FOR PUBLIC RELEASE

PENALTY NOTICE

POLICE SERVICE OF NORTHERN IRELAND

26 September 2024

Table of Contents

DATA PROTECTION ACT 2018

ENFORCEMENT POWERS OF THE INFORMATION COMMISSIONER

PENALTY NOTICE

To: The Chief Constable of the Police Service of Northern Ireland

Of: PSNI Headquarters
65 Knock Road
Belfast
BT5 6LE

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 the Chief Constable of the Police Service of Northern Ireland (the "**PSNI**") to pay the Commissioner £750,000.

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

[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.

including the circumstances of the infringements and the nature of the personal data involved.

3. In accordance with paragraph 2 of Schedule 16 to the DPA, the Commissioner gave a notice of intent to the PSNI on 20 May 2024, setting out the reasons why the Commissioner proposed to give the PSNI a penalty notice. In that notice of intent, the Commissioner indicated that the amount of the penalty he proposed to impose was £750,000.

4. On 14 June 2024, the PSNI made written representations about the Commissioner's intention to give a penalty notice. On 5 July 2024 the Commissioner sought clarification on the written representations, which the PSNI provided on 12 July 2024. This Penalty Notice takes into account the written representations from the PSNI and, where appropriate, makes specific reference to them.

5. The Commissioner finds that between 25 May 2018[2] and 14 June 2024[3] the PSNI infringed Articles 5(1)(f), 32(1) and (2) UK GDPR for the reasons set out in this Penalty Notice. In summary:

    a) The infringements relate to the processing of personal data of PSNI officers and staff that took place whenever workforce data[4] downloaded from the PSNI human resources management system was analysed in Excel by PSNI staff to prepare information to be disclosed in response to freedom of information requests (the "**Relevant Processing**").

[2] The date of commencement of the DPA and application of the GDPR.
[3] The date on which the Commissioner finds the PSNI implemented appropriate security measures (see paragraphs 90 to 93 below).
[4] Specifically, the data file called "Combined 3C & Perlist", which includes (for all officers and staff who are in post, suspended or on a career break at the time of download) the following categories of personal data: surnames and first name initials, job role, rank/grade, department, location of post, contract type, gender and PSNI service/staff number.

b) The infringements of Article 5(1)(f) and Article 32 UK GDPR occurred because the Relevant Processing was not carried out in a manner that ensured appropriate security[5] of the personal data of PSNI officers and staff, using appropriate technical and organisational measures as required by Article 5(1)(f) and Article 32 UK GDPR.

6. As a consequence of the PSNI not having appropriate security measures in place as required by Article 5(1)(f) and Article 32 UK GDPR, the personal data of 9,483 police officers and staff was disclosed to a public-facing website on 8 August 2023 (the "**8 August Incident**").

7. The 8 August Incident involved the unauthorised disclosure[6] of the personal data of all PSNI police officers and staff, when a spreadsheet released in response to a freedom of information ("**FOI**") request was published on the website https://www.whatdotheyknow.com/.

8. On 10 August 2023, the PSNI described the 8 August Incident as an "*unprecedented and industrial scale data breach*".[7] On 14 August 2023, the PSNI made the following statement: "*We are now confident that the workforce data set is in the hands of Dissident Republicans. It is now a planning assumption that they will use this list to generate fear and uncertainty as well as intimidating or targeting officers and staff.*"[8]

9. On 22 August 2023, the PSNI and the Northern Ireland Policing Board commissioned an independent review into the circumstances surrounding the 8 August Incident. The final report of that independent

[5] Specifically, protection against unauthorised disclosure.
[6] Article 4(12) 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.
[7] Statement from the Chief Constable on the data breach investigation | PSNI, 10 August 2023 (accessed 26 September 2024).
[8] Update from the Chief Constable on the data breach investigation | PSNI, 14 August 2023 (accessed 26 September 2024).

review described the 8 August Incident as "*the most significant data breach that has ever occurred in the history of UK policing, not only because of the nature and volume of compromised data, but because of the political history and context that sets the backdrop of contemporary policing in Northern Ireland and therefore the actual, or perceived, threats towards officers, staff, and communities.*"[9]

10. The Commissioner received complaints from data subjects (PSNI officers and staff) describing the damage they suffered as a consequence of the 8 August Incident. The damage and distress described in the complaints is often severe and includes concerns about personal safety and the safety of family members, changes required to home security measures and the need to relocate.

11. In deciding to give this Penalty Notice, the Commissioner has had regard to the matters listed in Articles 83(1) and (2) UK GDPR. The Commissioner considers the imposition of a penalty is an effective, proportionate and dissuasive measure. The Commissioner has had regard to the revised approach to public sector enforcement[10] and is satisfied that this case is sufficiently egregious to warrant the imposition of a penalty.

12. Having had regard to the matters listed in Articles 83(1) and (2) UK GDPR, and in accordance with his Data Protection Fining Guidance,[11] the Commissioner determined the amount of the penalty as £5,600,000. The Commissioner has however had regard to the revised approach to public sector enforcement and has reduced the penalty amount to **£750,000**.

[9] PSNI Independent review final report, 11 December 2023, p. 2-3.
[10] Open letter from UK Information Commissioner John Edwards to public authorities, 30 June 2022. The revised approach (which was trialled for a two-year period ending in June 2024) is currently under review. The revised approach continues to be applied pending the outcome of that review: ICO statement on its public sector approach trial | ICO.
[11] Data Protection Fining Guidance | ICO, 18 March 2024.

II. RELEVANT LEGAL FRAMEWORK

13. Section 155 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 notice, require the person to pay to the Commissioner an amount in sterling specified in the notice.

14. 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).*"

15. Chapter II of the 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 at point (f) includes the requirement that "*personal data shall be … processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised … processing … using appropriate technical or organisational measures*". This is referred to in the UK GDPR as the "*integrity and confidentiality*" principle.

16. 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 … unauthorised disclosure of … personal data transmitted, stored or otherwise processed."

17. The legal framework for penalties is set out at Section V(A) below.

III. BACKGROUND TO THE INFRINGEMENTS

18. 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.

A. The personal data breach reported by the PSNI

19. The PSNI is the police service responsible for law enforcement within Northern Ireland. The PSNI is "*the only routinely armed service in the United Kingdom with the unique additional challenge of policing in the context of a 'substantial' terrorist threat*".[12]

20. On 8 August 2023 at 17:10, the PSNI contacted the Commissioner's office (the "**ICO**") by phone to make the ICO aware of a personal data breach. At 20:20 on the same day, the PSNI submitted an online form to the Commissioner, formally reporting the personal data breach which had taken place at 14:31 that day.[13] The PSNI reported that at approximately 16:10, the PSNI's Operational Support Department

[12] A History of Policing in Ireland | PSNI (accessed 26 September 2024). At the time of the 8 August Incident, the national security threat level was "severe" (a level higher than "substantial"). Further information about the context in which the PSNI operates has been set out at Section IV(B) below.
[13] PSNI Initial breach report, 08 August 2023, p. 1.

became aware that information which had been used to generate a response to an FOI request had been "*provided by PSNI's HR department in an unmarked tab on the Excel spreadsheet released as part of the FOI response. Whilst the FOI response had high level information being released in full under the FOIA, the unmarked tab used to generate the information was not deleted from the spreadsheet. It contained the names (surname and initial), ranks, contract types, cost codes regarding post funding for all PSNI officers and staff. The incident is now being investigated by PSNI under a Gold command structure*".

21. The timeline of events leading up to the 8 August Incident was as follows:[14]

3 August 2023

a) On 3 August 2023 the PSNI received an FOI request via the WhatDoTheyKnow website asking for "*the number of officers at each rank and number of staff at each grade in tables as of 01/08/2023*".

b) Six minutes later, the PSNI received another request (from the same person) via the WhatDoTheyKnow website: *"Could you please provide the number of officers and staff at each rank or grade distinguishing between how many are substantive/temporary/acting as of 01/08/2023. Could you please provide this information in the form of tables for officers and tables for staff."*

[14] The PSNI and the Northern Ireland Policing Board jointly commissioned an independent review into the 8 August Incident. The independent review was led by Pete O'Doherty, Temporary Commissioner for the City of London Police and National Police Chief's Council Lead for Information Assurance and Cyber Security. The independent review's final report (titled "Protecting From Within") was published on 11 December 2023. The timeline of the 8 August Incident is set out in that final report at p. 15.

c) The Corporate Information Branch ("**CIB**") is the department within the PSNI responsible for handling FOI requests received by the PSNI. A member of staff in the CIB sent an acknowledgement to the requester. The acknowledgement explained that the requester's "*…requests on this subject [Officers and Staff by Rank and Grade] have been aggregated…*". Effectively, the PSNI would respond to the second request.

4 August 2023

d) The (second) FOI request was assigned to an FOI Decision Maker within CIB. FOI Decision Makers are the staff within CIB with day-to-day responsibility for handling FOI requests. They co-ordinate the identification and preparation of requested information and make decisions regarding the application of FOI exemptions.[15] For each FOI request, FOI Decision Makers are required to (contemporaneously) complete an FOI Audit Log. The FOI Audit Log is a checklist which sets out the various stages of handling an FOI request and the checks required at each stage.

e) The assigned FOI Decision Maker identified Human Resources (specifically, the Workforce Planning Team) as the business area within the PSNI which held information relevant to the FOI request. The FOI Decision Maker asked the Workforce Planning Team to provide that information by sending the Workforce

[15] The PSNI's FOI Service Instruction (updated October 2019) describes their role as follows: "*The Decision-Maker will be the first port of call for FOI enquiries. This involves obtaining all relevant information and compiling responses to requests and appeals, through liaising with business areas*." (FOI Service Instruction, 2 October 2019, p. 16).

