For Public Release

PENALTY NOTICE

DPP LAW LTD

14 April 2025

DATA PROTECTION ACT 2018

ENFORCEMENT POWERS OF THE INFORMATION COMMISSIONER

PENALTY NOTICE

To: DPP Law Ltd

Of: Pinnacle House,
Stanley Road,
Bootle L20 7JF

I. INTRODUCTION AND SUMMARY

1. Pursuant to section 155(1) of the Data Protection Act 2018 ("**DPA**"), the Information Commissioner (the "**Commissioner**"), by this written notice ("**Penalty Notice**") requires DPP Law Ltd ("**DPP**") to pay the Commissioner £60,000.

2. This Penalty Notice is given in respect of infringements of the UK General Data Protection Regulation ("**UK GDPR**").[1] It contains the reasons why the Commissioner has decided to impose a penalty, including the circumstances of the infringements and the nature of the personal data involved.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

For the period 25 May 2018 to 31 December 2020, references in this Penalty Notice to the UK GDPR should be read as references to the GDPR (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) as it applied in the UK during that period.

3. On 11 December 2024, in accordance with paragraph 2 of Schedule 16 to the DPA, the Commissioner issued DPP with a Notice of Intent which set out the Commissioner's reasons for proposing to issue a penalty notice. In that notice, the Commissioner indicated that the amount of the penalty he proposed to impose was £60,000.

4. On 29 January 2025, DPP provided written representations about the Commissioner's Notice of Intent to issue a penalty notice. In reaching the decision to issue this Penalty Notice, the Commissioner has taken full account of DPP's representations and, where appropriate, the Penalty Notice makes specific reference to them.

5. The Commissioner finds that DPP has infringed Articles 5(1)(f), 32(1), 32(2) and 33(1) UK GDPR for the reasons set out in this Penalty Notice. In summary:

    a) The infringements of Articles 5(1)(f), 32(1), 32(2) and 33(1) UK GDPR relate to DPP's provision of legal services to its clients (the "**Relevant Processing**"). In particular, the processing of personal data relating to DPP's clients and experts instructed to give evidence in legal proceedings to which DPP's clients were a party.

    b) The infringements of Articles 5(1)(f), 32(1) and 32(2) UK GDPR occurred because the Relevant Processing was not carried out in a manner that ensured appropriate security of the personal data of DPP's clients and experts, including protection against unauthorised processing, and using appropriate technical and organisational measures as required by Articles 5(1)(f), 32(1) and 32(2) UK GDPR. In particular, DPP failed to adopt the principle of least privilege and failed to regularly audit administrative accounts on its network.

c) As a consequence of DPP not having appropriate security measures in place as required by Articles 5(1)(f), 32(1) and 32(2) UK GDPR, the personal data of 791 individuals (clients and experts) were exfiltrated by a threat actor and posted on the dark web (the "**Cyber Incident**").

d) The infringement of Article 33(1) UK GDPR occurred because DPP did not notify the Commissioner without undue delay or within 72 hours of becoming aware of the personal data breach (i.e. that there was a loss of access to the personal data it was processing and this was likely to result in a risk to data subjects). By focusing its efforts on bringing its systems back online and neglecting to undertake an assessment of the risks posed to data subjects, DPP did not notify the Commissioner until 43 days after the Cyber Incident. Furthermore, DPP demonstrated a lack of understanding of its obligation to notify the Commissioner of a personal data breach in accordance with Article 33 UK GDPR.[2]

6. This Penalty Notice is issued in respect of the infringements on the basis that, in all the circumstances, and having regard to the matters listed in Articles 83(1) and 83(2) UK GDPR, a financial penalty in the sum of £60,000 is an effective, proportionate and dissuasive measure.

II. RELEVANT LEGAL FRAMEWORK

7. Section 155(1) DPA provides that, if the Commissioner is satisfied that a person has failed, or is failing, as described in section 149(2) DPA, the Commissioner may, by written penalty notice, require the person to pay to the Commissioner an amount in sterling specified in the penalty notice.

[2] Telephone attendance ICO & DPP 21 July 2022; DPP Response to ICO 7 September 2022, Q1a.

8. The types of failure described in section 149(2) DPA include, at section 149(2)(a), "*where a controller or processor has failed, or is failing, to comply with… a provision of Chapter II of the UK GDPR… (principles of processing)*" and at section 149(2)(c), "*where a controller or processor has failed, or is failing, to comply with… a provision of Articles 25 to 39 of the UK GDPR… (obligations of controllers and processors).*"

9. Chapter II UK GDPR sets out the principles relating to the processing of personal data that controllers must comply with. Article 5(1) UK GDPR lists these principles and includes the requirement at Article 5(1)(f) UK GDPR 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*". This is referred to in the UK GDPR as the "*integrity and confidentiality"* principle.

10. Article 32 UK GDPR (security of processing) materially provides:

> *"(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…*
>
> *(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".*

11. Article 33(1) UK GDPR (notification of a personal data breach) provides:

> *"In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification under this paragraph is not made within 72 hours, it shall be accompanied by reasons for the delay".*

12. Article 4(1) UK GDPR defines a personal data breach as:

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

13. The legal framework for setting penalties is set out in Section V: 'Decision to impose a penalty' below.

III. BACKGROUND TO THE INFRINGEMENTS

14. This section summarises the relevant background to the findings of infringement. It does not seek to provide an exhaustive account of all the details of the events that have led to the issue of this Penalty Notice.

15. DPP is a law firm, headquartered in Bootle, England. It employs fewer than 250 staff and has offices in Birmingham, Bootle, Liverpool, London and Tolworth. It specialises in the practice of law related to crime, military, family fraud, sexual offences and actions against the police.[3]

[3] https://dpp-law.com

A. Cyber Incident

16. On 4 June 2022 at approximately 11:30, DPP's email server stopped working and staff had no access to DPP's IT network.[4] DPP's in-house IT manager established that all files across its servers had been corrupted.[5] DPP's external IT supplier believed that DPP had suffered a ransomware incident, despite not receiving any payment demands.[6]

17. The timeline of events leading up to (and following) the Cyber Incident was as follows:

19 February 2022

18. DPP told the Commissioner that, following an analysis of log files by a third party consulting firm, there was evidence to suggest brute force attempts on its network as early as 19 February 2022.[7] This occurred a further 12 times and there were in total 400 attempts to gain access to the network.[8] The brute force incidents were targeted at an administrator account for a legacy case management system (see further points on 'sqluser' below at paragraph 25 to 28) which was only available online sporadically.[9]

3 June 2022

19. An administrator account, sqluser, authenticated onto [redacted].[10] It is considered likely that an end-user laptop was compromised by the threat actor and subsequently authenticated onto the network. It was this compromise that allowed the threat actor to access sqluser.[11] Following this login, there are indicators

[4] DPP Response to ICO, 7 September 2022, Q1a; DPP Breach Report, 17 July 2022.
[5] DPP Response to ICO, 7 September 2022, Q1a; DPP Breach Report, 17 July 2022.
[6] DPP Response to ICO, 7 September 2022, Q1a, Q1b; DPP Breach Report, 17 July 2022.
[7] Secore Consulting, Incident Response – Log File Analysis, 20 June 2022, p. 11.
[8] Secore Consulting, Incident Response – Log File Analysis, 20 June 2022, p. 5-6.
[9] DPP Response to ICO, 18 August 2022, Q3.
[10] Secore Consulting, Incident Response – Log File Analysis, 20 June 2022, p. 4, 9.
[11] DPP Response to ICO, 7 September 2022, Q2, Q5.

that Cobalt Strike was deployed onto the network and the threat actor began running PowerShell commands.[12] At the time of the incident DPP had multi-factor authentication ("**MFA**") for the purposes of connecting to its network via a VPN.[13] However, the administrator account, sqluser, did not have MFA due to its role as a service-based account.[14]

4 June 2022

20. DPP's email server stopped working but incoming emails remained available through its firewall.[15,16] In the early hours, logs show Windows Defender being disabled on [redacted] and a Virtual Machine backup service stopping on [redacted].[17] Forensic investigators believe at this point the threat actor deployed ransomware.[18]

21. During the incident MegaSync and Rclone software were installed on [redacted].[19] The threat actor utilised tools to perform the exfiltration of data from the network. Towards the end of the incident the threat actor utilised the administrator account, sqluser, to download and run an anti-virus which acted as a form of clean-up for the incident (and thus making the incident response investigation more difficult).[20]

