's investigation. The circumstances and documents identified below are a proportionate summary.

Events prior to the Incident

37. Interserve is the parent company for the Interserve group, a group of construction companies headquartered in the UK. Interserve became the successor company to Interserve Plc in March 2019 when the latter went into administration in March 2019.

38. In 2016, Interserve Plc's Group Information Security team created an Information Security Policy Framework ratified by the executive board for implementation across the Interserve group.

39. In the Relevant Period, Interserve had in place a number of policies and standards directed at information security including the following (i) System Management Policy, (ii) Information Security Training Policy, (iii) Threat and Vulnerability Management Policy, (iv) System Management Standard, (v) Network Management Standard, (vi) Technical Security Infrastructure Standard, (vii) Incident Management Standard, (viii) Threat and Vulnerability Management Standard, (ix) Access Control Standard and (x) Ransomware Incident Response Guidelines.

40. Interserve had responsibility for overseeing and ensuring the implementation of, and compliance with, the relevant policies and standards.

The Incident

41. An investigation carried out by Interserve with support and assistance from external agencies established that, in relation to the Incident:

    a. On 30 March 2020, a phishing email was sent to Interserve Construction Limited's accounts team mailbox which was designed to appear as though the document required urgent review. This was then forwarded on 31 March 2020 by one employee to another employee responsible for paying invoices. The Commissioner notes that, over the Relevant Period, Interserve had in place an appropriate secure email gateway (Forcepoint) in accordance with industry norms, but the Commissioner's view is that this was not relevant to the risks or causes of the Incident

    b. The phishing email was opened by the latter employee on 1 April 2020, who downloaded and extracted the ZIP file linked in the email, and opened the script file. This executed the installation of malware onto their workstation and gave the cyber-attacker access to the relevant employee's workstation.

    c. At the relevant time the employee was working from home and had access to Interserve's systems via a split tunnelling method. As a result of the split tunnelling method, the employee who clicked on the link in the email did not go through Interserve's Internet Gateway system (Bluecoat) which was designed to restrict access to malicious sites.

    d. Whilst actions were taken by Interserve's System Centre Endpoint Protection tool to remove some of the files resulting from the extraction of the ZIP file, which reported that the automatic

removal of malware files had been successful, no further action was taken by Interserve at this time to verify that all malware had been removed. In fact the attacker retained access to the employee's workstation.

e. Following this initial access, on 3 April 2020 a server was compromised by the attacker, which was then used to move laterally to other systems.

f. On 1 and 2 May 2020, an attacker used tools to compromise 283 systems and 16 accounts (including 12 privileged accounts) across four domains.

g. Using a compromised account, the attacker executed a script to uninstall Interserve's Anti-Virus solution.

h. The attacker compromised Interserve's servers including four HR databases known as the AX12 system, iTrent system, Profund system and File Director System which together contained personal data relating to up to 113,000 individuals including special category data.

i. The personal data on those systems was encrypted and rendered unavailable to Interserve by the attacker.

j. [redacted]

Discovery and Reporting of the Breach

42. On 2 May 2020 as part of a routine maintenance check Interserve discovered a message on its server infrastructure stating that it had been hacked. [redacted]

43. On investigation, it determined that it had been subjected to a ransomware attack and on 2 May 2020 notified the National Cyber Security Centre ("NCSC") of the incident.

44. Over the period 4 – 6 May 2020 Interserve engaged the services of external agencies to investigate and provide advice and support in relation to the cyber-attack.

45. On 5 May 2020 Interserve notified the National Crime Agency ("NCA") of the breach.

Reporting the Breach to the Information Commissioner

46. On 5 May 2020 Interserve submitted a personal data breach notification to the Commissioner. The Commissioner subsequently commenced an investigation in relation to the matters relating to the Incident.

47. As part of that investigation the Commissioner sought information and relevant documents from Interserve. Interserve has co-operated with the Commissioner throughout its investigation.

Personal Data Involved in the Incident

48. The data affected by the Incident comprised the personal data of up to 113,000 individuals held across four HR databases which were

compromised by the attack. These individuals were current or former employees of Interserve.

49. The personal data held on the compromised databases included contact details namely telephone number, email address, national insurance number, bank account details, marital status, birth date, education, country of birth, gender, number of dependants, emergency contact information and salary[14].

50. The databases also held special category personal data including ethnic origin, religion, details of disabilities, sexual orientation, health information relevant to ill-heath retirement applications.

THE CONTRAVENTIONS OF ARTICLE 5(1)(F) AND 32 OF THE GDPR

51. For the reasons set out below, and having carefully considered Interserve's representations, the Commissioner has concluded that Interserve has failed to comply with its obligations under Article 5(1)(f) and Article 32.

Article 5(1)(f)

52. Interserve failed to process personal data 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 and organisational measures as required by Article 5(1)(f).

[14] Each of these items of information was not necessarily held for each of the 113,000 individuals, rather these categories of information were recorded in the relevant databases.

53. The Commissioner relies on the following matters as constituting a breach of the requirements imposed by Article 5(1)(f).