Planning Team the wording of the FOI request along with a case tracker form.[16]

7 August 2023

f) A member of the Workforce Planning Team prepared the information requested using workforce data. Specifically, they used a file of data downloaded from the PSNI's human resources management system (referred to internally as "SAP"). This data file, referred to as "Combined 3C & Perlist",[17] was an Excel file (workbook) containing a single worksheet titled "SAP DOWNLOAD". The workforce data included (for all officers and staff who were in post, suspended or on a career break at the time of download) the following categories of personal data: surnames and first name initials, job role, rank/grade, department, location of post, contract type, gender and PSNI service/staff number. The workforce data was analysed to prepare information relevant to the FOI request. Multiple other worksheets were created within the Excel file as part of this analysis, with one worksheet containing the final information prepared for FOI disclosure (the "**Return worksheet**").

g) The member of the Workforce Planning Team then deleted all the tabs visible on their screen from the Excel file, other than the tab for the Return worksheet.[18] They did not know that the three

[16] Case tracker forms "*seek views from the business areas on the application of any relevant harm in releasing information into the public domain as well as the application of any cost considerations*" (PSNI Second enquiries response letter, 22 September 2023, p. 5).
[17] PSNI Further enquiries response letter, 22 March 2024, p. 2-3.
[18] Worksheets are typically displayed as tabs at the bottom of an Excel file (a workbook). A workbook can contain hundreds of worksheets, but the number of tabs that are displayed at any given time is limited (how many tabs are displayed can also be affected by the length of the horizontal scrollbar at the bottom of the workbook). When there are more worksheets than there are visible tabs, three

horizontal dots to the left of the remaining visible tab (the tab for the Return worksheet) indicated that the Excel file continued to contain the "SAP DOWNLOAD" worksheet which contained the workforce data (as originally downloaded from the human resources management system, SAP).

8 August 2023:

h) The Excel file was then sent to the Head of Workforce Planning for quality assurance, who opened the Excel file and inspected the (only) visible tab (the tab for the Return worksheet). They checked that the information contained in the Return worksheet was accurate and relevant to the FOI request.[19] The Head of Workforce Planning did not notice the three horizontal dots or was unaware of what they represented.[20] Following this quality assurance, the Excel file was sent at 10:09 to the FOI Decision Maker in CIB.[21]

i) Using Microsoft Word, the FOI Decision Maker then drafted a letter responding to the FOI request. The FOI Decision Maker attempted to copy the prepared information across (from the Return worksheet of the Excel file to the Word document) but, on this occasion, they were unable to do so. They therefore decided to disclose the Excel file as a separate file accompanying their response letter. The FOI Decision Maker also did not notice the three horizontal dots or was unaware of what they

horizontal dots appear to the left of the visible tabs (and another set of three horizontal dots can appear to the right). These dots indicate that there are more worksheets than there are visible tabs. Deleting visible tabs does not guarantee deletion of all worksheets in a workbook (unless a user attempts to delete all visible tabs).

[19] PSNI Fourth enquiries response letter, 13 December 2023, p. 2.

[20] PSNI Third enquiries response letter, 15 November 2023, p. 3.

[21] PSNI Fourth enquiries response letter, 13 December 2023, p. 2.

represented. The FOI Decision Maker sent the response letter and accompanying Excel file to the PSNI's Strategic Communications and Engagement Department ("**SCED**").[22] SCED had asked to have sight of the prepared information prior to its disclosure to the FOI requester. The SCED staff who reviewed the Excel file (and approved its disclosure[23]) also did not notice the three horizontal dots or were unaware of what they represented.

j) At 14:31 the FOI Decision Maker uploaded the response letter and accompanying Excel file to the WhatDoTheyKnow website. The Excel file contained the Return worksheet (as was intended) but also contained (unknown to the FOI Decision Maker) the "SAP DOWNLOAD" worksheet.

k) Either by clicking on the three horizontal dots to the left of the visible tab or by using the arrows to the left of those three horizontal dots, the "SAP DOWNLOAD" worksheet would become visible as a tab, which, once clicked, would make the "SAP DOWNLOAD" worksheet visible on screen.

l) The PSNI became aware of the presence of the "SAP DOWNLOAD" worksheet in the uploaded Excel file at approximately 16:10, when officers alerted the PSNI's Operational Support Department Staff Office.[24] The PSNI contacted the WhatDoTheyKnow website administrators at 16:47 to request removal of the Excel file. The WhatDoTheyKnow website administrators responded at 16:51 to confirm that the

[22] PSNI Second enquiries response letter, 22 September 2023, p. 4.
[23] PSNI Initial enquiries response letter, 29 August 2023, p. 4.
[24] PSNI Initial enquiries response letter, 29 August 2023, p. 2.

Excel file had been hidden from external view, and at 17:27 confirmed that the Excel file had been deleted from the website.

m) The "SAP DOWNLOAD" worksheet was accessible to the public via the WhatDoTheyKnow website for approximately 2 hours and 20 minutes (between the hours of 14:31 and 16:51).

22. At 17:10 on the same day, the PSNI's Head of Corporate Information informed the ICO of the incident by telephone. At 20:20, they submitted a data breach report online.[25] The report confirmed that the PSNI considered the 8 August Incident met the threshold for notifying a personal data breach to the Commissioner under Article 33 UK GDPR.

23. The 8 August Incident was communicated to the data subjects whose personal data had been disclosed (all PSNI officers and staff) on the same day at 17:07 by email.[26]

24. Upon becoming aware of the 8 August Incident the PSNI launched "*Operation Sanukite*". The Gold Commander[27] of this operation was Assistant Chief Constable Todd, who is also the PSNI's Senior Information Risk Owner ("**SIRO**"). The strategy for Operation Sanukite was first drawn up on 10 August 2023, and set 15 objectives, the first two of which were "*1) To prioritise the protection of officers and staff. 2) To contain the data leak as much as possible to prevent further consequences.*" In describing the 8 August Incident, the strategy noted that "*The implications for the police service in terms of reputation etc. are immense.*"[28]

[25] PSNI Initial breach report, 8 August 2023.
[26] Internal meeting notes from PSNI visit on 18 October 2023, p. 1.
[27] A GSB (gold silver bronze) structure is a command hierarchy that is often applied to police operations. The Gold Commander has overall strategic command of an operation. See Command structures | College of Policing (accessed 26 September 2024)
[28] PSNI Gold Strategy - Op Sanukite, 10 August 2023 p. 3.

25. On 14 August 2023 the PSNI provided a public update on Operation Sanukite, which included the following statement: "*We are now confident that the workforce data set is in the hands of Dissident Republicans. It is now a planning assumption that they will use this list to generate fear and uncertainty as well as intimidating or targeting officers and staff. I won't go into detail for operational reasons but we are working round the clock to assess the risk and take measures to mitigate it.*"[29]

26. The PSNI provided an in-person briefing on Operation Sanukite to the Commissioner's investigation team on 18 October 2023.[30] The PSNI explained that as part of Operation Sanukite, the PSNI was taking steps to change officer and staff identification numbers and to reduce their use. The Commissioner understands these steps were aimed at reducing the identifiability of PSNI officers and staff. They included:

    a) Ensuring service numbers and staff numbers do not appear on payslips. Service numbers are identification numbers which are not public-facing, and which are issued to all officers. They are equivalent to "warrant numbers" or "police numbers". Staff numbers are identification numbers issued to police staff. Both service numbers and staff numbers were included in the workforce data that was disclosed as part of the 8 August Incident.

    b) Seeking legislative changes so that officers could be identified on search records, warrants and other legal documents other than by means of their service numbers.[31]

[29] Update from the Chief Constable on the data breach investigation | PSNI, 14 August 2023 (accessed 26 September 2024).
[30] Internal meeting notes from PSNI visit on 18 October 2023.
[31] PSNI Op Sanukite Update, 18 October 2023 and Internal meeting notes from PSNI visit on 18 October 2023.

c) Changing the shoulder numbers of all officers. A shoulder number is an identification number (different to a service number) worn on epaulettes by uniformed officers at certain ranks. They were not included in the workforce data which was disclosed as part of the 8 August Incident.

27. Other steps the PSNI has taken to mitigate the impact of the 8 August Incident on the affected data subjects include[32]:

a) Setting up an Emergency Threat Management Group ("**ETMG**"). PSNI staff and officers were able to refer themselves to the ETMG to raise their concerns at a one-to-one meeting with a senior manager. Appropriate risk mitigations (such as financial support for security enhancements to homes[33] or relocation[34]) would be discussed at these meetings. Due to the high volume of referrals, the ETMG first categorised referrals using a RAG rating. Those referrals which the ETMG categorised as "red" were prioritised. The factors taken into account in this assessment included: the area where the individual lived and their relevant community background; whether the individual had an uncommon name; whether the individual had received previous threats; whether the individual had a personal protection weapon; whether the individual worked in a high-risk area such as source handling or terrorism investigations; and any other specific factors raised in the referral. The ETMG was set up to operate seven days a week, 7am to 7pm, with out of hours availability.

b) Senior officers visiting and engaging with their officers and staff to offer support and reassurance.