5 June 2022 to 12 June 2022

22. DPP reviewed firewall and server logs and it assessed that no data had been exfiltrated.[21] At the time of the Cyber Incident, DPP's firewall logs did not record egress data flows, it would therefore not have been possible for DPP to ascertain if data had in fact been exfiltrated. DPP established that data was recoverable by off-site backups within 24

[12] Secore Consulting, Incident Response – Log File Analysis, 20 June 2022, p. 4.
[13] DPP correspondence dated 18 August 2022.
[14] DPP Response to ICO, 2 October 2023, Q5.
[15] DPP Breach Report, 17 July 2022.
[16] DPP Written Representations, 29 January 2025, p.2.
[17] Secore Consulting, Incident Response – Log File Analysis, 20 June 2022, p. 4-5, 7.
[18] Secore Consulting, Incident Response – Log File Analysis, 20 June 2022, p. 4-5.
[19] Secureworks, Cyber Incident Response Summary of Findings, 9 August 2022, p. 2.
[20] Secureworks, Cyber Incident Response Summary of Findings, 9 August 2022, p. 3.
[21] DPP Response to ICO, 7 September 2022, Q1b.

hours. However, DPP's systems were not operating properly for around one week leaving it unable to access the personal data it was processing. Whilst DPP staff did not have access to DPP's case management software for eight days, DPP told the Commissioner that staff retained the ability to access, and respond to, incoming emails with no impact on client cases.[22]

15 July 2022

23. The National Crime Agency ("**NCA**") contacted DPP to advise them that three folders of DPP's data, totalling 32.4Gb, had been published on the dark web. This included court bundles, PDFs, Word documents, photos and video (including police body cam footage) relating to DPP's clients and experts instructed to give evidence in legal proceedings to which DPP's clients were a party.

17 July 2022

24. 43 days after the Cyber Incident, DPP reported the personal data breach to the Commissioner. DPP were unaware that the loss of access to personal data constituted a personal data breach and therefore that they were required to notify the Commissioner about the Cyber Incident.

B. Sqluser account

25. Sqluser was an administrator account for a legacy case management system. The account was setup by FWBS Ltd (subsequently acquired by Thomson Reuters) in 2001 for the purposes of automating communication between DPP's servers.[23] Despite having a limited role on the network, it had full administrator rights (i.e. unrestricted access) across DPP's network.[24] DPP were aware of the sqluser account as far

[22] DPP Written Representations, 29 January 2025, p.2.
[23] DPP Response to ICO, 7 September 2022, Q3a; DPP Response to ICO, 6 October 2022, Q5; DPP Response to ICO, 2 October 2023, Q1c.
[24] DPP Response to ICO, 31 March 2023, Q7; DPP Response to ICO, 2 October 2023, Q5.

back as 2011.[25] DPP told the Commissioner that previous attempts to change the password had blocked access to the legacy case management system.[26] DPP did not know the password and could not reset it.[27] The password was only known by FWBS Ltd/Thomson Reuters.

26. DPP stated that they did not conduct a risk assessment to understand the risks associated with the sqluser account because FWBS Ltd told them that the sqluser account was *"critical to the data replication of the servers"* and because DPP was *"reliant on our suppliers for the correct functioning and protection of our system"*.[28]

27. The legacy case management system was taken out of service on 30 April 2019 as DPP changed case management systems to DPS Software Ltd.[29] DPP's service agreement for the sqluser account later came to an end in 2021. However, due to DPP's data retention policy of six years, this system was still operational as DPP needed to access data in the system.[30] DPP stated that its retention policy was in accordance with guidance issued by the Solicitors Regulation Authority (**SRA**).

28. The threat actor used sqluser to authenticate onto [redacted], a remote desktop machine that facilitated access to the legacy case management system (as outlined above in paragraph 19). By compromising the sqluser account the threat actor was able to perform lateral movement across DPP's network.

C. Post-Cyber Incident

29. DPP subsequently moved its complete case management, accounts and email system to a managed hosted environment operated by its case

[25] DPP Email to ICO, 8 February 2024.
[26] DPP Email to ICO, 8 February 2024.
[27] DPP Response to ICO, 7 September 2022, Q3b.
[28] DPP Email to ICO, 8 February 2024.
[29] DPP Response to ICO, 7 September 2022, Q3a; DPP Response to ICO, 2 October 2023, Q1c; DPP Email to ICO, 8 February 2024.
[30] DPP Response to ICO, 6 October 2022, Q2.

management software suppliers, The Access Group.[31] This supplier controls all security aspects including the use of Microsoft 365 MFA.

30. DPP suspended sqluser from the DPP network and it is now only accessible [redacted].[32] In its report into the Cyber Incident, a second consultancy firm instructed by DPP also recommended that DPP mandates MFA for all remote access methods (a process that was ongoing at the time of the Cyber Incident).[33]

31. In the months following the Cyber Incident, DPP sent notifications to affected data subjects, in line with its obligations under Article 34 UK GDPR.

IV. THE COMMISSIONER'S FINDINGS OF INFRINGEMENT

A. Controllership and jurisdiction

32. DPP was the controller in respect of the Relevant Processing.[34] DPP determined the purpose and means within the meaning of Article 4(7) UK GDPR.

33. The UK GDPR applied to the Relevant Processing by virtue of Articles 2(1) and 3(1) UK GDPR. The Relevant Processing was structured processing of personal data, it took place in the context of the activities of a controller established in the UK, and none of the exceptions in Article 2 UK GDPR applied.

34. Part 2 of the DPA applied to the Relevant Processing by virtue of section 4 DPA.

B. Nature of the personal data and context of the Relevant Processing

[31] DPP Response to ICO, 2 October 2023, Q3.
[32] DPP Responses to ICO, 7 September 2022, Q4h and 2 October 2023, 23c.
[33] Secureworks Incident Response Summary Report dated 18 August 2022 (p.5).
[34] The processing of personal data of DPP's clients and experts that took place in DPP's provision of legal services to clients.

35. DPP processes personal data in order to provide legal services to its clients. This includes personal data relating to its clients and ongoing court cases. As a law firm that specialises in criminal defence (including sexual offences), family law and actions against the police, DPP processes highly sensitive personal data, including special category data (e.g. data concerning a natural person's sex life), DNA data, legally privileged information and allegations of criminal offences (including child sexual abuse).

36. This information is likely to reveal private details about individuals, including the offences of which they are accused and DPP's confidential legal advice. As a law firm, DPP has responsibilities to its clients both as a data controller and as a law firm to protect the personal data that it processes, particularly that which is protected by legal privilege.

37. Several categories of DPP's clients are vulnerable, including children and victims of sexual offences. Recital 38 of UK GDPR explains that children merit specific protection with regard to their personal data.

C. The infringements: Articles 5(1)(f) and 32 UK GDPR

38. The fact that the Cyber Incident took place is not, in and of itself, sufficient to make a finding that DPP has infringed Articles 5(1)(f) and 32 UK GDPR.[35] The Commissioner has considered whether the facts set out at paragraphs 16 to 31 above constitute infringements of the UK GDPR.

39. In order to assess DPP's compliance with Articles 5(1)(f) and 32 UK GDPR, the Commissioner must necessarily exercise his judgement, as a regulator, as to what "*appropriate*" security and "*appropriate*" technical and organisational measures would be in the circumstances (that is,

[35] See the CJEU's recent judgment in *VB v Natsionalna agentsia za prihodite* (Case C-340/21) at paragraphs 22-39, which the Commissioner has had regard to.

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*").

40. For the reasons set out below, the Commissioner's view is that DPP has infringed Articles 5(1)(f), 32(1) and 32(2) UK GDPR. The infringements involved DPP's failure to use appropriate technical and organisational measures to ensure appropriate security of the personal data subject to the Relevant Processing.

Appropriate security of the personal data

41. In assessing the "*appropriate security of the personal data*" under Article 5(1)(f) UK GDPR (and, equivalently, the "*level of security appropriate to the risk*" under Article 32 UK GDPR), the Commissioner has considered the risk to the rights and freedoms of DPP's clients and experts which the Relevant Processing presented. Recital 75 UK GDPR states that such risk "*may result from personal data processing which could lead to physical, material or non-material damage*".