(1) Unsupported operating systems

54. During the Relevant Period, Interserve was processing personal data on unsupported operating systems. In particular, Interserve was processing personal data on 18 servers that hosted Server 2003 R2, and 22 servers that hosted Microsoft Server 2008 R2. This included iTrent, Interserve's HR system which processed significant volumes of personal information and some of the affected Pensions systems.

55. Microsoft Server 2003 R2 ended mainstream support in 2010 and became end-of-life in July 2015, and Microsoft Service 2008 R2 ended mainstream support in 2015 and became end-of-life in January 2020. Accordingly, for a number of years prior to the Incident and at the time of the Incident these operating systems were no longer the subject of security updates to fix known vulnerabilities in the system which could be exploited by malicious actors.

56. The failure to implement supported operating systems was contrary to:

a. Interserve's Systems Management Policy which required Interserve to (i) adopt standardised secure builds that are regularly updated and enables secure functions and services and (ii) adopt computer and network services from service providers capable of providing malware protection and patch management capabilities.

b. Interserve's Systems Management Standards which required Interserve to (i) adopt information systems designed to support the prompt application of security updates to respond to changing

threats and vulnerabilities and (ii) keep servers up to date by applying patch management practises.

c. Industry best practices standard NIST 800-53 which requires organisations to (i) plan for and implement a technology refresh schedule through the system development life cycle, (ii) replace system components when support for the components is no longer available from the developer, vendor or manufacturer, and (iii) conduct a risk assessment including identifying threats to and vulnerabilities in the system.

d. Guidance on "Security Outcomes" (2018) issued by the NCSC and the Commissioner which recommends managing software vulnerabilities including using in-support software.

e. Guidance on "Mitigating Malware and Ransomware attacks" (2020) issued by the NCSC which recommends the use of the latest version of an operating system to take advantage of the latest security features to prevent against ransomware attacks.

57. Interserve ought reasonably to have been aware of the risks posed by running outdated support systems, in particular in circumstances where (i) the risks of running outdated support systems were well-known and documented, (ii) Microsoft Threat Intelligence team had warned in April 2020 of ransomware campaigns targeting healthcare and critical service sectors and stated these attackers were exploiting, amongst others, older operating systems such as Windows Server 2003 and 2008, (iii) Interserve's Threat and Vulnerability policy required it to monitor external intelligence sources such as security vendors to protect against malware and (iv) Interserve's senior management were aware of historic and legacy issues within the IT estate.

58. Further, Interserve failed to undertake any formal risk assessments in relation to using unsupported operating systems on its data processing servers.

59. In these circumstances the failure to implement supported operating systems contributed to a breach of Article 5(1)(f).

(2) End-point protection

60. At the time of the attack, Interserve failed to implement appropriate end-point protection. In particular:

a. The majority of the servers that formed part of the server estate, including those compromised, were using "McAfee VirusScan Enterprise", an endpoint protection product which, at the time of the Incident, was not running its latest Anti-Virus protection.

b. At the time of the Incident host-based firewalls were not enabled.

c. Interserve did not implement application 'allow or deny' lists.

d. Interserve did not prevent macros from executing on the initial compromised host.

61. These failures were contrary to:

a. Interserve's Technical Security Infrastructure standard and Network Management standard.

b. Industry best practices standard ISO27001 which requires that "detection, prevention and recovery controls to protect against malware should be implemented".

c. Guidance on "Mitigating Malware and Ransomware attacks" (2020) issued by the NCSC which recommends detection, prevention and recovery controls including but not limited to: (i) keeping anti-virus or anti-malware software up to date, (ii) implementing application allow/deny list solutions, (iii) disabling or constraining scripting environments and macros, (iv) configuring host-based firewalls.

d. The warning of McAfee in October 2019 which stated: "If you're running McAfee VirusScan Enterprise, you are not using our latest and most effective endpoint protection. McAfee Endpoint Security is a free security upgrade that leverages machine learning and application containment to halt threats in their track".

62. Interserve ought reasonably to have been aware of the risks posed by failing to implement appropriate endpoint protection, in particular in circumstances where (i) the risk of such a failing was well-known and documented, and (ii) Interserve's Threat and Vulnerability policy required it to monitor external intelligence sources such as security vendors to protect against malware and Interserve therefore should have been aware of the weakness identified on the McAfee website.

63. In these circumstances the failure to implement appropriate end-point protections contributed to a breach of Article 5(1)(f).

(3) Threat and vulnerability policy

64. In response to questions posed by the Commissioner on 26 May 2020 and 12 June 2020 in relation to the testing of the security of its data processing system and penetration testing, Interserve provided evidence

of annual vulnerability scans and failed to provide any evidence of penetration testing in the two years prior to the Incident.

65. The failure to undertake adequate vulnerability scanning and penetration testing is contrary to:

a. Interserve's threat and vulnerability policy which requires penetration testing to be carried out as follows: (i) annual testing of externally facing IP addresses, (ii) external testing of new systems that expose services and data to public access, (iii) internal tests of new systems or where significant changes may have altered levels of security and (iv) where regulation or compliance requires testing e.g. PCI DSS.

b. Interserve's threat and vulnerability standard required "Vulnerability scanning of business applications, information systems and network devices should be performed: a) using automatic vulnerability scanning software or a commercial vulnerability scanner server b) on a regular basis (e.g. daily)".

c. Industry best practice standard NIST 800-53 which requires organisations to "monitor and scan for vulnerabilities in the system and hosted applications" and "employ an independent penetration testing agent or team to perform penetration testing on the system or system components".

d. The "Vulnerability Management Guidance" (2016) published by the NCSC which recommends monthly vulnerability scans.