[32] PSNI Initial enquiries response letter, 29 August 2023, p. 11.
[33] PSNI Op Sanukite Update, 18 October 2023, p. 1.
[34] Internal meeting notes from PSNI visit on 18 October 2023, p. 2.

c) Regularly communicating updates relating to the 8 August Incident to officers and staff.

d) Enabling officers and staff to access a copy of their personal data that had been disclosed as part of the 8 August Incident.[35]

e) Providing additional guidance to line managers around the range of welfare and wellbeing support available to officers and staff, as well as guidance on holding crisis management briefings with teams.

f) Setting up FAQ pages on the PSNI intranet to assist officers and staff, such as by providing guidance on how to remove entries from the open electoral register and on how to remove personal information from the Companies House register. The PSNI has agreed to reimburse officers and staff for the costs of removing information from the Companies House register.[36]

g) Offering financial support to officers and staff who have been directly linked to a terrorist investigation to support security enhancements to their home.[37]

28. Policies and guidance (relevant to the security of the Relevant Processing) which the PSNI introduced following the 8 August Incident are described at paragraphs 45 to 47 below.

[35] PSNI Initial enquiries response letter, 29 August 2023, p. 4.
[36] Internal meeting notes from PSNI visit on 18 October 2023, p. 4.
[37] PSNI Op Sanukite Update, 18 October 2023, p. 1.

29. On 4 September 2023, the Secretary of State for Northern Ireland made a statement on the 8 August Incident in the House of Commons.[38] The Secretary of State noted that "*This data breach is deeply concerning and significant. Recent events in Northern Ireland, including the terrible attack on Detective Chief Inspector John Caldwell, show there are still a small minority in Northern Ireland who wish to cause harm to PSNI Officers and staff in Northern Ireland. ... there is significant concern about the consequences of this data breach. Many PSNI officers and staff have raised concerns about themselves and their family … In response to these concerns, the PSNI and wider security partners are taking appropriate action and are working around the clock to investigate the incident, provide reassurance and mitigate any risk to the safety and security of officers and staff. As of 30 August 3,954 self referrals have been made to the PSNI's Emergency Threat Management Group. This is part of the welfare and support services which have been made available to PSNI officers.*"

30. The UK Parliament's Northern Ireland Affairs Committee launched a probe into the 8 August Incident,[39] taking oral evidence in September and December 2023.[40] Evidence was taken from the PSNI, bodies representing officers and staff, and the Northern Ireland Policing Board ("**NIPB**").[41]

31. The PSNI and the NIPB jointly commissioned an independent review into the 8 August Incident. The independent review was led by Pete O'Doherty, Temporary Commissioner for the City of London Police and

[38] Secretary of State's speech - PSNI data breach - GOV.UK (www.gov.uk), 4 September 2023 (accessed 26 September 2024).
[39] Other personal data breaches were also within the scope of the probe.
[40] PSNI data breaches - Committees - UK Parliament (accessed 26 September 2024).
[41] The NIPB is an independent public body with a range of statutory functions, including oversight of the PSNI.

National Police Chief's Council ("**NPCC**") Lead for Information Assurance and Cyber Security. The independent review's final report (titled "Protecting from Within") was published on 11 December 2023. The report referred to the 8 August Incident as "*the most significant data breach that has ever occurred in the history of UK policing, not only because of the nature and volume of compromised data, but because of the political history and context that sets the backdrop of contemporary policing in Northern Ireland and therefore the actual, or perceived, threats towards officers, staff, and communities*."

B. The PSNI's relevant procedures, policies and guidance

Organisational measures in place prior to the 8 August Incident

32. During his investigation, the Commissioner asked for information about the PSNI's procedure for handling FOI requests. The PSNI initially responded by referring to the FOI Service Instruction.[42]

33. The PSNI's FOI Service Instruction purports to be a document which "*clearly defines the responsibilities placed on the Police Service of Northern Ireland to ensure compliance with the Freedom of Information Act 2000 and the Environmental Regulations 2004*".[43] It was first issued on 17 May 2018. It was updated in October 2019 and again in July 2023.[44]

34. During the investigation, the PSNI explained that the FOI Service Instruction contained only a high-level description of how FOI requests

[42] PSNI Initial enquiries response letter, 29 August 2023, p. 4.
[43] PSNI FOI Service Instruction, 2 October 2019, p. 1.
[44] PSNI Fourth enquiries response letter, 13 December 2023, p. 4.

were handled;[45] the PSNI went on to provide more detailed explanations of the procedure.

35. On the basis of those explanations, the Commissioner finds that in practice, the procedure (as it related to the Relevant Processing[46]) consisted of the following key steps:

a) Each FOI request is assigned to an FOI Decision Maker from CIB, whose responsibilities include completing an FOI Audit Log (a checklist which sets out the stages of handling an FOI request and the checks required at each stage).

b) The assigned FOI Decision Maker identifies the relevant team (in this case, the Workforce Planning Team) as the business area within the PSNI which holds information relevant to the FOI request. The FOI Decision Maker asks the Workforce Planning Team to provide that information.[47]

c) A member of the Workforce Planning Team uses workforce data to prepare the information requested. Specifically, they use a file of data downloaded from the PSNI's human resources management system (SAP). This data file, referred to as "Combined 3C & Perlist",[48] is an Excel file (workbook) containing a single worksheet titled "SAP DOWNLOAD". The workforce data

[45] PSNI Second enquiries response letter, 22 September 2023, p. 5. The July 2023 version was not, however, in effect at the time of the 8 August Incident.
[46] That is, the procedure for handling those FOI requests which required analysis of workforce data downloaded from SAP.
[47] Specifically, the FOI Decision Maker sends the Workforce Planning Team the wording of the FOI request along with a case tracker form. Case tracker forms "*seek views from the business areas on the application of any relevant harm in releasing information into the public domain as well as the application of any cost considerations*" (PSNI Second enquiries response letter, 22 September 2023, p. 5).
[48] PSNI Further enquiries response letter, 22 March 2024, p. 2-3.

within the Excel file is analysed to prepare information relevant to the FOI request.[49] Multiple other worksheets are created within the Excel file as part of this analysis, with one worksheet (a Return worksheet) containing the information prepared for FOI disclosure. This prepared information usually takes the form of a table (and can sometimes be an Excel Pivot Table). All other worksheets (containing the workforce data as downloaded and any other data workings) are deleted from the Excel file, which is then saved as a "return copy" file. The return copy Excel file ought to contain only the Return worksheet.[50]

d) The Head of Workforce Planning (as the relevant Operational Lead) quality assures the return copy Excel file,[51] which involves checking the information prepared is accurate and relevant to the FOI request.[52] It is then sent to the FOI Decision Maker in CIB.

e) The FOI Decision Maker[53] reviews the return copy Excel file and drafts an FOI response letter. The return copy Excel file may be disclosed to the FOI requester as a separate attachment to the FOI response letter; alternatively, the prepared information contained in the return copy Excel file may be incorporated into the FOI response letter itself. The FOI Decision Maker applies redactions as appropriate.

[49] The analysis of this personal data in Excel is the Relevant Processing with respect to which this Penalty Notice is given.
[50] PSNI Fourth enquiries response letter, 13 December 2023, p. 2.
[51] PSNI Third enquiries response letter, 15 November 2023, p. 4.
[52] PSNI Fourth enquiries response letter, 13 December 2023, p. 2.
[53] Also referred to as "Corporate Information Decision-Makers" in the FOI Service Instruction.

f) The FOI Decision Maker may[54] discuss the draft FOI response letter with their line manager (a Corporate Information Team Leader) ("**Team Leader**"). If a discussion takes place, the Team Leader will assess whether quality assurance[55] is required (for instance, if the request is sensitive[56] or complex[57]). The types of issues which would typically be raised in these discussions would include the statutory exemptions that might apply, any harm that might arise in making the FOI disclosure and whether there had been any similar FOI requests. If quality assurance is considered necessary, the draft FOI response letter (along with any attachment) is sent to the Team Leader. Quality assurance by the Team Leader involves completion of the FOI Response Quality Assurance Checklist, which includes points such as "*Are the relevant exemptions listed by number, subsection and title*" and "*If prejudice based exemptions is the harm correctly explained*" and "*Format Correct / Spellchecked*".[58]

[54] The PSNI stated (PSNI Third enquiries response letter, 15 November 2023, p. 4) that "*only FOI responses identified as requiring further QA are discussed at 1-1 meetings*". The PSNI subsequently stated (PSNI Fourth enquiries response letter, 13 December 2023, p. 3) that "*while all responses should be discussed in general terms with a manager, these discussions may not take place at a 1-1 meeting*". The Commissioner is not convinced that the PSNI's procedure required the FOI Decision Maker to discuss every proposed FOI response with a line manager (whether in general or specific terms, and whether at pre-scheduled weekly 1-1 meetings or outside such meetings). The Commissioner notes that in the specific instance of the 8 August Incident, the FOI Decision Maker did not discuss the proposed response with a line manager; despite this, the PSNI maintain that the FOI Decision maker involved in the 8 August Incident *"followed the current process"* (PSNI Fourth enquiries response letter, 13 December 2023, p. 3; Copy of the FOI Audit Log completed by FOI Decision Maker, p. 3; PSNI Third enquiries response letter, 15 November 2023, p. 2).

[55] PSNI Second enquiries response letter, 22 September 2023, p. 5.

[56] PSNI Third enquiries response letter, 15 November 2023, p. 4 and PSNI Second enquiries response letter, 22 September 2023, p. 6.

[57] PSNI Second enquiries response letter, 22 September 2023, p. 6.

[58] PSNI 2019 QA Log.

g) Following any quality assurance by the Team Leader, the FOI decision maker discloses the FOI response letter (along with any attachment) to the FOI requester.[59] This may be done through the WhatDoTheyKnow website.