42. As explained in paragraphs 35 to 37, DPP processes highly sensitive personal data relating to its clients. The disclosure of this personal data to the public is likely to result in a high risk to the rights and freedoms of DPP's clients, in particular:

    a) It risked jeopardising ongoing criminal proceedings in that details of privileged legal communications between DPP and its clients may now be in the hands of malicious actors.

    b) It risked identifying DPP's crime clients under criminal investigation, but who had not been charged, in circumstances

where they had a reasonable expectation of privacy in respect of that investigation.[36]

c) DPP's instructions included identities of victims and witnesses of crime. It therefore risked enabling the identification of individuals afforded statutory protection through the legal process. For example:

i. victims of sexual offences;[37]
ii. child victims and witnesses of crime.[38]

d) The highly sensitive nature of the personal data processed by DPP may leave its clients susceptible to bad actors exploiting that information for their own nefarious purposes.

43. The Commissioner considers all three categories of damage as identified in Recital 75 UK GDPR (physical, material and non-material) would be likely to flow from the risks identified at paragraph 42 above.

44. Recital 75 provides certain examples of damage. Of those examples, the Commissioner considers the following examples of damage were reasonably foreseeable from the Cyber Incident given the categories of personal data processed by DPP (see paragraph 35) and the risks identified at paragraph 42 above:

a) Loss of control over personal data.
b) Deprivation of rights and freedoms (right to life, right to respect for private and family life, peaceful enjoyment of property).
c) Loss of confidentiality of personal data protected by professional secrecy.
d) Financial loss.

[36] See ZXC v Bloomberg [2022] UKSC 5.
[37] See section 1 Sexual Offences (Amendment) Act 1992.
[38] See sections 44-45A Youth Justice and Criminal Evidence Act 1999; sections 39, 49 Children and Young Persons Act 1933.

e) Damage to reputation.

45. Paragraphs 85 to 91 below set out the types of damage which materialised as a result of the Cyber Incident.

46. In ensuring a level of security appropriate to the risk, Article 32(1) UK GDPR requires a controller to take into account the likelihood and severity of the risk to the rights and freedoms of data subjects.

47. Regarding the likelihood of the risk, DPP should have been aware that any unauthorised access to confidential information relating to ongoing criminal cases was likely to jeopardise such cases, including heightening reputational risks and risking the identification of individuals afforded protection (e.g. victims of sexual assault).

48. The factors above indicate that a high level of security was appropriate to the risk presented by the Relevant Processing. DPP was required to implement appropriate technical and organisational measures to ensure this high level of security.

49. The Commissioner notes that guidance is widely available to assist organisations (such as DPP) to make decisions on the implementation of appropriate technical and organisational measures to ensure the secure processing of personal data. For example:

a) The Commissioner's guidance on ransomware[39] relevantly provides:

i. "The security of privileged accounts should be a high priority for you. Basic account hygiene can support you in protecting these accounts, such as:

- *regular reviews of permissions;*

[39] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/ransomware-and-data-protection-compliance/.

- *following the principle of least privilege;*
- *risk assessments of membership into privileged groups; and*
- *senior level approval of privileged group membership."*

ii. Organisations should *"regularly audit… user accounts to ensure they are still required and contain the appropriate privileges".*[40]

b) The National Cyber Security Centre's (**NCSC**) guidance on protecting bulk personal data[41] provides:

i. **User access and privilege** | *"User access to data is limited to the minimum necessary".*

ii. **Administrator access** | *"The list of system administrators with access has been reviewed within the last 12 months".*

iii. **All external dependencies** | *"You understand which of your suppliers would have the ability to compromise your data"*.

c) The NIST SP 800-53 security framework outlines that organisations should *"employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks".*[42] This is a well-established rule within IT security which significantly reduces the chance a threat actor can perform lateral movement across a network. Sqluser was only

[40] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/ransomware-and-data-protection-compliance/.

[41] Who has access to your data? - NCSC.GOV.UK.

[42] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

required on a single server and system, yet it had privileges which afforded it access to the full suite of network devices within the DPP infrastructure.

Assessment of compliance

50. Under the UK GDPR, it is for DPP to demonstrate compliance with Article 5(1)(f) (by virtue of Article 5(2)). It is also for DPP to demonstrate compliance with Article 32(1) and (2) (by virtue of Article 24).

51. The Commissioner finds that whilst DPP attempted to secure the external perimeter of the network there were critical failings in the provisioning and management of the sqluser account. These included:

    a) Sqluser was an over privileged account, the compromise of which enabled the threat actor full access to DPP's network.[43]

    b) It was not necessary for DPP to access the sqluser account on a day-to-day basis, particularly following:

        i. the migration of its case management system from sqluser in April 2019; and

        ii. the closure of the maintenance support window for sqluser in 2021.

    c) Whilst DPP was aware of sqluser, it did not undertake a risk assessment. DPP explained to the Commissioner that this was because it viewed sqluser as a supplier account which it did not consider it had any need to risk assess.[44]

52. DPP failed to have in place measures to audit all accounts on DPP's servers and to limit the privileges associated with these accounts or

[43] DPP response dated 6 October 2022.
[44] DPP response to ICO dated 8 February 2024, 7.

disable them where they were not necessary. DPP's failure to implement these measures constituted a failure to implement appropriate technical and organisational measures to ensure an appropriate level of security over the personal data it was processing.

53. The Commissioner also finds that DPP failed to ensure the ongoing confidentiality of its systems, as required by Article 32(1)(b) UK GDPR.

54. DPP failed to perform any kind of asset management or suitable alternative measure, which should have been audited and risk assessed periodically in accordance with the Commissioner's Accountability Framework.[45]

55. Upon carrying out an asset management audit, DPP would have discovered that sqluser had a narrow scope of duties and was only required on a single server and system but that it had privileges that afforded it access to the full suite of network devices within the DPP network.

56. DPP should have carried out a risk assessment based on the excessive privileges granted to sqluser. Following this risk assessment, DPP should have given the sqluser account the minimal set of privileges that it required to perform its function.

57. In its written representations, DPP highlighted the unsophisticated nature of its internal IT function. DPP noted that tasks routinely undertaken by its internal IT team only required qualifications such as *"IT studies at college"* or a *"government apprenticeship scheme with the aim of becoming Microsoft certified"*.[46] As such, DPP did not have its own

[45] Available at: https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework-0-0.pdf (see Records management and security at pp.55-63) [last accessed 19 November 2024].
[46] DPP Written Representations, 29 January 2025, p.1.

technical resources and was *"totally reliant"* on third party IT contractors.[47]

58. DPP itself should have had full visibility of the sqluser account (including the password). Furthermore, at the end of the service agreement for the sqluser account, it would have been reasonable for DPP to have convened a meeting with its service provider to understand the implications of operating the out-of-support account on its network. Support for the legacy case management system ceased on 30 April 2019.

59. It appears to the Commissioner that there were alternative ways in which DPP could have mitigated the risks associated with its continued operation of the sqluser account:

    a) DPP could have suspended sqluser or limited how and when sqluser was used. Particularly given support for the legacy case management system ceased on 30 April 2019.[48]

    b) DPP could have assigned sqluser fewer privileges and kept those privileges under tight control according to the principle of least privilege.

    c) DPP should have had full visibility of the sqluser account at the end of the service agreement enabling it to assess the risks presented by the continued operation of the account (as noted at paragraph 58 above) and consider appropriate mitigating measures.

    d) As demonstrated in the steps taken by DPP after the Cyber Incident (see paragraphs 29 to 30 above), there were alternative means of operating the sqluser account which were available to

[47] DPP Written Representations, 29 January 2025, p.1.
[48] DPP response to ICO 7 September 2022, Q3a.

DPP. The Commissioner has not been provided with any evidence to suggest DPP considered these (or other) alternative means of operating sqluser between the end of the service agreement and the Cyber Incident.

60. The assessment of risks presented by the continued use of the sqluser account following the end of the service agreement, and the implementation of alternative means of continuing to operate the account, would have, in high likelihood, prevented the Cyber Incident from occurring.

61. In its written representations, DPP told the Commissioner that it had worked alongside its suppliers to ensure it was fully compliant with Lexcel standards (to which it was accredited).[49] Lexcel is a practice management and client care standard introduced by the Law Society of England and Wales. The Commissioner notes that the Lexcel self-assessment checklist[50] for accreditation states *"Practices… should be accredited against Cyber Essentials"*.[51] DPP's written representations confirmed that, at the time of the cyber incident, DPP did not have Cyber Essentials accreditation, although it was working towards accreditation. The Commissioner understands that this has now been obtained.[52]

62. The Commissioner finds that DPP failed to implement appropriate technical and security measures to ensure the security of personal data it was processing on the sqluser account. DPP's isolation of the legacy case management system following the Cyber Incident demonstrated that alternative methods to secure its IT environment were available.