66. Interserve ought reasonably to have been aware of the risks posed by failing to undertake regular vulnerability scanning and penetration testing in particular in circumstances where (i) the requirement for

conducting such checks was well-known and documented, and (ii) Interserve's own policies and standards required such testing and scanning.

67. In these circumstances the failure to conduct regular and effective vulnerability scanning and penetration testing contributed to a breach of Article 5(1)(f).

(4) Information Security Training

68. At the time of the attack, one of the two employees who received the phishing email had not undertaken data protection training.

69. This was contrary to:

a. Interserve's Information Security Training policy which required that (i) employees will be trained in how to protect information correctly and how to develop and apply information security controls and (ii) training should target all colleagues and other business users in order to promote good information security behaviours.

b. Industry best practice standard ISO27001 which requires "all employees of an organisation and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organisational policies and procedures, as relevant to their job function".

c. Industry best practice standard NIST 800-50 which provides that organisations should "ensure that all individuals are appropriately trained in how to fulfil their security responsibilities before allowing them access to the system".

d. Guidance on "Security Outcomes" (2018) issued by the NCSC and the Commissioner recommends that organisations "give [their] staff appropriate support to help them manage personal data securely, including the technology they use. This includes relevant training and awareness as well as provision of the tools they need to effectively undertake their duties in ways that support the security of personal data*."*

e. Guidance on "Mitigating Malware and Ransomware attacks" (2020) issued by the NCSC recommends providing security education and awareness training as part of an in-depth approach to preventing ransomware.

70. Interserve ought reasonably to have been aware of the risks posed by failing to implement effective and appropriate security training for all employees prior to obtaining access to the IT system, in particular in circumstances where (i) the importance of training employees was well-known and documented, and (ii) Interserve's own policies required training of all employees. While the Commissioner acknowledges that the employee who opened the phishing email had in fact received appropriate training, he notes that the employee who forwarded the phishing email had not received such training. This deficiency exposed Interserve to risks of the kind giving rise to the Incident.

71. In these circumstances the failure to implement appropriate and effective information training contributed to a breach of Article 5(1)(f).

(5) Outdated protocols

72. At the time of the attack, SMB version 1 was in widespread use within Interserve's network. SMB version 1 had, however, been replaced by

SMB versions 2 and 3 which were recommended for use by the manufacturer, Microsoft, following the identification of vulnerabilities in SMB version 1.

73. The use of SMB version 1 was contrary to:

a. Interserve's Systems Management Policy which required Interserve to (i) adopt standardised secure builds that are regularly updated and enables secure functions and services and (ii) use secure technologies to protect necessary use of any vulnerable functions.

b. Interserve's Systems Management Standards which required Interserve to ensure (i) servers are to be built using a pre-configured standard and kept up to date, including the disabling of protocols inherently insecure and (ii) servers are to be kept up to date, use secure technologies to protect insecure services, and reviewed on a regular basis.

c. Industry best practices standard NIST 800-54 which requires organisations to "develop, document and maintain under configuration control, a current baseline configuration of the system; and to review and update the baseline configuration of the system at regular defined intervals".

d. Advice published by Microsoft TechNet in an article in 2016[15] which warned organisations against using SMB 1 on the basis that it did not contain key protections offered by later SMB protocol versions". Accordingly, from 2016 onwards Microsoft were recommending not to use SMB version 1.

[15] https://techcommunity.microsoft.com/t5/storage-at-microsoft/stop-using-smb1/ba-p/425858

74. Interserve ought reasonably to have been aware of the risks posed by failing to update protocol SMB 1, in particular in circumstances where (i) the risk of outdated protocols was well-known and documented, (ii) Interserve's Threat and Vulnerability policy required it to monitor external intelligence sources such as security vendors to protect against malware and Interserve therefore should have been aware of the weakness identified by the Microsoft TechNet article.

75. Further, at the time of the incident Interserve did not follow any hardening processes or standards.

76. In these circumstances the failure to update protocol SMB 1 contributed to a breach of Article 5(1)(f).

(6) Incident Response

77. Following the initial attack, the matter was not investigated by Interserve's Information Security Team. The reason for this failure put forward by Interserve is that it had been reported by the anti-virus software that it had removed the malicious software. In fact, the attacker retained access on the compromised account and was able to proceed with the second stage of the attack.