36. This procedure was followed by PSNI staff in connection with the 8 August Incident (see the timeline at paragraph 21 above). The PSNI informed the Commissioner that *"staff members followed the current process but this did not prevent the additional data from being attached to the response … no misconduct proceedings against staff are being initiated as a result."*[60]

37. The Commissioner has considered whether the FOI Service Instruction, FOI Audit Log or FOI Response Quality Assurance Checklist contained any guidance that could have prevented incidents such as the 8 August Incident. In particular, the Commissioner considered whether these documents contained any guidance relating to Excel files and checks for hidden data.

38. Prior to the 8 August Incident, the PSNI's FOI Service Instruction did not contain any guidance relating to the secure analysis of personal data in Excel (in particular, the importance of ensuring personal data was – if appropriate - removed from Excel files once analysis had been completed). The FOI Service Instruction did not contain any guidance relating to the format in which electronic files should be disclosed to an FOI requester. Whilst the FOI Service Instruction referred to checks and quality assurance, it provided no guidance as to what those checks and

[59] The PSNI's Strategic Communications and Engagement Department may also review the proposed response prior to disclosure.
[60] PSNI Third enquiries response letter, 15 November 2023, p. 2.

assurance processes should entail. In particular, there was no guidance to check FOI response letters and their attachments for hidden data.[61]

39. The template FOIA Audit Log includes questions such as: "*Have you double-checked the contact details of the requester to ensure they are accurate?*" and "*Has the requester expressed a format to receive the information?*". There is however no guidance relating to the appropriate format in which electronic files should be disclosed, and there is no question prompting the FOI decision maker to check FOI response letters and attachments for hidden data. The FOI Response Quality Assurance Checklist is similarly deficient.

40. The PSNI also confirmed that, prior to the 8 August Incident, there was no guidance or policy on the use of Excel, whether specific to the context of handling FOI requests or more generally.[62]

41. The Commissioner also investigated whether PSNI staff and officers involved in handling FOI requests had received any training which might have prevented incidents such as the 8 August Incident.

42. The Commissioner reviewed the mandatory FOI training for all PSNI staff and officers ("**all-staff FOI training**"). Staff in the PSNI's Workforce Planning Team, who would carry out the Relevant Processing, would

[61] Once FOI Decision Makers have made any redactions to the prepared information, the July 2023 FOI Service Instruction states "*Whilst all requests are discussed at a weekly 1-1, where relevant, requests will be sent to a team leader or other senior staff member if appropriate for quality assurance*" (FOI Service Instruction, July 2023, p. 15). The October 2019 version on the other hand simply instructs FOI Decision Makers to "*Send* [the proposed response] *to team leader for quality assurance*" (FOI Service Instruction, 2 October 2019, p. 15). For the reasons given at footnote 54 above, the Commissioner does not consider that, in practice, a discussion with a Team Leader was a required step in the PSNI's FOI handling procedure.

[62] PSNI Initial enquiries response letter, 29 August 2023, p. 5.

receive this training. The Workforce Planning Team staff involved in the 8 August Incident had received this training.[63]

43. The Commissioner also reviewed the "FOI/SAR Decision Maker" training which is mandatory for staff in the CIB (such as FOI Decision Makers and the Team Leader). The CIB staff involved in the 8 August Incident had received this training.[64]

44. Prior to the 8 August Incident, neither the all-staff FOI training nor the "FOI/SAR Decision Maker" training raised awareness of the risk that FOI response letters and their attachments might contain hidden data.[65] There was no guidance relating to checks for hidden data or the format in which electronic files should be disclosed.

Organisational measures introduced in August/September 2023

45. Once aware of the 8 August Incident, on the day of the personal data breach, the PSNI's SIRO[66] decided that, going forward, FOI responses should be provided in PDF format only (Excel files were not to be

[63] PSNI Third enquiries response letter, 15 November 2023, p. 5.
[64] PSNI Third enquiries response letter, 15 November 2023, p. 5.
[65] The Commissioner notes that the "FOI/SAR Decision Maker" training contained the following paragraph: "*Metadata: Metadata collected in electronic documents is also classed as being held for the purposes of FOI and if requested there is an expectation that this will be released to the requester. This metadata may contain the author, date, size; file paths, editing history, and formatting information of the document. In PSNI this is not normally provided and if requested we need to be mindful of the security of our staff (remove names) and our information.*" This paragraph only refers to scenarios where metadata is specifically requested by an FOI requester. It does not require the metadata of electronic documents to be checked as a matter of course (i.e. in scenarios where the FOI requester has not specifically requested metadata). The paragraph therefore does not relate to a check for hidden data.
[66] The SIRO role is at Assistant Chief Constable (ACC) rank and provides "*strategic decision making at a senior level responsible for promoting information governance and ensuring mitigation of information risks, including those linked to personal data*" (Data Protection Service Instruction, 11 February 2019, p. 5). The SIRO was (and continues to be) ACC Todd, who is also the Gold Commander of Operation Sanukite (PSNI Gold Strategy - Op Sanukite, 10 August 2023, p. 8).

attached), regardless of the format in which information had been requested.[67] This decision (the "**PDF Policy**") was communicated as a "direction" to CIB staff on 9 August 2023.[68]

46. By 29 August 2023 the PSNI had taken the decision "*that all external products must be flattened by PDF unless authorised by the Gold command structure in place*."[69]

47. On 8 September 2023, the PSNI issued an "*Interim Guidance on Sharing Data Securely"* (the "**Interim Guidance**").[70] The Interim Guidance applied to any instance of "*sharing MS Excel data externally*" (not just in the context of FOI responses) and it advised officers and staff on how to do so securely. In relation to FOI responses specifically, the Interim Guidance stated "*Flattened PDF/CSV files only for responses to all public requests, FOI or otherwise*." The Interim Guidance went on to illustrate how an Excel file can be saved as a PDF or CSV file. It was provided to staff within the CIB.[71]

IV. THE COMMISSIONER'S FINDINGS OF INFRINGEMENT

A. Controllership and jurisdiction

[67] PSNI Initial breach report, 08 August 2023, p. 4. As the Commissioner explains at paragraph 88 below, this policy was contrary to the PSNI's obligations under the Freedom of Information Act 2000.
[68] PSNI Email to the ICO responding to an additional query, 25 March 2024.
[69] PSNI Initial enquiries response letter, 29 August 2023, p. 5. The Commissioner understands this decision did not apply to FOI responses: the PDF Policy and the Interim Guidance indicate that FOI responses were not capable of such authorisation by the Gold command structure (i.e. FOI responses had to be flattened to PDF/CSV format, without exception).
[70] PSNI Interim security guidance on safe data sharing, 8 September 2023.
[71] PSNI Further enquiries response letter, 22 March 2024, p. 4.

48. The PSNI was the controller in respect of the Relevant Processing.[72] The PSNI determined its purpose and means within the meaning of Article 4(7) UK GDPR. The PSNI's Adult Privacy Notice confirms the PSNI is "*obliged to process*" personal data of "*personnel including … police officers and police staff*" pursuant to "*legal obligations including enactments*", and that it is a controller in respect of such processing.[73]

49. 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.

50. 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

51. The workforce data[74] involved in the Relevant Processing was personal data. It included a field for a (unique) service or staff number, which was an identifier (enabling the PSNI to directly distinguish one officer/staff member from another). The workforce data also contained two further fields: a data subject's full surname and first name initials. Collectively, these two further fields are highly likely to have been an identifier from the PSNI's perspective.

---

[72] The processing of personal data of PSNI officers and staff that took place whenever workforce data was analysed in Excel by PSNI staff to prepare information in response to freedom of information requests.
[73] Adult Privacy Notice | PSNI (accessed 26 September 2024).
[74] Specifically, the data file downloaded from the PSNI's human resources management system called "Combined 3C & Perlist". Whilst PSNI staff may have analysed other types of human resources data in Excel to prepare FOI responses, the Commissioner's investigation has focused solely on "Combined 3C & Perlist".

52. These identifiers (staff/service number; and the combination of surname and initials) and the 28[75] other fields contained in the workforce data which were associated with these identifiers (fields such as job role, rank/grade, department, post location, contract type and gender) constituted personal data: they were information relating to identified natural persons. The workforce data did not contain personal addresses of data subjects.

53. The workforce data downloaded and analysed to prepare a response to an FOI request (both in connection with the 8 August Incident and otherwise) was therefore personal data within the meaning of Article 4(1) UK GDPR and section 3(2) DPA. The 8 August Incident involved the unauthorised disclosure of this personal data.[76]

54. To understand the sensitivity of this personal data, it is important to recognise the history and unique political and policing context within Northern Ireland.

55. Since the foundation of Northern Ireland in 1921, the region has experienced sectarian conflict and violence known as "the Troubles". Throughout much of Northern Ireland there has been a long history of deep and seemingly irreconcilable divisions between nationalists (predominantly Roman Catholic) and unionists (generally Protestant).

56. It is however relevant to note that that whilst the Belfast Agreement (known as the Good Friday Agreement) was signed in 1998 and brought an end to the majority of the violence of the Troubles, there are dissident paramilitary groups who reject the political process and the institutions

[75] PSNI Anonymised copy of the spreadsheet disclosed as part of data breach contains 32 fields, but one of these is "*not used*". There is therefore a total of 31 information fields.
[76] PSNI Initial breach report, 8 August 2023.

created by the Good Friday Agreement. It has been reported that these dissident groups seek to destabilise Northern Ireland through the tactical use of violence, targeting members of the PSNI and other security personnel as well as seeking to cause disruption and economic damage.[77]

57. There remains a real risk to members of the PSNI[78] and the shooting of a senior police officer in February 2023 was a reminder of the threat still faced by police officers in Northern Ireland. As a result of this shooting, in March 2023 MI5 raised the national security threat level for Northern Ireland from *"substantial"* to *"severe*", meaning that the risk of a (Northern Ireland-related) terrorist attack was *"highly likely*".[79]

58. In response to the 8 August Incident, Assistant Chief Constable Chris Todd recognised that the PSNI *"is operating in an environment where there is a Severe threat of attack against our officers and staff from Northern Ireland Related Terrorism (NIRT). From the outset therefore a key planning assumption will be that a "reasonable worst case scenario" is that the data falls into the hands of those that would use it to cause harm to our officers, staff and their families*".[80]

59. The threat from dissident republicans is particularly acute in the case of PSNI officers/staff who are from a Catholic community background.