Conclusion

[49] DPP written representations, p.2.
[50] Available at: How to apply for Lexcel England and Wales (v6.1) | The Law Society.
[51] See 3.2 of the Lexcel self-assessment checklist.
[52] DPP written representations, p.4.

63. The Commissioner finds that the DPP's failure to audit and adequately manage the accounts on its servers (including password administration and access privileges) constituted a failure to implement appropriate technical and organisational measures to ensure appropriate security. For this reason, the Commissioner finds that DPP has infringed Articles 5(1)(f), 32(1) and 32(2) UK GDPR.

D. The infringements: Article 33(1) UK GDPR

64. Controllers must notify the Commissioner within 72 hours of becoming aware of a personal data breach unless it is unlikely to result in a risk to the rights and freedoms of natural persons. The Commissioner considers that the Cyber Incident constituted a personal data breach about which DPP should have notified the Commissioner.

65. A personal data breach includes the *"loss of availability of personal data"*.[53]

66. As set out in paragraphs 16 and 20, when the Cyber Incident occurred DPP's email server stopped working and staff no longer had access to the personal data on its IT network. Given that DPP processes personal data relating to ongoing court cases including confidential information, which is subject to legal professional privilege, the loss of availability of that personal data, even for a few days, was likely to result in a risk to the rights and freedoms of its clients.[54]

67. DPP did not notify the Commissioner within 72 hours of becoming aware that the Cyber Incident had caused a notifiable personal data breach. It took DPP 43 days to notify the Commissioner about the breach, and it only made a notification after being contacted by the NCA regarding the exfiltration of personal data from its network (see paragraph 23 and 24).

[53] https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/.

[54] Recital 85 UK GDPR explains that *"a personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as… the loss of confidentiality of personal data protected by professional secrecy"*.

68. DPP told the Commissioner that its efforts had been initially focused on bringing its systems back online, and it did not believe that, in the absence of any evidence of third party access to personal data, it had an obligation to notify the Commissioner.[55]

69. It was the responsibility of DPP to assess the Cyber Incident and determine whether it met the threshold for notification to the Commissioner as required by Article 33(1) UK GDPR. In the circumstances, DPP was required to notify the Commissioner within 72 hours of becoming aware of the personal data breach. If DPP did not have all the required information for the notification, it should have made an initial notification and provided a further update once more information became available (as stated in Article 33(4) UK GDPR and the Commissioner's guidance).[56] In its written representations, DPP accepted that, in hindsight, it *"should have made the notification at the time of the incident"*.[57]

70. The Commissioner finds that:

    a) DPP focused its efforts on bringing its systems back online after the Cyber Incident.

    b) In so doing, DPP neglected to undertake an assessment of the risks likely to be caused to data subjects resulting from their personal data becoming unavailable.

    c) Consequently, DPP only notified the Commissioner of the personal data breach 43 days after the Cyber Incident that had caused a personal data breach.

[55] Telephone attendance ICO & DPP 21 July 2022; DPP Response to ICO 7 September 2022, Q1a.
[56] https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/.
[57] DPP Written Representations, 29 January 2025, p.5.

d) The delay in DPP's notification to the Commissioner was compounded by DPP's lack of understanding of the circumstances in which it was required to make a notification to the Commissioner under Article 33 UK GDPR.

71. The Commissioner therefore finds DPP to have infringed Article 33(1) UK GDPR.

V. DECISION TO IMPOSE A PENALTY

72. For the reasons set out below, the Commissioner has decided to impose a penalty on DPP in respect of the infringements of Article 5(1)(f), 32(1), 32(2) and 33(1) UK GDPR.

A. Legal Framework – penalties

73. When deciding whether to issue a penalty notice to a person and determining the appropriate amount of that penalty, section 155(2)(a) DPA requires the Commissioner to have regard to the matters listed in Article 83(1) and (2) UK GDPR, so far as they are relevant in the circumstances of the case.

74. Article 83(1) UK GDPR requires any monetary penalty imposed by the Commissioner to be effective, proportionate, and dissuasive in each individual case.

75. Article 83(2) UK GDPR requires the Commissioner to have due regard to the following factors when determining whether to issue a penalty notice and the appropriate amount of any such penalty in each individual case:

> *"(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 Commissioner, 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 Commissioner, 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".

B. The Commissioner's decision on whether to impose a penalty

76. Paragraphs 78 to 134 below set out the Commissioner's assessment of whether it is appropriate to issue a penalty in relation to the infringements set out above. That assessment involves consideration of the factors in Articles 83(1) and 83(2) UK GDPR. The order in which these considerations are set out below follows the Commissioner's Data Protection Fining Guidance, (the "**Fining Guidance**"):[58]

    a) Seriousness of the infringements (Article 83(2)(a), (b) and (g))

    b) Relevant aggravating or mitigating factors (Article 83(2)(c)-(f), (h)-(k))

    c) Effectiveness, proportionality and dissuasiveness (Article 83(1))

77. The Commissioner has not conducted a separate assessment for each infringement. As explained further below (paragraphs 136 to 138), the Commissioner considers the four infringements relate to the Relevant Processing. An assessment of whether it is appropriate to issue a penalty has been taken in relation to the four infringements collectively.[59]

<u>Seriousness of the infringements: Article 83(2)(a) the nature, gravity and duration of the infringements</u>

78. In assessing the seriousness of the infringements, the Commissioner has given due regard to their nature, gravity and duration.

Nature of the infringements

[58] https://ico.org.uk/about-the-ico/our-information/policies-and-procedures/data-protection-fining-guidance/ (dated March 2024).

[59] For the avoidance of doubt, the Commissioner considers Articles 5(1)(f), 32(1), 32(2) and 33 UK GDPR to be evidently distinct provisions of the UK GDPR. Had he calculated penalties for infringements of these provisions separately, the Commissioner would have had to ensure, in accordance with Article 83(3) UK GDPR, that the total penalty did not exceed the amount specified for the gravest infringement (that of Article 5(1)(f) UK GDPR). However, in this Penalty Notice, the Commissioner has simply calculated a single penalty ensuring that the amount does not exceed the maximum amount specified for the infringement of Article 5(1)(f) UK GDPR.

79. Article 5(1)(f) UK GDPR (integrity and confidentiality) is a basic principle for processing. An infringement of this provision is subject to the higher maximum fine,[60] reflecting its seriousness. Meanwhile, infringements of Articles 32(1), 32(2) and 33(1) UK GDPR are subject to the standard maximum amount.[61]

Gravity of the infringements

80. In assessing the gravity of the infringements, the Commissioner has considered the nature, scope and purpose of the Relevant Processing, as well as the number of data subjects affected by the Relevant Processing and the level of damage they have suffered.[62]

81. **Nature** | The nature of the Relevant Processing concerned DPP's delivery of legal services and advice to clients (including the instruction of experts, where required). In the absence of appropriate security measures, the nature of the processing was likely to result in a high risk to the data subjects if unauthorised access and processing took place (as discussed in paragraphs 41 to 49). Some of the data subjects were vulnerable, including children and victims of sexual offences. The personal data impacted included sensitive personal data. It also included information relating to ongoing court cases, including DNA data, legally privileged information and police body-cam footage. In line with the Fining Guidance, the Commissioner gives more weight to this factor where the processing involves children's personal data and personal data of other vulnerable people, which is the case here. Recital 38 UK GDPR explains that children merit specific protection with regard to their personal data.

[60] £17,500,000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (Article 83(5) UK GDPR).
[61] £8,700,000 or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher (Article 83(4) UK GDPR).
[62] Article 83(2)(a) UK GDPR.

82. **Scope** | The Commissioner notes that the territorial scope of the Relevant Processing extended to clients and experts from across England and Wales.

83. **Purpose** | The purpose of the Relevant Processing was to provide legal advice in both criminal and civil proceedings, which has the possibility of significantly affecting people's rights and freedoms. The Commissioner considers this to increase the gravity of the infringements.