78. This was contrary to:

    a. Interserve's Incident Management Standards which required the following steps to be taken following an information security incident:

        i. "The recovery from information security incidents should involve: Rebuilding systems or networks to previously

known secure state (i.e. the same state they were in before the information security incident occurred)".

ii. "Following recovery from information security incidents reviews should be performed involving an information security specialist to undertake a root cause analysis of the information security incident" … "Ransomware attacks are the result of poor or defective security controls; therefore, the entire system should be viewed as untrusted …. If a malicious cyber actor has carried out a successful ransomware attack, questions must be raised about the possibility of more indirect and lasting impacts. For example, how many instances of the ransomware are still present in the system waiting to be activated? How should they be removed, and how should users be warned? Were other types of malware also deployed at the same time? What are they, what will they do and when".

b. Industry best practice standard ISO27001 which requires "information security incidents shall be responded to in accordance with the documented procedures".

c. Industry best practice standard ISO27002 requires the response should include "conducting information security forensic analysis, as required", "dealing with information security weakness(es) found to cause or contribute to the incident" and "post-incident analyses should take place, as necessary, to identify the source of the incident".

79. Interserve ought reasonably to have been aware of the risks posed by failing to investigate the initial attack in particular in circumstances where (i) the requirement for conducting analysis of the root cause and

source of a security incident was well-known and documented, and (ii) Interserve's own policies required such investigation.

80. In these circumstances the failure to conduct an effective and timely investigation into the cause of the initial attack contributed to a breach of Article 5(1)(f).

(7) Privileged Account Management

81. At the time of the Incident, Interserve had over 280 users within the domain administrator group. These users were given wide permissions within the organisation's domain by their line manager who approved the permissions, including in some instances the ability to uninstall antivirus software. Of these users, 12 were compromised by the attacker.

82. The number of users within the domain administrator group and process for approval is contrary to:

a. Interserve's Access Control Standard which required (i) individual approval for the use of special access privileges (e.g. by a sufficiently senior business representative), (ii) restricting the use of special access privileges to narrowly-defined circumstances and (iii) assigning users with default access based on the principle of least privilege.

b. Industry best practice standard NIST 800-53 requires organisations to "employ the principle of least privilege, allowing only authorised accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organisational tasks".

c. Guidance published by Microsoft in 1999, and updated in 2017 recommended not to have any users within the domain administrator group save for a disaster recovery user.

83. Interserve ought reasonably to have been aware of the risks posed by failing to ensure that the minimum number of users were given domain privileges only where strictly necessary in circumstances where (i) the requirement for conducting such restrictions was well known and documented, and (ii) Interserve's own policies required such limitations.

84. In these circumstances the failure to effectively manage privileged accounts access contributed to a breach of Article 5(1)(f).

85. As to the above matters, the Commissioner accepts that each of the above contraventions, if considered in isolation, are not necessarily causative of the Incident nor a serious contravention of Article 5(1)(f) justifying the imposition of a financial penalty, however the cumulative failures materially increased the risk of an attack occurring, and the seriousness of the consequences of an attack, and taken together do constitute a serious contravention of Article 5(1)(f).

Article 32

86. The Commissioner also finds that Interserve failed to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk as required by Article 32(1).

87. By virtue of the use of outdated operating systems, outdated protocols, ineffective endpoint security and the failure to ensure employees had undertaken phishing training (set out at paragraphs 54 – 63, 68 - 76 above), Interserve failed to implement appropriate technical and organisational measures to ensure the ongoing confidentiality, integrity,

availability and resilience of processing systems and services contrary to Article 32(1)(b).

88. Further, Interserve failed to implement appropriate technical and organisational measures to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident contrary to Article 32(1)(c).

89. In particular, the availability and access to personal data was not restored in a timely manner:

    a. Personal data stored on the iTrent system was unavailable from 2 May 2020 until 6 July 2020, with full user access being restored on 6 July 2020.

    b. Personal data stored on the AX12 system was unavailable from 2 May 2020 until 10 July 2020, with partial user access being restored on 13 July 2020 and full user access being restored on 28 July 2020.

    c. Personal data stored on the Fire Director system was unavailable from 2 May 2020 until 17 July 2020, with partial user access being restored on 28 August 2020 and full user access being restored on 28 October 2020.

    d. Personal data stored on the Profund system was unavailable from 2 May 2020 until 17 July 2020, with partial user access being restored on 28 August 2020 and full user access being restored on 20 January 2021.

90. [redacted]

[redacted]

91. By virtue of the matters set out at paragraphs 64 - 67 above, Interserve failed to implement appropriate technical and organisational measures for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing contrary to Article 32(1)(d).

Notice of Intent

92. On 27 April 2022, in accordance with s.155(5) and paragraphs 2 and 3 of Schedule 16 DPA, the Commissioner issued Interserve with a Notice of Intent to impose a penalty under s.155 DPA. The Notice of Intent described the circumstances and the nature of the personal data breach in question, explained the Commissioner's reasons for a proposed penalty, and invited written representations from Interserve.

93. On 18 May 2022, Interserve provided written representations in respect of the Notice of Intent.

94. The Commissioner subsequently notified Interserve that it intended to serve an updated Notice of Intent, which it did on 2 September 2022. The Commissioner invited Interserve to serve supplemental representations in response to this updated Notice of Intent.

95. On 4 October 2022, the Commissioner held a 'representations meeting' to thoroughly consider the representations provided by Interserve. At that meeting it was decided that a monetary penalty remained appropriate in all of the circumstances.