[77] Dissident republicans in Northern Ireland - what do they want? An explainer – The Irish News, 10 September 2023 (accessed 26 September 2024)
[78] Dissident republicans: Why Northern Ireland police are still a target - BBC News, 14 August 2023 (accessed 26 September 2024).
[79] Northern Ireland-related Terrorism threat level raised - GOV.UK (www.gov.uk), 28 March 2023 (accessed 26 September 2024). The threat level was reduced to "substantial" on 6 March 2024: Statement from the Secretary of State on the Northern Ireland Security Update - GOV.UK (www.gov.uk) (accessed 26 September 2024).
[80] PSNI Gold Strategy - Op Sanukite, 10 August 2023.

According to the latest PSNI workforce composition statistics, 33% of officers and 19% of staff are "*perceived Roman Catholic*".[81]

60. In light of this threat, in order to protect themselves and their friends and family, many PSNI officers and staff take steps to conceal their occupation from the world at large.[82]

61. The Commissioner notes that the extent to which PSNI officers and staff are able to conceal their occupation will vary according to specific role. PSNI officers in public-facing roles may only be able to conceal their occupation to a limited extent. PSNI staff who are in back-office roles may be more able to conceal their occupation.

62. The Commissioner also notes that some PSNI officers and staff choose not to conceal their occupation, despite their roles permitting them to do so.

63. Officers involved in covert roles, however, have no choice but to conceal their occupation. The workforce data which was subject to the Relevant Processing (and which was disclosed in the 8 August Incident) included the personal data of officers involved in covert roles (including their last name and first name initials). The Commissioner understands that although the workforce data did not explicitly label a given data subject as an officer involved in a covert role, strong inferences could be drawn to that effect (for instance, a data subject in the Crime Department's Intelligence Branch whose unit was marked "secret"[83] was likely to be an officer involved in a covert role).

---

[81] Workforce Composition Statistics | PSNI, 1 September 2024 (accessed 26 September 2024).
[82] PSNI data breach: 'Family fears for my safety as a police officer' - BBC News, 9 August 2023 (accessed 26 September 2024).
[83] Dissident republicans claiming to possess information from PSNI data breach, says Byrne – The Irish Times, 10 August 2023 (accessed 26 September 2024).

64. The PSNI has accepted the sensitivity of the workforce data. The PSNI explained in the data breach report that "*there is a risk of identification of officers and staff including those in crime operational roles*". The PSNI acknowledged the "*scale of this breach and the impacts to the safety of officers and staff*". The PSNI explained that "*our criminal investigation has confirmed the information is now in the hands of Dissident Republican Terrorists in Northern Ireland and PSNI has made this fact public*".[84]

C. The infringements

65. The fact that an unauthorised disclosure took place on 8 August 2023 (the 8 August Incident) is not, in and of itself, sufficient to find that the PSNI has infringed Articles 5(1)(f) and 32 UK GDPR.[85] The Commissioner has considered whether the facts set out at paragraphs 32 to 47 above (the PSNI's relevant procedures, policies and guidance) constitute infringements of the UK GDPR.

66. In order to assess the PSNI's compliance with Articles 5(1)(f) and 32 UK GDPR, the Commissioner must necessarily exercise his judgement, as regulator, as to what "*appropriate*" security and "*appropriate*" technical and organisational measures would be in the circumstances (that is, 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*").[86]

[84] PSNI Initial enquiries response letter, 29 August 2023.
[85] 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.
[86] See the text of Articles 5(1)(f) and 32 UK GDPR reproduced at paragraphs 15 and 16 above.

67. For the reasons set out below, the Commissioner's view is that the PSNI infringed Articles 5(1)(f), 32(1) and (2) UK GDPR. The infringements involved a failure by the PSNI 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

68. 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 PSNI officers and staff[87] which the Relevant Processing presented, in particular from unauthorised disclosure. Recital 75 UK GDPR states that such risk "*may result from personal data processing which could lead to physical, material or non-material damage*".

69. Unauthorised disclosure of the workforce data risked data subjects being identified as PSNI officers/staff by family and friends (to whom the data subject had not revealed their occupation). It also risked data subjects being physically identified by dissident republicans.

70. If dissident republicans physically identified a data subject as a PSNI officer/staff member, this carried a further risk that other individuals would be physically identified as family members or friends of that data subject.

71. The Commissioner recognises that the threat to PSNI officers and staff is not from dissident republicans alone; there is a threat from organised

[87] As well as of those officers and staff in post at the time, the workforce data contained the personal data of officers and staff who were suspended or on a career break (PSNI Initial enquiries response letter, 29 August 2023, p. 4).

crime groups and also from other paramilitary groups in Northern Ireland.

72. The Commissioner considers all three categories of damage as identified in Recital 75 UK GDPR (physical, material and non-material) could flow from the risks identified at paragraphs 69 to 71 above. Psychological harm, severe injury and even death could flow from those risks.

73. Recital 75 provides specific examples of damage. Of those examples, the Commissioner considers the following could have arisen from the risks identified at paragraphs 69 to 71 above:

a) loss of control over personal data (that is, a data subject losing control of information about their occupation);
b) deprivation of rights and freedoms (right to life, right to respect for private and family life, peaceful enjoyment of property);
c) discrimination;
d) financial loss;
e) damage to reputation.

74. Paragraph 113 below sets out the types of damage which materialised as a result of the 8 August Incident.

75. 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.

76. The severity of the risk is self-evident.

77. The following factors are relevant to the likelihood of the risk presented by the Relevant Processing:

a) The PSNI regularly received FOI requests which would require a member of the Workforce Planning Team to carry out the Relevant Processing. The PSNI confirmed that it was "*normal practice*" for the Workforce Planning Team to use workforce data[88] to "*create a pivot table to display the required data*".[89] This regularity increased the likelihood that an unauthorised disclosure would occur.

b) Electronic files often contain data which is 'hidden' (i.e. data which is not immediately visible on screen, but is elsewhere within the file - the most obvious example being an electronic file's metadata). It is particularly easy for spreadsheet files (such as Excel files) to contain hidden data; they are therefore particularly prone to human error. The fact that Excel files can contain worksheets which are not automatically visible as tabs has been noted at footnote 18 (page 12 above). Other examples of how Excel files can contain hidden data include: the fact that it is possible to purposefully hide worksheets, rows and columns; and the fact that the underlying data used to generate a pivot table can be embedded in the pivot table as hidden data.[90] Further examples of how spreadsheet files (and other electronic files) can contain hidden data are set out in the ICO's guidance, *How to disclose information safely – Removing personal data from information requests and datasets.*[91]

[88] Specifically, the data file called "Combined 3C & Perlist", which includes (for all officers and staff who are in post, suspended or on a career break at the time of download) the following categories of personal data: surnames and first name initials, job role, rank/grade, department, location of post, contract type, gender and PSNI service/staff number.
[89] PSNI Fourth enquiries response letter, 13 December 2023.
[90] This underlying data can be accessed simply by double-clicking the pivot table.
[91] How to disclose information safely (ico.org.uk), June 2018 (accessed via search engine 26 September 2024).

c) The Relevant Processing involved the personal data of all (almost 10,000) PSNI officers and staff. This increased the likelihood of risk to rights and freedoms.

d) Responses to FOI requests were usually publicly available (they were often published on the WhatDoTheyKnow website and the PSNI website's FOI disclosure log).[92]

e) The workforce data included information such as the data subject's rank/grade (which would likely be correlated with their age) as well as their gender and their post location. This increased the likelihood of identification (described at paragraph 69 above).

78. The following factors are relevant to the likelihood of the risk to the rights and freedoms of particular groups of PSNI officers and staff from the Relevant Processing:

a) The uniqueness of many Irish surnames (and the possibility of associating some such surnames with a Catholic community background). A data subject with such a surname would be more likely to be identified as described at paragraph 69 above.

b) Similarly, the uniqueness (within Northern Ireland) of surnames of police officers and staff from ethnic minority backgrounds. A data subject with such a surname would be more likely to be identified as described at paragraph 69 above.

[92] For the avoidance of doubt, the Commissioner recognises that the use of online platforms to submit and receive responses to FOI requests can be efficient and help promote transparency and are within the scope of the legislation. The use of online platforms is however a relevant factor in considering the likelihood of risk in this case.

c) As regards officers involved in covert roles:

i. The likelihood of damage flowing from identification by family and friends was higher in the case of officers involved in covert roles, as their occupation was more likely to be concealed in the first place.

ii. The likelihood of physical identification by paramilitary groups including dissident republicans was, on balance, higher in the case of officers involved in covert roles who engaged (in person) with paramilitaries as part of their role. This would be the case if, for instance, an identity in the workforce data could be (directly or indirectly) linked to an image of that individual.

iii. The workforce data would enable paramilitaries to infer that a given data subject was an officer involved in covert roles.[93] Paramilitary groups including dissident republicans would likely concentrate their efforts on physically identifying such data subjects, thereby increasing the likelihood of such identification.

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

Assessment of compliance prior to the 8 August Incident

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

[93] See paragraph 63 above.