84. **Number of data subjects and level of damage suffered** | The number of data subjects affected by the infringements carries significant weight. The Cyber Incident affected 791 data subjects in total. This included: 306 crime clients, 225 family clients, 14 matrimonial clients, 137 actions against the police clients and 109 expert witnesses.[63] 791 is not an insignificant number considering the sensitivity of the personal data involved. This included highly sensitive information relating to court proceedings and DPP's legal advice to its clients. The Commissioner has also had regard to complaints received (discussed in paragraphs 86 to 86.b) below).

85. In relation to the level of damage suffered by affected data subjects, the Fining Guidance states:

> *"The Commissioner's assessment of the level of damage suffered by data subjects will be limited to what is necessary to evaluate the seriousness of the infringement. Typically, it would not involve quantifying the harm, either in aggregate or suffered by specific people. It is also without prejudice to any decisions a UK court may make about awarding compensation for damage suffered".*

86. In assessing the level of damage suffered as a result of the infringements, regard has been given to both potential and actual

[63] DPP Response to ICO, 7 September 2022, Q8, Q9; DPP Response to ICO, 6 October 2022, Q6.

damage suffered by data subjects as a result of the Cyber Incident. Complaints lodged by data subjects under Article 77 UK GDPR can assist with the assessment of the level of damage. Two complaints were made to the Commissioner:

a) The first complaint related to an individual who was accused of sexually assaulting a child. The police wrote to this individual explaining that following the Cyber Incident details of the allegation were published online. As outlined in paragraph 42, this individual had a reasonable expectation of privacy in relation to the police investigation. In the complaint to the ICO, the complainant described his reaction: *"I'm now a prisoner in my own home again. In fear of my life. My family's also".* The individual further explains: *"I'm seriously worried again and I don't think I can cope. It's dredged everything back up. I haven't been allowed to see my children… because of these allegations and it's very nearly ended me. I can't do this again, I'm just trying to live my life while fighting a losing battle with social services. It's a nightmare".*

b) The second complaint related to an individual who was informed by the police that their personal data was now online following the Cyber Incident. The information disclosed related to a closed criminal investigation in which the complainant was a suspect. Again, this individual had a reasonable expectation of privacy in relation to the police investigation. The complainant requested compensation to increase security at his home. This individual also complained to DPP directly.

87. DPP received five potential claims for professional negligence related to the Cyber Incident. However, two of these came from individuals whose data had not in fact been exfiltrated in the Cyber Incident. The remaining three individuals cited in their claims that they suffered distress (as well

as shock, anxiety, worry and lack of sleep), loss of control (and autonomy) of their personal data and the possibility of fraud. One of these individuals is a vulnerable individual as per his GP records.

88. The Commissioner considers that, in particular, three types of (non-material) damage (actual or foreseeable) arose from the infringements. These are:

a) **Loss of control of personal data** | The loss of control of personal data is evident from DPP's loss of access to its network and the exfiltration of personal data from its network.

b) **Loss of human dignity** | Loss of human dignity is evident from the nature of the personal data affected. For example, the data relating to victims of crime, special category data relating to an individual's sex life and bodycam footage of individuals during their interactions with police.

c) **Psychological harms** (distress, shock, anxiety, worry and lack of sleep, anxiety and embarrassment from sensitive details regarding allegations made public; reputational loss; loss of confidence in the legal profession) | The psychological harm is adequately demonstrated by the personal account of the complainant (cited at paragraph 86.a) above).

89. The release of personal data of the type in this case on the dark web is likely to increase distress to the affected individuals, not least given:

a) the vulnerability of some individuals to whom the data related;
b) the dark web's common association with nefarious activity;[64]

[64] It is common for threat actors to exploit victims of cyberattacks by threatening publication of exfiltrated data on the dark web. The dark web enables threat actors to sell stolen data to other individuals / organisations with an interest in exploiting it.

c) that individuals expect that information they disclose to their legal representatives is kept confidential and secure;
d) that experts involved in judicial proceedings also have an expectation that law firms will treat their personal data confidentially and securely.

90. DPP stated in notification letters to affected data subjects that the personal data *"is not in the public domain, but in a place on the dark web that is not indexed by search engines".* However, this is not necessarily accurate given that the data exists in an online space and the dark web is accessible to anyone with the correct browser. DPP also further stated that only six pieces of information were readily accessible, while the rest was in an encrypted format that is *"very difficult to access".* Whilst the Commissioner acknowledges that a level of encryption may mean the data is not immediately accessible, it does not necessarily mean it is difficult to access as the level of encryption that the threat actor applied to the other information may be simple; alternatively, the threat actor could publish the decryption key making the information immediately accessible.

91. Given the sensitivity of the personal data involved there is a greater potential for rights and freedoms of data subjects to be adversely affected, the Commissioner has therefore given significant weight to this factor in his assessment of the gravity of the infringement.

92. With regards to the infringement of Article 33(1) UK GDPR, Recital 85 UK GDPR makes it clear that one of the purposes of notification to the Commissioner is to limit the damage to individuals as a result of a personal data breach. If DPP had notified the Commissioner when the personal data breach occurred (i.e. at the time of the Cyber Incident), the Commissioner may have initiated an investigation earlier that would have prompted DPP to take steps to mitigate the breach. DPP may have acted sooner rather than waiting to hear from the NCA about the

personal data being uploaded onto the dark web. The delay of 43 days before reporting the matter to the Commissioner also caused a delay in the Commissioner's investigation.

93. To summarise the Commissioner's assessment of the gravity of the infringements: the scope of the Relevant Processing was across England and Wales, the nature and purpose of the Relevant Processing, the number of data subjects affected, and the level of damage suffered by them all increase the gravity of the infringements. The gravity of the infringements increases their seriousness.

Duration of the infringements

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

94. The duration of the infringements was from at least 25 May 2018 (the date of commencement of the DPA and application of the UK GDPR)[65] until the 4 June 2022 (the date of the Cyber Incident, which caused DPP to suspend sqluser from its network and move its case management, accounts and email system to the new managed hosted environment operated by a case management software supplier).

95. The risk of damage (i.e. potential damage) to data subjects existed from at least as early as 25 May 2018 and could have materialised at any point during this lengthy period. The risk materialised on 4 June 2022.

96. The infringements subsisted for (at the very least) four years before the risk materialised. The duration of the infringements increases their seriousness.

Article 33(1)

[65] DPP was aware of the sqluser account as far back as 2011 but despite being aware, failed to ensure the ongoing confidentiality of its systems, as required at the commencement of the DPA 2018 and application of the UK GDPR.

97. Article 33(1) UK GDPR requires personal data breaches within the meaning of Article 4(12) UK GDPR to be notified to the Commissioner without undue delay and where feasible not later than 72 hours after having become aware of it. DPP had 72 hours from becoming aware of the Cyber Incident on 4 June 2022 to notify the Commissioner.

98. The duration of this infringement was from 7 June 2022 until 17 July 2022 (i.e. the date on which DPP notified the Commissioner about the personal data breach). It is important to emphasise that this delay meant that the infringements were not satisfactorily dealt with and caused a consequential delay to the Commissioner's investigation.

Conclusion on the nature, gravity and duration of the infringements

99. The nature, gravity and duration of the infringements all increase the seriousness of the infringements.

Seriousness of the infringements: Article 83(2)(b) the intentional or negligent character of the infringements

100. The Commissioner does not consider that DPP acted intentionally in committing the infringements. The Commissioner does, however, find that the infringements were negligent in character.

101. While the personal data breach occurred due to a malicious and criminal cyberattack, it was successful due to DPP's negligent security practices. DPP acted negligently in failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. In particular, DPP failed to have in place measures to audit all accounts on DPP's servers and to limit the privileges associated with these accounts or disable them where they were not necessary. It failed to recognise the risk associated with an administrator account that had unrestricted access across the network. These were all routine measures that could have been taken by DPP to secure its network and the

personal data it was processing (see guidance referred to at paragraph 49 above).

102. It would have been straightforward for DPP to implement measures that ensured appropriate security of the personal data (such as: suspending the account when not needed; being (at least) aware of the password; and performing risk assessments on the account). Any risk assessment may have identified further ways in which the account could have been secured more appropriately. Each of these measures could have been implemented prior to the incident at minimal cost.