Factors relevant to whether a penalty is appropriate, and if so, the amount of the penalty

96. For the reasons set out above, the Commissioner's view is that Interserve has failed to comply with Article 5(1)(f) and Article 32 of the GDPR. This failure falls within the scope of section 149(2) and 155(1)(a) DPA. The Commissioner has considered the factors set out in Article 83(2) of the GDPR in deciding whether to issue a penalty. For the reasons given below, he is satisfied that (i) the contraventions are sufficiently serious to justify issuing a penalty in addition to exercising his corrective powers; and (ii) the contraventions are serious enough to justify a significant fine.

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

(i) Nature of the infringement

97. During the Incident, the relevant attackers were able to access the personal data of up to 113,000 employees including special category data, and the integrity of this data has been compromised. Further, for a period of up to three months data subjects were unable to obtain timely access to all of their personal data.

98. Whilst Interserve had adopted appropriate policies and standards directed at security, these were not effectively implemented or adhered to. Industry standards, such as ISO27001, highlight the importance of management oversight of adherence to policies including through the use of internal audits to confirm the information security management

system is effectively implemented and maintained together with senior management review of the security management systems at planned intervals to ensure its continuing suitability, adequacy and effectiveness. The Commissioner has not seen evidence of appropriate management oversight or review of security systems prior to the Incident.

99. Whilst the Commissioner recognises that Interserve did, at the time of the Incident, have in place some security measures, Interserve did not have an information security programme consistent with the requirements of the GDPR; namely a set of technical and organisational measures which, viewed holistically, ensured a level of security appropriate to the known risks, taking into account the state of the art, costs of implementation and the nature, scope, context and purpose of the processing it performs. Measures such as processing personal data on supported operating systems, removing legacy protocols, using endpoint protection, data protection training and appropriate incident response could have very significantly reduced the likelihood of personal data being compromised. The failure to implement such measures exposed that personal data to serious risks.

(ii) Gravity of the Infringement

100. The Commissioner takes the view that this was a significant contravention of the GDPR in particular having regard to the volume of personal data processed by Interserve and the nature of the personal data processed by Interserve including special category data. The volume and type of personal data being processed by Interserve required robust security measures to be put in place with appropriate controls and oversight.

101. Further, the infringement contributed towards the breach of personal data relating to up to 113,000 individuals.

102. The Commissioner is not persuaded that the gravity of the contravention is materially reduced by Interserve's financial constraints at the time of the Incident, in particular in circumstances where (i) some of the contraventions could have been avoided at no or low cost, (ii) additional measures, such as those taken following the Incident, would have entailed significant costs, but those costs were proportionate to the scale and nature of the personal data Interserve was processing, (iii) industry standards of best practice, for example ISO27001 requires leadership to ensure resources are provided to achieve security policies, (iv) appropriate risk assessments could have been undertaken to identify the risks involved in not complying and/or modifying the relevant policies but were not.

(iii) Duration of the infringement

103. The seven identified infringements set out above at paragraphs 54 - 85 vary in duration.

104. Some of the matters pre-date the point when Interserve became the relevant data controller in respect of the personal data processed by Interserve and its related group companies with effect from 18 March 2019 when it became the parent company of the Interserve group. Accordingly, the earliest start date in respect of the following infringements is 18 March 2019.

a. The processing of personal data on unsupported servers.

b. The continued use of SMB version 1 namely out-of-date protocols.

c. The failure to run up-to-date anti-virus software.

d. The failure to carry out regular vulnerability scans and penetration testing.

e. The existence of numerous users within the domain administrator group.

105. The Commissioner considers that those matters constituted infringements from the period 18 March 2019 until 1 December 2020 when remediation measures had been completed.

106. Interserve's failure to properly investigate the initial attack was of relatively short duration.

The number of data subjects affected and the level of damage suffered by them

107. The personal data of up to 113,000 individuals was compromised by the data breach.

108. All the data subjects had their personal data processed unlawfully, and the potential for concern, anxiety and stress that could be suffered by the data subjects is exacerbated in the following circumstances:

a. Personal data has been unlawfully accessed by criminal actors with malicious intent. [redacted]

b. The personal data which was compromised included personal data commonly used to facilitate identity and financial fraud, including home addresses, bank account details, pay slips, passport data and national insurance numbers.

c. Special category data including sexual orientation, disabilities (health) and religion were compromised by criminal actors. Recital 51 of the GDPR explains that special category data are, by their nature, particularly sensitive to a person's fundamental rights and freedoms. Whilst employees may be content with sharing this personal data in the context of their employment it is unlikely individuals would want this data to be accessed by malicious individuals.

d. The compromised database included salary details of individuals. This type of personal data can enable social and financial profiling, which is particularly dangerous in the hands of criminal actors.

e. Interserve has stated that there is no evidence of data exfiltration and the investigations it carried out, together with those carried out by its external expert advisors, had not identified any evidence of data exfiltration. The Commissioner notes that there is no direct evidence of exfiltration or of data being used to cause detriment to affected data subjects. However, this possibility cannot be completely ruled out, and the risks of exfiltration remain significant given that (i) the privileged accounts were capable of exfiltrating data, (ii) advanced attack groups use covert methods to prevent the detection and evidence of exfiltration, (iii) measures that can identify data exfiltration including firewall filtering and logging of endpoints were not implemented by Interserve until after the incident. Therefore individuals do not know if or how they may be targeted in future, for example targeted with identity theft.