81. Paragraphs 32 to 44 above detail the Commissioner's findings of fact in relation to the PSNI's relevant procedures, policies and guidance in place prior to the 8 August Incident.

82. The Commissioner finds that those procedures, policies and guidance did not amount to an appropriate organisational measure. They did not ensure appropriate security of the personal data which was subject to the Relevant Processing, in that they did not appropriately protect the workforce data from unauthorised disclosure as "hidden"[94] data. The PSNI therefore infringed Articles 5(1)(f) and 32(1) UK GDPR.

83. To explain his finding of infringement, the Commissioner considers it useful to indicate ways in which the PSNI's procedures, policies and guidance might have amounted to an appropriate organisational measure:

a) A policy whereby spreadsheet files are disclosed only when the FOI requester expresses a preference for the information to be provided in that format.[95]

b) An FOI handling procedure which includes requirements for –
   i. the FOI Decision Maker to check all FOI response letters and attachments (that are electronic files) for hidden data – such a check being incorporated into the FOI Audit Log;
   ii. the FOI Decision Maker to discuss all FOI response letters with a Team Leader (and to make the Team Leader aware

[94] I.e. data which is not immediately visible on screen, but is elsewhere within an electronic file.
[95] Such a policy would be consistent with the Commissioner's advisory note to all public authorities, issued on 28 September 2023: Information Commissioner's Office - Advisory note to public authorities | ICO.

of any attachments and the format in which any electronic files are to be disclosed); and

iii. the Team Leader to perform a second check for hidden data where information is to be disclosed as a spreadsheet file – such a check being incorporated into the FOI Response Quality Assurance Checklist.

c) The policy at (a) and the procedural requirements at (b) above to be clearly recorded in appropriate documents (here, the FOI Service Instruction, FOI Audit Log and FOI Response Quality Assurance Checklist).

d) CIB staff to be required to confirm to line managers that they have read and understood appropriate guidance on checking electronic files for hidden data (such as the ICO's guidance *How to disclose information safely – Removing personal data from information requests and datasets,* dated 24 May 2018).

e) The provision of appropriate training (at appropriate intervals) to CIB staff which –

i. raises awareness of the policy at (a) and the procedural requirements at (b); and

ii. ensures CIB staff are competent to perform checks for hidden data.

84. The Commissioner notes that there may be other ways in which the PSNI's procedures, policies and guidance prior to the 8 August Incident could have amounted to an appropriate organisational measure. That is, the PSNI could have demonstrated compliance (protected the workforce data from unauthorised disclosure as "hidden" data) in other ways.[96]

[96] The PSNI could also have implemented appropriate technical measures.

85. The PSNI was unable to provide evidence of any assessment of the appropriate level of security in relation to the Relevant Processing.[97] The Commissioner therefore finds that the PSNI also infringed Article 32(2) UK GDPR.

Assessment of compliance following introduction of August/September 2023 organisational measures

86. Paragraphs 45 to 47 above set out the Commissioner's findings of fact in relation to the procedures, policies and guidance introduced by the PSNI in August/September 2023 (following the 8 August Incident).

87. The direction issued by the SIRO on 9 August 2023[98] constituted a policy requiring all FOI responses to be in PDF format (the "**PDF Policy**"). The Interim Guidance issued on 8 September 2023 reinforced the PDF Policy but allowed FOI responses to be in CSV format (as well as PDF).

88. The Commissioner acknowledges that the PDF Policy and Interim Guidance will have improved the security of the personal data which was subject to the Relevant Processing. The Commissioner finds however that they did not amount to an appropriate organisational measure. This is for two reasons:

    a) If a FOI requester expresses a preference under section 11(1) of the Freedom of Information Act 2000 for receiving the information in a particular software format (such as an Excel file), the PSNI is required to give effect to that preference so far as reasonably

[97] PSNI Further enquiries response letter, 22 March 2024, p. 2.
[98] PSNI Email to the ICO responding to an additional query, 25 March 2024.

practicable.[99] The PDF Policy and Interim Guidance did not align with this legal requirement. In order to be appropriate, an organisational measure (implemented to protect personal data which is subject to the Relevant Processing) would need to form part of a single, coherent FOI handling procedure which ensured the PSNI's compliance with the Freedom of Information Act 2000.

b) Putting the above consideration to one side, the Commissioner considers the PDF Policy and Interim Guidance would only have ensured appropriate security of the workforce data if they had been properly integrated into the PSNI's FOI handling procedure. Such integration would have involved (at the very least) references to the PDF Policy and Interim Guidance in the FOI Service Instruction and the FOI Audit Log (the key corporate documents which govern, and which are used as part of, the FOI handling procedure). Neither the FOI Service Instruction nor the FOI Audit Log were updated in this way.[100] The Interim Guidance was a separate document that was not specific to the handling of FOI requests and which was "*interim pending its amalgamation into current service instructions and Information Security standards*".[101]

89. The Commissioner finds, therefore, that despite the introduction of organisational measures in August/September 2023, the PSNI continued to infringe Article 5(1)(f) and Article 32(1) UK GDPR. It had yet to use appropriate organisational measures to protect the workforce data from unauthorised disclosure as hidden data.

[99] *Innes v the Information Commissioner and Buckinghamshire County Council* [2014] EWCA Civ 1086. See the Commissioner's guidance on s.11 FOIA: Means of communicating information (section 11) | ICO, last updated 11 October 2021.
[100] FOI Audit Log v4, November 2023.
[101] Interim security guidance on safe data sharing dated 8 September 2023.

Assessment of compliance as of 14 June 2024

90. On 20 May 2024, the Commissioner informed[102] the PSNI that the Commissioner intended to give an enforcement notice pursuant to section 149 DPA (in addition to a penalty notice).

91. The proposed enforcement notice would have required the PSNI to implement points (a) to (e) at paragraph 83 above (steps which the Commissioner considers would have resulted in the implementation of an appropriate organisational measure).

92. On 14 June 2024, the Commissioner received written representations from the PSNI about his intention to give an enforcement notice. The written representations confirmed that the PSNI had, as of 14 June 2024, taken the steps which the proposed enforcement notice would have required (the steps at paragraph 83 above). The written representations attached copies of updated versions of the FOI Service Instruction, FOI Audit Log and FOI Response Quality Assurance Checklist. A copy of the PSNI's "*Policy on the Safe and Secure Use of Spreadsheets for Data Sharing*" was also provided.

93. Having considered the written representations and accompanying documents, the Commissioner finds that by 14 June 2024, the PSNI had implemented appropriate measures to ensure appropriate security of the workforce data which was subject to the Relevant Processing, in so far as the workforce data was protected from unauthorised disclosure as "hidden"[103] data. The ongoing infringements of Articles 5(1)(f) and 32 UK GDPR were therefore remedied by that date.[104]

[102] By way of a "preliminary" enforcement notice.
[103] I.e. data which is not immediately visible on screen, but is elsewhere within an electronic file.
[104] As a result, there are no longer grounds to give the proposed enforcement notice.

V. DECISION TO IMPOSE A PENALTY

94. For the reasons set out below, the Commissioner has decided to impose a penalty on the PSNI in respect of the infringements of Articles 5(1)(f), 32(1) and 32(2) UK GDPR during the period 25 May 2018 to 14 June 2024.

A. Legal framework – penalties

95. When deciding whether to give 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 relevant.

96. Article 83(1) UK GDPR requires the Commissioner to ensure that the imposition of a penalty is effective, proportionate, and dissuasive in each individual case.

97. Article 83(2) UK GDPR requires the Commissioner to give due regard 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 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

98. Paragraphs 101 to 164 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**"):[105]

    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)).

99. The Commissioner has not conducted a separate assessment for each infringement. As explained further below, the Commissioner considers the three infringements are of the same nature.[106] An assessment of whether it is appropriate to impose a penalty has been taken in relation to the three infringements collectively.

100. The Commissioner's decision is to impose a penalty.

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

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

Nature of the infringements

[105] Data Protection Fining Guidance | ICO, 18 March 2024.
[106] See footnote 145.

102. 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,[107] increasing its seriousness.

Gravity of the infringements

103. 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.[108]

104. In the absence of appropriate security measures, the nature of the Relevant Processing was likely to result in high risk to data subjects for the reasons set out at paragraphs 68 to 79 above. The data subjects were at greater risk because of their occupation as PSNI officers/staff (especially officers involved in covert roles).

105. As regards the scope of the Relevant Processing, the Commissioner notes that its territorial scope extended to officers and staff from across the whole of Northern Ireland.

106. The purpose of the Relevant Processing was to respond to FOI requests. The Commissioner considers this to be a regular activity of the PSNI (and of all public authorities). Organisations are expected to ensure compliance in respect of all their processing, but particularly so in respect of processing which forms part of a regular activity. If an organisation cannot ensure compliance in respect of regular activities, this diminishes

[107] £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)(a) UK GDPR).
[108] Article 83(2)(a) UK GDPR.

confidence in the organisation's compliance overall. The purpose of the Relevant Processing therefore increases the gravity of the infringements.

107. The Relevant Processing, and therefore the infringements, affected all PSNI officers and staff. In the context of the 8 August Incident, this amounted to 9,483 affected data subjects. When considered in light of the level of damage suffered, this factor increases the gravity of the infringements. Further consideration of the number of data subjects who suffered damage as a result of the 8 August Incident is set out at paragraph 112 below.

108. In relation to the level of damage suffered by affected data subjects, the Fining Guidance makes clear that the Commissioner will have regard to both potential and actual damage.

109. The infringements involved a failure to protect the workforce data from unauthorised disclosure as "hidden" data. The types of damage which data subjects could have potentially suffered as a result of unauthorised disclosure have been set out at paragraphs 72 and 73 above. They include the gravest type of damage: severe physical injury and even death. This increases the gravity of the infringements.