103. In addition, DPP ought to have known that the unavailability of systems constituted a personal data breach, about which DPP should have notified the Commissioner. The Commissioner's guidance on personal data breaches states: *"Personal data breaches can include… loss of availability of personal data".*[66] The guidance also states that organisations should notify the Commissioner within 72 hours of becoming aware of a breach, even if they don't have all the required information. For instance, the guidance provides an example of a comparable situation, which demonstrates that DPP ought to have notified the Commissioner earlier when investigating the incident:

> **Example**
>
> You detect an intrusion into your network and become aware that files containing personal data have been accessed, but you don't know how the attacker gained entry, to what extent that data was accessed, or whether the attacker also copied the data from your system.
>
> You notify the ICO within 72 hours of becoming aware of the breach, explaining that you don't yet have all the relevant details, but that you expect to have the results of your investigation within a few days. Once your investigation uncovers details about the incident, you give the ICO more information about the breach without delay.

[66] https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/.

104. The clearly negligent character of the infringements increases their seriousness.

Seriousness of the infringements: Article 83(2)(g) categories of personal data affected

105. The personal data exfiltrated in the Cyber Incident included:[67]

a) Relating to 306 crime clients:

i. Name
ii. Address
iii. Date of birth
iv. Details of offence
v. Police station instructions, which includes a significant amount of sensitive information. For example, special category data including ethnicity and disability (where applicable). It also includes details of the police station, arrest and detention, previous advice and assistance that DPP offered, samples taken, whether searches and seizures were made, relevant medical conditions, DPP's instructions and advice to the client, police interview details, outcome of the interview/arrest, charges and bail conditions, and custody details.[68]
vi. DPP advice
vii. May include email and phone number

b) Relating to 225 family clients:

i. Name
ii. Court case

[67] DPP Response to ICO, 7 September 2022, Q9; DPP Response to ICO, 6 October 2022, Q7; DPP Response to ICO, 7 August 2024, Q1.
[68] DPP Response to ICO, 7 September 2022, Appendix 7.

iii. Details of closed family cases
iv. May include date of birth

c) Relating to 14 matrimonial clients:[69]

i. Name
ii. Date of birth
iii. Address
iv. Email
v. Financial details

d) Relating to 137 actions against the police clients:[70]

i. Name
ii. Address
iii. Date of birth
iv. Phone
v. Email
vi. National insurance number
vii. Medical records (e.g. medical report, NHS number)
viii. Next of kin
ix. Driver's license
x. DPP instructions

e) Relating to 109 experts:

i. Name
ii. Address
iii. Phone
iv. Email
v. Bank account information

[69] DPP Response to ICO, 7 September 2022, Appendix 8.
[70] DPP Response to ICO, 7 September 2022, Appendix 9.

106. The Fining Guidance sets out at paragraph 70: *"The UK GDPR… make[s] clear that the processing of certain categories of personal data deserves special protection. These categories include… special category data (Article 9 UK GDPR); personal data relating to criminal convictions and offences (Article 10 UK GDPR)".* Infringements that involve the processing of such data are regarded by the Commissioner as being particularly serious.[71]

107. The Fining Guidance further states at paragraph 72:

> *"In assessing seriousness, the Commissioner may also take into account other types of personal data affected by the infringement where that data may be regarded as particularly sensitive. This includes where the dissemination of the personal data is likely to cause damage or distress to data subjects, for example:… private communications (particular those involving intimate details or confidential information about the data subject)".*

108. The personal data exfiltrated in the Cyber Incident included a significant proportion of personal data that deserves special protection and is sensitive, including special category data, personal data relating to criminal convictions and offences, and privileged communications.

109. As discussed in paragraphs 35 to 37, this information revealed intimate details about individuals, including the offences of which they were accused and DPP's confidential legal advice, as well as information relating to children. This points to the seriousness of the infringements and is given significant weight in the Commissioner's findings.

Conclusion on seriousness of infringements

[71] Paragraph 71 of the Fining Guidance.

110. The nature, gravity and duration as well as the clearly negligent character of the infringements coupled with the impact on sensitive information militates towards a high degree of seriousness. However, when the relatively limited number of data subjects is taken into account the Commissioner categorises the infringements as having a medium degree of seriousness.

111. In the absence of any aggravating or mitigating factors, the infringements would warrant a monetary penalty. The Commissioner's consideration of any aggravating or mitigating factors follows below.

Relevant aggravating or mitigating factors: Article 83(2)(c) any action taken by the controller or processor to mitigate the damage suffered by the data subjects

112. In line with Article 34 GDPR requirements, DPP notified affected individuals of the personal data breach by letters, email and phone. DPP notified the majority of data subjects by the end of August 2022. Where the data subjects were children, DPP notified the children's guardian via CAFCAS (the Children and Family Court Advisory and Support Service), rather than directly with the parents, as the children were subject to care proceedings and did not live with their parents. Where DPP identified data subjects as having mental health difficulties, DPP considered the most appropriate means of contact was via a phone conversation.

113. DPP stated that when notifying those affected, DPP enclosed information from the NCA with advice on how to protect personal data and stay safe in the digital environment. This cannot be considered a mitigating factor given that this information would not mitigate the possible damage suffered by data subjects as a result of the Cyber Incident.

114. Following the Cyber Incident, steps were taken to improve DPP's security system, including moving its complete case management, accounts and

email system to a managed hosted environment operated by its case management software suppliers, The Access Group. DPP also removed the legacy case management system from the DPP Network and it is now only accessible through [redacted].

115. The Commissioner considers that these actions (notifying affected data subjects and improving the DPP security system) do not amount to a mitigating factor in his decision on whether to impose a penalty. These actions were all legal requirements and include what would reasonably be expected of an organisation in response to a personal data breach.

Relevant aggravating or mitigating factors: Article 83(2)(d) the degree of responsibility of the controller or processor

116. DPP was the sole controller in respect of the Relevant Processing. DPP therefore bears full responsibility for the infringements. While the compromised administrator account was originally setup for third party access to the network, DPP as controller is ultimately responsible for the security measures that it has in place.

117. The Commissioner considers DPP's degree of responsibility to be an aggravating factor in his decision to impose a penalty.

Relevant aggravating or mitigating factors: Article 83(2)(e) any relevant previous infringements by the controller or processor

118. The Commissioner is not aware of any relevant previous infringements. This factor is therefore not relevant to his decision.

Relevant aggravating or mitigating factors: Article 83(2)(f) the degree of cooperation with the Commissioner

119. Controllers and processors are expected to cooperate with the Commissioner in the performance of the Commissioner's tasks, for

example by responding to requests for information and attending meetings. The Commissioner considers that the ordinary duty of cooperation is required by law and meeting this standard is therefore not a mitigating factor.

120. DPP provided full cooperation with the Commissioner throughout the investigation. DPP did not however go above and beyond the normal level of expected cooperation. The Commissioner considers this to be a neutral, rather than mitigating, factor.

Relevant aggravating or mitigating factors: Article 83(2)(h) the manner in which the infringements became known to the Commissioner

121. DPP reported the Cyber Incident to the Commissioner but not until 43 days after its systems went offline. However, this is not considered as an aggravating factor given it has already been taken into account in the consideration of the seriousness of the infringement of Article 33(1) UK GDPR.

Relevant aggravating or mitigating factors: Article 83(2)(i) measures previously ordered against the controller or processor

122. There are no measures referred to in Article 58(2) UK GDPR which have previously been ordered against DPP concerning the same subject matter. This factor is therefore not relevant to the Commissioner's decision.

Relevant aggravating or mitigating factors: Article 83(2)(j) adherence to approved codes of conduct or certification mechanisms

123. There were no approved codes of conduct pursuant to Article 40 UK GDPR or approved certification mechanisms pursuant to Article 42 UK GDPR. This factor is therefore not relevant to the Commissioner's decision.

Relevant aggravating or mitigating factors: Article 83(2)(k) any other applicable aggravating or mitigating factors

124. The Commissioner has considered whether DPP has adhered to approved codes of conduct set out by its regulatory body.

125. The SRA has a published 'Code of Conduct for Firms'. Of particular relevance are the requirements to:

- **Paragraph 2.1(a)** | *"Have effective governance structures, arrangements, systems and controls in place that ensure [compliance] with all the SRA's regulatory arrangements, as well as with other regulatory and legislative requirements, which apply to you"*;
- **Paragraph 2.5** | *"…identify, monitor and manage all material risks to your business…"*;
- **Paragraph 3.1** | *"…keep up to date with and follow the law and regulation governing the way you work"*; and
- **Paragraph 5.2** | *"…safeguard money and assets entrusted to you by clients and others"* – the reference to *"assets"* is defined to include documents.