109. Further, for a period of up to three months data subjects were unable to exercise full control over their personal data, for example, to exercise data subjects rights in respect of all of their personal data.

110. For completeness, the Commissioner records that he received one complaint in relation to the personal data breach. Interserve received communications in relation to the incident as follows: (i) 11 written queries, (ii) 37 phone calls to a dedicated helpline and 44 phone calls to a separate pension helpline, (iii) 1 communication from a trade union and (iv) 1 communication from a legal representative of a data subject. These raised a range of queries including what personal data was being processed by Interserve and whether a particular individual's personal data had been accessed during the cyber-attack.

(b) the intentional or negligent character of the infringement

111. The Commissioner considers that whilst the Incident was not intentional or deliberate, the infringements are the result of negligence. In particular:

a. Interserve failed to adequately consider the requirement to protect personal data.

b. Interserve failed to take reasonable steps to ensure appropriate oversight of their policies and standards designed to protect personal data.

c. Interserve failed to take reasonable care in ensuring that their policies designed to protect personal data were properly implemented.

d. Interserve's senior management did not have adequate oversight that its policies were being adhered to or of the systems and software in use.

e. Interserve's size, and particularly the size of its workforce and the volume and nature of personal data it processed about that workforce, meant that higher standards of security are expected of it than would be expected of a much smaller organisation.

112. At all material times Interserve was aware or should reasonably have been aware of the published guidance documents identified above in relation to the measures required to protect personal data, and in particular the Commissioner's GDPR guidance to which it had previously been directed in response to personal data breaches.

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

113. Whilst Interserve took the view that the breach did not meet the high-risk threshold for data subject notification, it still notified individuals in line with the requirements of Article 34.

114. Interserve engaged two Incident Response Investigators to support the Interserve investigation which provided professional support. Further, Interserve notified the NSCS and NCA during its incident response which supported the response and law enforcement action.

115. Interserve engaged third party monitoring of dark web activity to identify any evidence of personal data or Interserve. No such evidence has been found to date.

116. Interserve restored personal data, ensuring that individuals could still exercise their rights, although this was not undertaken in a timely manner.

117. Interserve has made substantial financial investments in raising its security standards since the incident. However, those steps could and should have been taken much earlier.

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

118. It is noted that Interserve was responsible for the security of its systems and the protection of personal data.

119. Interserve failed in its obligations under Article 5(1)(f) to have regard to considerations including the state of the art, likelihood of attack, its severity and what appropriate controls were available at the time.

120. Article 32 of the GDPR requires organisations to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks presented by their processing; to include the potential impacts these risks may have on the rights and freedoms of natural persons.

121. The infringements of Article 32 relied on by the Commissioner at paragraphs 86 – 91 above are repeated. The Commissioner also repeats that Interserve's size, and particularly the size of its workforce and the volume and nature of personal data it processed about that workforce, meant that higher standards of security are expected of it than would be expected of a much smaller organisation.

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

122. The Commissioner has not identified any relevant previous infringements by Interserve to date. However, in April and May 2019 the Commissioner

was notified by Interserve of two personal data breaches which resulted in Interserve being notified of the Commissioner's GDPR guidance, including Security Guidance.

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

123. Interserve has fully co-operated with the Commissioner during the investigation and provided evidence upon request.

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

124. The personal data affected by the incident comprised a wide spectrum of information held as part of employee personnel records including special category data. The categories of personal data affected are summarised at paragraphs 48 - 50 above.

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

125. The infringement was self-reported in a timely manner to the Commissioner and NCA by Interserve.

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

126. Not applicable.

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

127. Not applicable.

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

128. The Commissioner has considered the following **aggravating factor** in this case:

- Whilst Interserve has not been the subject of any previous regulatory action by the Commissioner, it is noted that Interserve has been the subject of two previous personal data breach incidents in 2019 which resulted in reports to the Commissioner. On both occasions the Commissioner directed Interserve to review the Commissioner's GDPR security guidance and on one occasion to advice of the importance of employee training in respect of managing phishing attacks.

129. The Commissioner has taken into account the following **mitigating factors**:

(1) Remediation

130. Interserve has independently and pro-actively addressed the areas of non-compliance identified by the Commissioner including taking the following steps by 1 December 2020 at a cost of [redacted]:

a. Updated servers, on-going client devices are now updated to [redacted], and outdated servers that are not updated have been isolated in a secure area.

b. Rolled out new enterprise level Endpoint Protection ([redacted]).

c. Disabled SMB version 1.

d. Reduced the number of users within the domain administrator group.

e. Implemented vulnerability scanning, improvements to email scanning, Network Segmentation and the enabling of host firewalls, improvements to email security, improvements to the security of its domain controllers and end-points.

f. Appointing a Chief Information Officer in May 2020, Chief Information Security Officer in June 2020 and Data Protection Officer in September 2020.

g. Implemented an Information Security Governance and Management Structure which reports into an Information Security Management Committee.

h. Implemented a new risk reporting and governance system which has identified 33 improvements across the Interserve business.