110. The Commissioner is of the view that, on the balance of probabilities, the 8 August Incident occurred as a consequence of the infringements set out in this Penalty Notice. In assessing the level of damage suffered as a result of the infringements, the Commissioner has therefore had regard to the damage suffered by data subjects as a result of the 8 August Incident. As stated in the Fining Guidance, however, "*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."

111. Complaints lodged by data subjects under Article 77 UK GDPR have assisted the Commissioner's assessment of the level of actual damage suffered. Five bulk complaints[109] from staff associations and networks were lodged with the Commissioner, as well as six individual complaints. The five bulk complaints were lodged by the Police Federation for Northern Ireland, the Superintendents' Association, the Catholic Police Guild, the Ethnic Minority Police Association and the Christian Police Association.

112. The Commissioner notes that not all affected data subjects will have suffered damage and that of those who did, the types and level of damage are highly specific to individual circumstances. In considering the number of data subjects who suffered damage as a result of the 8 August Incident, the Commissioner has had regard to the high volume of referrals made to the PSNI's Emergency Threat Management Group (such that the PSNI had to prioritise them by implementing a RAG rating system). Of the referrals received as of 22 September 2023, 879 had been categorised as red, 1,616 had been categorised as amber and 1,543 had been categorised as green.[110] As of 18 October 2023, a total of 4,024[111] referrals had been made. The Commissioner also

[109] On 18 September 2023 the PSNI and the ICO issued a joint statement to all PSNI officers and staff. The statement informed officers and staff that the ICO was engaging with staff associations and networks regarding complaints and that individuals did not need to lodge complaints separately (Joint comms email sent to PSNI staff, 18 September 2023). The ICO met with representatives of the associations and networks on 18 October 2023 and it was agreed that the associations and networks would gather information from their members and provide this to the ICO in the form of bulk complaints.
[110] PSNI Second enquiries response letter, 22 September 2023, p. 13.
[111] Though the PSNI had identified over 800 of these to be duplicate referrals. (Internal meeting notes from PSNI visit on 18 October 2023, p. 2).

understands that more than 6,000 claims have been brought against the PSNI for damages in connection with the 8 August Incident.[112]

113. Two types of (non-material) damage appear to the Commissioner to be common among many affected data subjects (albeit at varying levels of severity):
    a) psychological harm (fear and anxiety about personal safety and the safety of family and friends); and
    b) loss of control of personal data (diminished ability to control knowledge of occupation).

114. The Commissioner has not seen evidence of data subjects suffering physical injury from dissident republicans as a result of the 8 August Incident.

115. Below, the Commissioner sets out some examples from the lodged complaints which he has had regard to in assessing the level of damage suffered.[113] The Commissioner is aware that these examples are likely to represent the most severe levels of damage suffered. This is, however, precisely why the Commissioner considers these examples to be instructive in evaluating the gravity of the infringements.

Examples of damage suffered from the lodged complaints

"How has this impacted on me? I don't sleep at night. I continually get up through the night when I hear a noise outside to check that

[112] High Court order will deliver 'swift management' of compensation claims by those affected by PSNI data breach – The Irish News, 24 March 2024 (accessed 26 September 2024).
[113] Naturally, these examples reflect the damage suffered from 8 August 2023 up to the time at which the complaints were lodged. The last complaint was lodged in February 2024.

everything is ok. I have spent over £1000 installing modern CCTV and lighting around my home, because of the exposure."

"I am a Catholic police officer … My name as a police officer, which I tried so hard to conceal from family, acquaintances and wider society is now available to anyone. … I worry most days that at any minute, we don't know who is sitting scrutinising that list and trying to investigate and piece together the intel they may already have amassed and make it into something actionable to harm us with the data they have now been furnished with..."

"As a result of the spreadsheet data being released to the public… I have increased security at my home but also at my parents' home. I am struggling to sleep and find myself awake at night checking cameras. I have not visited my family home since the spreadsheet data was released as I believe it would put them in further danger. Furthermore, my parents do not want to visit my home for fear that someone would follow them to my address."

"… we have recently had to reconsider all our activities particularly as a result of the recent data breach with my name being in the public domain and the fact that it lists me as working in [PSNI department]*. … Following the data breach my wife … has become extremely concerned as to our own and our children's personal security, we have no security measures in our home and financially we have no surplus money to install these."*

"I have gone to great trouble to ensure that I have remained invisible, with no social media presence, removal from the electoral roll, 192.com, never revealing my job to others and lying about where I work whenever asked. … I have trouble sleeping, my children … are all stressed about my welfare, some of them have told me that they have nightmares about me getting attacked."

"I believe the risk to my personal security and the safety of my wife and …young children is more significant for me due to the fact that I grew up in the area where we are most active. As a result of this many persons involved and linked to paramilitary groups and wider criminal circles in this area would know me or remember me from both school and childhood. I have gone to great lengths to keep my occupation confidential. Only close family and friends previously had knowledge of it. I have a minimal social media footprint. I have also spent a considerable amount of effort to make our home private and secure to reduce potential for attacks. This has now been severely compromised and will require further expense to upgrade."

"Everything has culminated and become too much for me to the point that I have accepted another job outside of the police. I am essentially taking a pay cut … not to mention leaving the job that I dreamed of since I was a small child and geared my whole life towards. To say I am devastated is an understatement but I feel I have no choice."

"I have quite a unique surname which had been shared in the data breach, I feel that this not only puts my name in the hands of individuals who may seek to do harm but also affects my own personal family as well and my wider family… The PSNI recently had a senior Officer shot multiple times so the threat does feel very real, in that there are elements that seek to cause this harm to Police Officers on a daily basis. This data breach will have aided them in doing so."

"The breach is having an impact on my personal life as my family are now very anxious and concerned for their and my welfare. I don't sleep well maybe a couple of hours a night, I formulate plans in my head if I get attacked at home, away from home, in my car, and it's a lonely experience."

116. The above statements and those contained in the many other lodged complaints indicate the significant level of actual damage suffered, and therefore the gravity of the infringements. The Commissioner gives very significant weight to this factor in his assessment of the gravity of the infringements.

117. To summarise the Commissioner's assessment of the gravity of the infringements: 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

118. The duration of the infringements is from 25 May 2018 (the date of commencement of the DPA and application of the GDPR[114]) until 14 June 2024 (when the infringements were remedied[115]).

119. 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 of damage materialised on 8 August 2023.

120. The duration of the infringements increases their seriousness.

Conclusion on the nature, gravity and duration of the infringements

[114] That is, the PSNI infringed Articles 5(1)(f), 32(1) and 32(2) UK GDPR ever since its obligations under those provisions arose in respect of the Relevant Processing.
[115] See paragraphs 90 to 93 above.

121. 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

122. The Commissioner does not consider that the PSNI acted intentionally in committing the infringements. The Commissioner does, however, find that the infringements were clearly negligent in character.

123. The PSNI ought to have known the nature and severity of the risk described at paragraphs 69 to 73 above.

124. The PSNI ought to have known the likelihood of risk (the factors set out at paragraphs 77 and 78 above).

125. In particular, the PSNI ought to have known that spreadsheet files are prone to hidden data (and therefore human error) for the following reasons:

    a) The Commissioner's FOI guidance raises awareness of this issue:

i. Under the heading "*Is there anything else we should consider before sending the information?*", first published on the ICO website in July 2013:[116]

> Is there anything else we should consider before sending the information?
>
> You should double check that you have included the correct documents, and that the information you are releasing does not contain unnoticed personal data or other sensitive details which you did not intend to disclose.
>
> This might be a particular issue if you are releasing an electronic document. Electronic documents often contain extra hidden information or 'metadata' in addition to the visible text of the document. For example, metadata might include the name of the author, or details of earlier draft versions. In particular, a spreadsheet displaying information as a table will often also contain the original detailed source data, even if this is not immediately visible at first glance.
>
> You should ensure that staff responsible for answering requests understand how to use common software formats, and how to strip out any sensitive metadata or source data (eg data hidden behind pivot tables in spreadsheets).
>
> See the National Archives Redaction Toolkit for further information, or read our more detailed guidance:
>
> ← Previous Next →

ii. In the Commissioner's more detailed FOI guidance on "*Means of communication information (section 11)*", first published on 11 October 2021:[117]

> When providing information in a re-usable format, you should take steps to ensure that any exempt information in the underlying data is redacted to avoid inadvertent disclosure. For example, you should ensure that any personal data is redacted so it is not unintentionally disclosed. The risk of this happening occurs with spreadsheets in particular. Therefore, you should ensure that requested information is prepared safely for release. For example, when data is presented in the form of a 'pivot' table, the source data is retained. If possible, you should consider disclosing the information in a CSV file format instead.

b) In June 2018, the ICO published the guidance "*How to disclose information safely – removing personal data from information*

[116] Finding and preparing the information | ICO.
[117] Means of communicating information (section 11) | ICO.

requests and datasets" on its website.[118] This guidance discusses in detail the various ways in which electronic files can contain hidden data and how to check for such hidden data. In relation to spreadsheet files, for instance, the guidance suggests exporting data to a text file such as CSV,[119] and using (in the case of Excel) the "Document Inspector" tool.[120] A checklist is provided at the end, with questions such as "*Are you sure you know where all the data is? … Are there hidden work sheets?*[121] *… Is the file size larger than you might expect for the volume of data being disclosed?*"

c) Other relevant guidance available prior to and since the 8 August Incident includes:

i. Guidance from the National Archives (last updated April 2016) "*Redaction Toolkit: Editing exempt information from paper and electronic documents prior to release*",[122] which is aimed at "*all authorities subject to the Freedom of Information Act (FOIA), Data Protection (DP) legislation and Environmental Information Regulations (EIRs), from central Government departments to local, police, health and education authorities.*"