126. The Commissioner finds the determination of compliance or otherwise with the SRA Code of Conduct is a matter for the SRA and therefore does not consider this as an aggravating factor in his assessment. As far as the Commissioner is aware, no action has been taken by the SRA against DPP in respect of the Cyber Incident. However, the Commissioner finds that as an SRA regulated firm and, by virtue of the elements of the SRA Code of Conduct listed at paragraph 125 above, DPP should have had

greater awareness of the importance of compliance with the security principles under UK GDPR.

127. DPP explained in its written representations that it had worked with the NCSC regarding the attack.[72] However, this was not considered to be a mitigating factor as DPP did not take steps to pro-actively report the attack to the NCSC at the time of the incident and did not go beyond what was required in the circumstances.

128. There are no other aggravating or mitigating factors applicable to the circumstances of the case.

Conclusion on relevant aggravating and mitigating factors

129. The Commissioner has taken into account the degree of DPP's responsibility as an aggravating factor.

130. Consideration of the seriousness of the infringements (the first stage of the assessment) indicated that a penalty is appropriate. The aggravating factor strengthens that assessment.

131. The final stage involves a consideration of the effectiveness, proportionality and dissuasiveness of a penalty.

Effectiveness, proportionality and dissuasiveness

132. The Commissioner considers the imposition of a penalty would be effective and dissuasive. It would both promote compliance with data protection legislation and provide an appropriate sanction for the infringements. It would deter DPP from infringing the UK GDPR's security provisions, including the requirement to notify the Commissioner within 72 hours of becoming aware of a personal data breach. There is also a

[72] DPP Written Representations, 29 January 2025, p.4.

need to deter other organisations, such as law firms, that hold sensitive personal data from acting in the same way.

133. Taking into account the seriousness of the infringements and DPP's size and financial position (discussed in paragraph 146 below), the Commissioner considers that the imposition of a penalty would be proportionate (i.e. it would not exceed what is appropriate and necessary in the circumstances to ensure compliance with data protection legislation and to provide an appropriate sanction for the infringements). DPP will continue to process personal data as it offers legal services to vulnerable individuals and it will continue to need to implement appropriate technical and organisational measures to protect sensitive information, including legally privileged advice.

C. Conclusion on decision on whether to impose a penalty

134. In light of the assessment above, the Commissioner has decided to impose a penalty.

VI. CALCULATION OF PROPOSED PENALTY

135. The Fining Guidance sets out a five-step approach which the Commissioner proposes to apply to calculate the amount of a penalty:

Step 1: Assessment of the seriousness of the infringement.
Step 2: Accounting for turnover (where the controller or processor is part of an undertaking).
Step 3: Calculation of the starting point having regard to the seriousness of the infringement and, where relevant, the turnover of the undertaking.
Step 4: Adjustment to take into account any aggravating or mitigating factors.
Step 5: Assessment of whether the fine is effective, proportionate and dissuasive.

Statutory maximum penalty

136. Article 83(3) UK GDPR states that "*if a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of the UK GDPR, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement*". The four infringements set out in this Penalty Notice[73] all relate to the same or linked processing operations (the Relevant Processing). The gravest infringement was that of Article 5(1)(f) UK GDPR.

137. The infringement of Article 5(1)(f) UK GDPR, which is one of the principles of processing, is subject to the higher maximum statutory penalty of £17.5 million (Article 83(5)(a) UK GDPR) or 4% of an undertaking's worldwide turnover in the preceding financial year (whichever is higher). As an undertaking, DPP's turnover in the preceding financial year was £3,486,494 (see paragraph 146). Therefore, had the Commissioner imposed a separate penalty for each of the four infringements, the total of those four penalties could not have exceeded £17.5 million (given that this is higher than 4% of DPP's turnover in the preceding financial year).

138. In this case, however, the Commissioner has calculated a single penalty for all four infringements. This is because the four provisions infringed all relate to the same or linked processing operations: they all related to the failure to ensure the security of personal data processing including the response to personal data breaches. The calculation proceeds on the basis of a single statutory maximum of £17.5 million.

A. Step 1: Assessment of the seriousness of the infringement

[73] Infringements of Articles 5(1)(f), 32(1), 32(2) and 33(1) UK GDPR.

139. As set out at paragraphs 109 to 115 of the Fining Guidance, the Commissioner determines a starting point for the penalty first by assessing the seriousness of the infringement. The Commissioner categorises the infringement according to its degree of seriousness and then chooses a starting point based on a percentage of the relevant applicable statutory maximum.

140. In this Penalty Notice (paragraph 110 above), the Commissioner has categorised the infringements as having a medium degree of seriousness. This means that the starting point will be between 10% and 20% of the relevant legal maximum (£17.5 million).

141. The Commissioner has decided that the infringements warrant a starting point of 17%.

142. A starting point lower than 17% is not warranted due to the seriousness of the infringements, for the reasons set out at paragraphs 78 to 111 above. The Commissioner does not repeat those reasons here.

143. A starting point higher than 17% is not warranted for the following reasons:

    a) the fact that the infringements were not intentional; and
    b) there were no direct financial gains from the infringements.

B. Step 2: Accounting for turnover

144. Having assessed the seriousness of the infringements, the Commissioner next determines any adjustment to reflect the size of the recipient of the penalty.[74] This is consistent with the need to ensure the amount of the penalty is effective, proportionate and dissuasive.

[74] As set out at paragraph 128 of the Fining Guidance, any such adjustment is discretionary.

145. Where the recipient is an undertaking, the Commissioner will determine the adjustment by reference to the undertaking's turnover.

146. DPP provided a copy of its most recent financial statement. For the financial year in the 2023/2024 period, DPP had a turnover of £3,486,494.

147. As set out in the Fining Guidance, in the case of an undertaking with an annual turnover of between £2 million and £10 million, the Commissioner may apply an adjustment factor of 0.4% to 2% to the starting point (see below). The Commissioner considers this range of adjustment is also appropriate in DPP's case.

148. The Commissioner has decided that an adjustment of 0.8% is appropriate to reflect DPP's size.

C. Step 3: Calculation of the starting point

149. The starting point of the penalty is calculated as follows:

Fixed statutory maximum amount (£17.5 million) x adjustment for seriousness (17%) x turnover adjustment (0.8%) = £23,800

150. The starting point of £23,800 represents a figure which is 0.68% of DPP's turnover for the financial year 2023/2024,

D. Step 4: Adjustment to take into account any aggravating or mitigating factors.

151. The Commissioner next takes into account any aggravating or mitigating factors. These factors may warrant an increase or decrease in the level of the penalty calculated at the end of Step 3 (the starting point of £23,800).

152. On this occasion, the Commissioner has decided that no mitigating factors are present allowing for the adjustment of the fine.

153. The Commissioner has carefully considered the potential arguments in respect of compliance or otherwise with the SRA Code of Practice arising from the Cyber Incident. However, as the SRA has made no findings against DPP as a result of the Cyber Incident, the Commissioner decides not to take this factor into account as an aggravating factor.

154. Whilst DPP's degree of responsibility was considered as an aggravating factor in the decision to impose a penalty, the Commissioner has decided that, as this factor is taken into account in the assessment of the seriousness of the infringements at Step 1, it is not an aggravating factor which would merit the adjustment of the fine.

155. There are no other aggravating or mitigating factors and so there is no adjustment at Step 4.

E. Step 5: Adjustment to ensure the fine is effective, proportionate and dissuasive

156. The Fining Guidance provides that:

> *"the aim of Steps 1 to 4 of the calculation is to identify a fine amount that is effective, proportionate and dissuasive. The purpose of Step 5 is to provide the opportunity for the Commissioner to check that is the case".*

157. In evaluating the level of the fine, and in the exercise of his discretion, the Commissioner considers that a penalty of £23,800 (representing only 0.68% of DPP's turnover for the financial year 2023/2024) will neither be effective nor dissuasive for the following reasons:

a) A fine at this level is insufficient to serve as an effective deterrent. The Commissioner has reached this view having taken into consideration the categories of personal data affected (and which will continue to be processed by DPP) and the level of fines imposed in other cases involving security breaches.[75] In the Commissioner's judgement the penalty requires an increase to be effective and demonstrate the importance of compliance with Articles 5(1)(f), 32 and 33 UK GDPR.

b) It would not be dissuasive because a fine of £23,800 is not sufficient to discourage similar infringements. DPP could have implemented a solution to protect the personal data that it processes at minimal cost. A penalty representing a fraction of a percent of DPP's turnover would not be severe enough to secure specific and general deterrence. That is:

   i. Deterring DPP from infringing the security of processing provisions of the UK GDPR and encouraging compliance with the same (specific deterrence).

   ii. Deterring other organisations generally from infringing security of processing provisions of the UK GDPR and encouraging compliance with the same (general deterrence).