(2) Extent to which the non-compliance results from the coronavirus pandemic.

131. The Commissioner's updated regulatory action policy in response to the COVID-19 pandemic was published on 15 April 2020, and reviewed and updated in July 2020 stating that "in deciding whether to take formal regulatory action, we will consider whether the organisation's non-compliance results from the coronavirus pandemic".

132. The Commissioner has taken into account that when the relevant employee clicked on the phishing link which downloaded the ransomware software, this was not protected by Interserve's corporate Internet Filtering because the employee was working at home through a split tunnelling arrangement. This arrangement meant that activities other that essential traffic undertaken by the employee were routed through the employee's own internet connection. In normal circumstances the phishing link would have been blocked by Interserve's Internet Filtering but was not blocked by the employee's own arrangements.

133. However, whilst the Covid-19 pandemic may have given the malicious actors the opportunity to access the Interserve network, they were able to exploit negligent security practices within the network to unlawfully access and encrypt personal data.

134. The Commissioner has also taken into account that the restoration of personal data was in part delayed by the Covid-19 pandemic by reason of (i) IT staff being unable to attend the office and (ii) the incident response team working remotely. However, these matters do not fully explain the significant delays in restoring personal data. The lack of appropriate measures including offline back-ups was a more significant factor in the delay.

Summary and amount of the penalty

135. For the reasons set out above, the Commissioner has decided to impose a financial penalty on Interserve. Taken together the findings above concerning the infringements, and the fact that Interserve failed to comply with its GDPR obligations, the Commissioner considers it appropriate to apply an effective, dissuasive and proportionate penalty reflecting the seriousness of the breaches which have occurred. In making this decision, the Commissioner has given due regard to the representations made by Interserve following receipt of the Notice of Intent dated 27 April 2022, and the updated Notice of Intent dated 2 September 2022.

Calculation of Penalty

136. Following the 'Five Step' process set out in the RAP the calculation of the proposed penalty is as follows.

Step 1: An initial element removing any financial gain from the breach.

137. There is no evidence of financial gain from the infringement.

Step 2: Adding in an element to censure the breach based on its scale and severity, taking into account the considerations identified at section 155(2)-(4) DPA.

138. Sections 155(2)-(4) DPA refer to and reproduce the matters listed in Articles 83(1) and 83(2).

(1) The nature, gravity and duration of the failure (Article 83(2)(a))

139. This was a significant and multi-faceted contravention of the GDPR, in which the contraventions continued for a significant period of time. The

infringements enabled a cyber attacker to unlawfully access Interserve's IT systems and compromise the personal data, including special category data, of up to 113,000 employees or alternatively created a very real risk of such consequences occurring. Paragraphs 97 – 110 above are repeated.

140. In light of these matters, the Commissioner considers that an appropriate starting point for the penalty should be £4,000,000 (four million pounds).

(2) The intentional or negligent character of the infringement (Article 83(2)(b))

141. Paragraphs 111 - 112 above are repeated. Whilst the infringements were not deliberate, Interserve was negligent for the purposes of Article 83(2)(b). The Commissioner considers that, in the circumstances, this did not increase or reduce the assessment of the overall seriousness of the infringement and does not affect the starting point of the penalty.

(3) Any action taken by the controller or processor to mitigate the damage suffered by data subjects (Article 83(2)(c))

142. Paragraphs 113 – 117 above are repeated. In light of the remedial steps taken, the Commissioner considers that a reduction in the penalty starting point from £4,000,000 to £3,500,000 is appropriate.

(4) The degree of responsibility of the controller or processor (Article 83(2)(d))

143. Paragraphs 118 - 121 above are repeated. In light of the fact that the infringements occurred as a result of the failure to properly implement its policies and standards, the size of the controller and its workforce and

that some of the failings constituted basic security requirements which could have been rectified without significant cost, the Commissioner finds that an increase to the starting point of the penalty is justified. The Commissioner is further concerned that Interserve appears to have failed to take account of publicly available guidance, which would have alerted Interserve to its failings. The Commissioner considers that an increase from £3,500,000 to £4,500,000 is appropriate.

(5) Relevant previous infringements (Article 83(2)(e))

144. Paragraph 122 above is repeated. No further adjustment in considering this factor was appropriate.

(6) Degree of cooperation with supervisory authority (Article 83(2)(f))

145. Paragraph 123 above is repeated. The Commissioner recognises that Interserve has fully co-operated with the investigation, and in particular spent significant sums to improve cyber security to date. The Commissioner further acknowledges that some of its improvements went beyond the scope of the failings highlighted by the incident. The scale of response justifies a decrease from £4,500,000 to £4,400,000.

(7) Categories of personal data affected (Article 83(2)(g))

146. Paragraphs 48-50 and 124 above are repeated. The personal data affected included special category data, which has been considered as part of the nature and gravity of the infringement. The Commissioner recognises that there is no evidence that the data accessed has been used to cause damage to any data subjects, and accordingly no further adjustment in considering this factor was appropriate.

(8) Manner in which the infringement became known to the Commissioner (Article 83(2)(h))

147. Paragraph 125 above is repeated. No further adjustment in considering this factor was appropriate.

(9) Adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42 (Article 83(2)(j))

148. No further adjustment in considering this factor was appropriate.

(10) 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 (Article 83(2)(k))

149. Beyond the matters already taken into account, there were no additional aggravating or mitigating features.

(11) Conclusion at step 2

150. Having regard to (a) the matters set out in the preceding sections of this Notice, (b) the matters referred to in this section and (c) the need to apply an effective, proportionate and dissuasive fine, the Commissioner considers that a penalty starting point of £4,400,000 (four million, four hundred thousand pounds) is appropriate.

Step 3: Adding in an element to reflect any aggravating factors (Article 83(2)(k)).

151. There were no additional matters beyond those already taken into account above that required an increase in the proposed penalty. No adjustment is made to the penalty level determined at Step 2.

Step 4: Adding an amount for deterrent effect to others.

152. As to the need for an effective deterrent, the Commissioner considers that a fine, accompanied by appropriate communications in accordance with the Communicating Regulating Enforcement Action Policy, would serve as an effective deterrent. The Commissioner does not consider there is a requirement to increase the penalty level for a deterrent effect on others.

Step 5: Reducing the amount to reflect any mitigating factors including ability to pay.

153. The Commissioner does not consider that there are any mitigating factors, beyond those referenced in the sections above, which would cause a reduction in the proposed penalty amount.

154. Having considered the information provided by Interserve in relation to its financial position, there is insufficient evidence that Interserve would be unable to pay the proposed penalty such that it would not be appropriate to impose a penalty of that sum.

155. Taking into account all of the factors set out above, the Commissioner has decided to impose a penalty on Interserve of **£4,400,000** (**four million, four hundred thousand pounds**), on the basis that this would be effective, dissuasive and proportionate given the failings identified, the current status of the company and steps taken to improve measures which mitigate the future risk to data subjects**.**

156. In reaching this decision, the Commissioner has had regard to the factors set out in section 108 of the Deregulation Act 2015. This includes the risks to economic growth; the likely impact of the proposed intervention on the business, and the likely impact of the proposed intervention on the wider business community, both in terms of deterring non-compliance and economic benefits to legitimate businesses.

Payment of the penalty

157. The penalty must be paid to the Commissioner's office by BACS transfer or cheque by **21 November 2022** at the latest. The penalty is not kept by the Commissioner but will be paid into the Consolidated Fund which is the Government's general bank account at the Bank of England.

158. There is a right of appeal to the First-tier Tribunal (Information Rights) against:

(a) The imposition of the penalty; and/or,
(b) The amount of the penalty specified in the penalty notice

159. Any notice of appeal should be received by the Tribunal within 28 days of the date of this penalty notice.

160. The Commissioner will not take action to enforce a penalty unless:

- the period specified within the notice within which a penalty must be paid has expired and all or any of the penalty has not been paid;

- all relevant appeals against the penalty notice and any variation of it have either been decided or withdrawn; and

- the period for appealing against the penalty and any variation of it has expired.

161. In England, Wales and Northern Ireland, the penalty is recoverable by Order of the County Court or the High Court. In Scotland, the penalty can be enforced in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court of any sheriffdom in Scotland.

162. Your attention is drawn to Annex 1 to this Notice, which sets out details of your rights of appeal under s.162 DPA.

Dated the 19th day of October 2022.

Stephen Eckersley
Director of Investigations
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

Rights of appeal against decisions of the Commissioner

1. Section 162 of the Data Protection Act 2018 gives any person upon whom a penalty notice or variation notice has been served a right of appeal to the First-tier Tribunal (Information Rights) (the 'Tribunal') against the notice.

2. If you decide to appeal and if the Tribunal considers:-

   a) that the notice against which the appeal is brought is not in accordance with the law; or

   b) to the extent that the notice involved an exercise of discretion by the Commissioner, that he ought to have exercised his discretion differently,

   the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.

3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

   GRC & GRP Tribunals
   PO Box 9300
   Arnhem House
   31 Waterloo Way
   Leicester
   LE1 8DJ

   Telephone: 0203 936 8963
   Email: grc@justice.gov.uk

a) The notice of appeal should be sent so it is received by the Tribunal within 28 days of the date of the notice.

b) If your notice of appeal is late the Tribunal will not admit it unless the Tribunal has extended the time for complying with this rule.

4. The notice of appeal should state:-

a) your name and address/name and address of your representative (if any);

b) an address where documents may be sent or delivered to you;

c) the name and address of the Information Commissioner;

d) details of the decision to which the proceedings relate;

e) the result that you are seeking;

f) the grounds on which you rely;

g) you must provide with the notice of appeal a copy of the penalty notice or variation notice;

h) if you have exceeded the time limit mentioned above the notice of appeal must include a request for an extension of time and the reason why the notice of appeal was not provided in time.

5. Before deciding whether or not to appeal you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may

conduct his case himself or may be represented by any person whom he may appoint for that purpose.

6. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 162 and 163 of, and Schedule 16 to, the Data Protection Act 2018, and Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).