158. Where a penalty is a very small percentage of an organisation's total turnover, the impact of the penalty on that organisation may be very limited. It is only when the penalty imposed is sufficiently high to make a meaningful impact on the controller that the Commissioner can be confident that the infringing controller will take its compliance with data protection law seriously in the future.

[75] See Tuckers Solicitors LLP monetary penalty notice, Interserve Group Limited monetary penalty notice, Marriott International Inc, monetary penalty notice, British Airways monetary penalty notice.

159. The Commissioner finds that a fine at the level of £23,800 is not proportionate insofar as it would not deliver the objective of enforcing compliance with the UK GDPR and providing an appropriate sanction for the findings of infringement. Having taken into account the seriousness of the infringements, the impact on data subjects and DPP's size and financial position, the Commissioner is of the view that a fine of £23,800 is less than is necessary in the circumstances to meet those objectives.

160. The Commissioner therefore considers that a penalty of £60,000 would be more appropriate. A penalty of this amount represents 1.7% of DPP's turnover for the financial year 2023/2034 and is likely to have a genuine deterrent effect. This is so taking into account both the specific deterrence to DPP and the general deterrence to other organisations (e.g. other law firms). This would send a message to other organisations that they must implement appropriate security measures to protect personal data. This penalty would not be more than is appropriate or necessary in the circumstances. Therefore, a penalty of £60,000 would be proportionate.

161. In its written representations, DPP sought to argue that the fine proposed in the Notice of Intent was not in line with the Penalty Notice[76] issued by the Commissioner to Tuckers Solicitors LLP (**Tuckers**) on 28 February 2022 on the basis that Tuckers are a similar business to DPP in that a substantial part of their legal activities is legally aided criminal law.

162. DPP submitted that taking into account fees generated on an annual basis and numbers of staff employed in both firms, the fine proposed in the Notice of Intent was not comparable on a *per employee* basis. DPP

[76] Tuckers Solicitors LLP monetary penalty notice (https://ico.org.uk/media/action-weve-taken/mpns/4019746/tuckers-mpn-20220228.pdf).

further submitted that a penalty of less than £20,000 would be more appropriate.

163. Having considered DPP's written representations on this issue, the Commissioner remains satisfied that the Fining Guidance has been correctly applied to the outcome of his investigation into DPP's infringements. In particular, the Commissioner is satisfied that:

a) The monetary penalty notice issued to Tuckers cannot be directly comparable to DPP because the fine imposed on Tuckers was calculated under the Commissioner's previous guidance for calculating monetary penalties.[77] In any event, it is not appropriate for the Commissioner to compare enforcement action taken in previous cases because each case turns on its own facts and circumstances.

b) Neither the UK GDPR nor the DPA 2018 provide any legal basis for calculating a fine by reference to the number of people employed by an organisation.

c) In calculating the fine imposed on DPP, due regard has been given to all the factors set out in Article 83(2) UK GDPR (in particular, applicable factors aggravating or mitigating the circumstances of the case). These factors differ case-to-case and must be considered on the facts of each case.

d) Upon considering all the circumstances of the case, a fine in the sum of £60,000 is effective, proportionate and dissuasive, therefore an appropriate adjustment was required when applying Step 5 of the Fining Guidance to the facts of DPP's case. In determining the appropriate adjustment to make at Step 5 to

[77] The fine in Tuckers was calculated under the Commissioner's Regulatory Action Policy; whereas, the fine imposed on DPP has been calculated under the Fining Guidance.

ensure the fine is effective, proportionate and dissuasive, the Commissioner has exercised his evaluation and judgement taking into account all the relevant circumstances of this case.

164. In making his decision and setting the amount of the penalty, the Commissioner has also had regard to the desirability of promoting economic growth (as required by section 108(1) of the Deregulation Act 2015). In particular, the Commissioner has taken into consideration:

a) the nature and level of risk associated with non-compliance with data protection legislation (including risks to economic growth);

b) the steps taken by DPP to achieve compliance and the reasons for its failure;

c) the willingness and ability of DPP to address its non-compliance;

d) the likely impact of the proposed intervention on DPP's business and the likely impact of the Commissioner's regulatory intervention on the wider legal services sector (both in terms of deterrence and the economic benefit to legal services firms); and

e) the necessity and proportionality of imposing a penalty on DPP in the sum of £60,000 in respect of its infringements of the UK GDPR.

Having regard to the factors stated above, the Commissioner considers that this Penalty Notice is unlikely to have an impact on any measure of economic activity or growth in the United Kingdom, including levels of employment and Gross Domestic Product.

F. Conclusion - Penalty

165. For the reasons set out above, the Commissioner decides to impose a monetary penalty on DPP in the amount of £60,000.

G. Financial hardship

166. The Fining Guidance outlines that, in exceptional circumstances, the Commissioner may reduce a fine where an organisation is unable to pay due to its financial position.[78]

167. The Notice of Intent given to DPP on 11 December 2024 indicated that the amount of the penalty the Commissioner proposed to impose was £60,000. The Commissioner received no representations from DPP in relation to financial hardship.

VII. PAYMENT OF THE PENALTY

168. The penalty must be paid to the Commissioner's office by BACS transfer or cheque by 19 May 2025.

169. Under paragraph 9(1) of Schedule 16 to the DPA, the Commissioner cannot take action to recover a penalty unless:

a) the period specified in this Penalty Notice (i.e. by 19 May 2025) has ended;

b) any appeals against this Penalty Notice have been decided or otherwise ended;

c) if this Penalty Notice has been varied, any appeals against the penalty variation notice have been decided or otherwise ended; and

d) the period for DPP to appeal this Penalty Notice, and any variation of it, has ended.

[78] Fining Guidance at paragraph 151.

170. Under paragraph 9(2) of Schedule 16 to the DPA, in England and Wales, the Commissioner is able to enforce the payment of the penalty. The penalty is recoverable:

a) if the County Court so orders, as if it were payable under an order of that court; or
b) if the High Court so orders, as if it were payable under an order of that court.

VIII. RIGHTS OF APPEAL

171. By virtue of section 162 DPA, DPP may appeal to the First-tier Tribunal (General Regulatory Chamber) (Information Rights) against this Penalty Notice. DPP may appeal to the Tribunal against the amount of the penalty, whether or not it appeals against the Penalty Notice.

172. Information about the appeals process is set out in the Annex. Any notice of appeal should be sent or delivered to the Tribunal so that it is received within 28 days of the date of this Penalty Notice.

Dated: 14 April 2025

Andy Curry
Director of Investigations (Interim)
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX

DATA PROTECTION ACT 2018 (PART 6, SECTION 162)

RIGHTS OF APPEAL

1. By virtue of section 162(1) of the DPA, you may appeal to the Tribunal against this Penalty Notice. By virtue of section 162(3), you may appeal to the Tribunal against the amount of the penalty specified in this Penalty Notice, whether or not you appeal against this Penalty Notice.

2. If you appeal and if the Tribunal considers:

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

    b. to the extent that the notice or decision involved an exercise of discretion by the Commissioner, that the Commissioner ought to have exercised the discretion differently,

    the Tribunal must allow the appeal or substitute another notice or decision which the Commissioner could have given or made.

3. You may bring an appeal by sending a notice of appeal to the Tribunal at:

    grc@justice.gov.uk

    or

    General Regulatory Chamber
    HM Courts and Tribunals Service
    PO Box 9300
    Leicester
    LE1 8DJ
    UK
    (Telephone: 0300 123 4504)

a. The notice of appeal should be received by the Tribunal within 28 days of the date of this Penalty Notice (which is the date that this Penalty Notice was sent).

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

4. The notice of appeal **must** include:

a. your name and address;

b. the name and address of your representative (if any);

c. an address where documents may be sent or delivered to you;

d. the name and address of the respondent (the Information Commissioner);

e. details of the decision to which the proceedings relate;

f. the result you are seeking;

g. the grounds on which you rely;

h. a full copy of this Penalty Notice; and

i. (if the notice of appeal is late) a request for an extension of time, giving the reason(s) why the notice of appeal is late and why the Tribunal should accept it.

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 their case themselves or may be represented by any person whom they 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 The Tribunal

Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).