[118] How to disclose information safely (ico.org.uk), June 2018 (accessed via search engine 26 September 2024). Between June 2018 and August 2022, a link to this guidance was contained in the full index of freedom of information and environmental information guidance on the ICO website. After August 2022, the link to this guidance was removed from the full index. The guidance nevertheless remained on the ICO website and could be found through search engines.
[119] On attempting to export data to a text file, a dialog box opens reminding the user that only the current worksheet will be saved to the new file.
[120] Though use of this tool would not alert a user to the presence of worksheets which are not visible as tabs.
[121] As noted at paragraph 21(g), in the case of the 8 August Incident, the worksheet containing the personal data was not hidden, it was simply not visible as a tab.
[122] redaction_toolkit.pdf (nationalarchives.gov.uk), April 2016 (accessed 26 September 2024).

ii. The UK Government's guidance "*Creating and sharing spreadsheets*" (first published June 2021).[123]

iii. The National Police Chiefs' Council ("**NPCC**") "*Manual of Guidance for the FOIA*"[124] (v.8.0, dated January 2021) also contained guidance stating, "*If forces choose to provide the information in a re-usable format (pivot tables) they must ensure that any "hidden" information is redacted so as not to disclose data unintentionally.*"[125]

iv. Advice (sent directly to all police forces) from the NPCC's National Police Freedom of Information and Data Protection Unit in June 2023. This advice referred specifically to the risk of "hidden" data in Excel files. The advice included a link to the ICO's May 2018 guidance, and even highlighted how there can be more worksheets than there are visible tabs.[126]

---

[123] Creating and sharing spreadsheets - GOV.UK (www.gov.uk), June 2021 (accessed 26 September 2024).

[124] Microsoft Word - NPCC Manual Of Guidance 2021 v8.0 (cityoflondon.police.uk), January 2021 (accessed 26 September 2024).

[125] The PSNI stated that this Manual is "supplied to all staff" (PSNI Initial enquiries response letter, 29 August 2023). For the avoidance of doubt, the Commissioner does not consider the supplying of this document to have been (either on its own or in conjunction with the procedures, policies and guidance set out at paragraphs 32 to 47 above) an appropriate security measure. Whilst the Manual raises the issue of "hidden" data, it provides very limited guidance on it. The PSNI has also been unable to point to any requirement for CIB staff to confirm that they had read and understood the Manual.

[126] PSNI internal emails re NPCC FOI advice, 21 June 2023. When asked to explain how the PSNI acted on this piece of advice, the PSNI stated that the advice was circulated to FOI Decision Makers and line managers within CIB by email (PSNI Further enquiries response letter, 22 March 2024, p. 4). The Commissioner does not consider this action (either on its own or in conjunction with the procedures, policies and guidance set out at paragraphs 32 to 47 above) amounted to an appropriate security measure. Notably, the PSNI has been unable to point to any requirement for CIB staff to confirm that they had read and understood the advice. The email received from the NPCC was simply forwarded to CIB staff without any further instruction from the PSNI. The PSNI has also been unable to demonstrate that the advice was properly integrated into the FOI handling procedure. Indeed, was accepted by the current Chief Constable in oral evidence to the Northern Ireland Affairs Committee on 13 December 2023: "*We had had a number of warnings with*

d) The ICO has fined data controllers (under the Data Protection Act 1998) for failing to take appropriate measures against unauthorised processing of personal data (in contravention of the seventh data principle)[127] when using spreadsheet files to share information externally:
   i. In April 2018, the Royal Borough of Kensington and Chelsea, £120,000.[128]
   ii. In April 2016, Blackpool Teaching Hospitals NHS Foundation Trust, £185,000.[129]
   iii. In August 2013, Islington Borough Council, £70,000.[130]

---

regards to the use of PDFs. I think the report references the National Police Chiefs' Council in January and June of last year sending out notifications about best practice. Some of it was adopted in the PSNI and some of it was not. There was no standard operating procedure to bring that all of that together."

[127] The seventh data protection principle read as follows: *"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."*

[128] The contravention was as follows: (a) The Council did not provide the FOI team with any (or any adequate) training on the functionality of Excel spreadsheets or possible alternatives; (b) The Council had in place no guidance for the FOI team to check spreadsheets for data hidden in any pivot table before they are disclosed under FOI.

[129] The contravention was as follows: (a) The Trust had in place no procedure governing requests for information from ESR [the electronic staff records system] to control its use and further dissemination; (b) The Trust did not provide the team with any (or any adequate) training on the functionality of Excel spreadsheets or possible alternatives; (c) The Trust had in place no guidance for the web services team to check the spreadsheets for hidden data before they were uploaded to its website.

[130] The contravention was as follows: a) Whilst the data controller had dedicated IGOs [Information Governance Officers] in post, there was no formal or consistent process in place for checking an FOI response; b) There were no specific checking procedures built into that process to check whether personal or sensitive personal data was present ahead of providing a response to an FOI request; c) There were no sufficient procedures in place to train staff to carry out such checks and as such the data controller failed to equip its staff with the appropriate knowledge and skills. … i) An effective training programme for staff had not been implemented. The person responsible for disclosing the information had not been trained properly to enable them to identify sensitive personal data contained in the pivot tables nor had they received any specific data protection training. They were therefore unable to

These cases further raised awareness of how spreadsheet files are prone to containing hidden data.

126. Having regard to paragraph 83 above, the Commissioner considers an appropriate organisational measure would have been straightforward and uncostly to implement.

127. The fact that the PSNI ought to have known the likelihood, nature and severity of the risk, coupled with the ease with which an appropriate security measure could have been implemented, renders the PSNI's infringements of Articles 5(1)(f) and 32(1) UK GDPR negligent. It was also negligent not to carry out a data security risk assessment as required by Article 32(2) UK GDPR.

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

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

129. The Commissioner does not consider the workforce data[131] which was subject to the Relevant Processing to be special category data.

mitigate against the risk of an unlawful disclosure. ii) Whilst the data controller had some standard procedures in place for dealing with FOI requests, the data controller did not have appropriate technical or organisational measures in place to firstly screen and check whether personal data was present in information being prepared for disclosure and secondly to check it, prior to it being disclosed in response to an FOI request. iii) There is no documented procedure that specified that a request must be checked by a peer.

[131] Specifically, the data file called "Combined 3C & Perlist", which includes (for all officers and staff who are in post, suspended or on a career break at the time of download) the following categories of personal data: surnames and first name initials, job role, rank/grade, department, location of post, contract type, gender and PSNI service/staff number.

130. The Commissioner notes, however, paragraph 72 of the Fining Guidance: *"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…".*

131. For the reasons set out at Section IV(B) (Nature of the personal data and context of the Relevant Processing), the workforce data was sensitive. Where that data related to officers involved in covert roles, it was particularly sensitive. Disclosure of the workforce data was likely to cause damage to data subjects. This further increases the seriousness of the infringements.

Conclusion on seriousness of infringements

132. Having considered the nature, gravity and duration of the infringements, as well as their clearly negligent character and the categories of personal data affected, the Commissioner categorises the infringements as having a high degree of seriousness.

133. In the absence of any aggravating or mitigating factors, the infringements would warrant the imposition of a 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

134. In assessing this factor, the Commissioner has considered the actions taken by the PSNI to mitigate both actual and potential damage suffered as a result of the 8 August Incident. The Commissioner has considered the relatively prompt removal of the disclosed data from the WhatDoTheyKnow website, the PSNI's criminal investigation, the steps taken to reduce the identifiability of PSNI officers and staff and the support the PSNI offered them.

135. Naturally, the most effective mitigating action which the PSNI could have taken was to seek the removal of the disclosed data from the WhatDoTheyKnow website promptly. The Commissioner notes that the PSNI requested removal of the disclosed data from the WhatDoTheyKnow website 37 minutes after becoming aware of the breach.[132] The Commissioner considers this to be a relatively prompt response.

136. The Commissioner notes the criminal investigation launched by the PSNI on 9 August 2023 to investigate possible offences under the Terrorism Act 2000[133]. Using IP addresses, the PSNI sought to identify all individuals who had accessed the disclosed data on the WhatDoTheyKnow website.[134] As of 18 October 2023, the investigation had led to six arrests: one individual was charged, and five individuals were bailed. As of 18 October 2023, the investigation had also been

[132] PSNI Initial enquiries response letter, 29 August 2023, p. 2.
[133] The disclosed data was considered to be information of a kind likely to be useful to a person committing or preparing an act of terrorism.
[134] PSNI officers and staff who were identified as having accessed the disclosed data were instructed to delete it.

monitoring the dark web for the disclosed data.[135] Public statements made by the PSNI in connection with the arrests have reiterated that the PSNI "*… continue to work toward establishing those who possess information relating to the data breach on August 8th, and will take action to ensure that any criminality identified is dealt with robustly to keep communities, and our officers and staff who serve them, safe*."[136]

137. In a briefing to the Commissioner on 18 October 2023, the PSNI suggested the criminal investigation, the arrests and public statements are all likely to have made possession of the disclosed data undesirable.[137] The Commissioner agrees this is likely to be true for ordinary members of society, and that this goes some way to reducing the risk of data subjects' occupations becoming known to their family and friends.

138. The Commissioner thinks it unlikely, however, that dissident republicans would be much deterred by the PSNI's actions. Indeed, as early as 10 August 2023, the then Chief Constable stated, "*We have since become aware of dissident republican claims that they are in possession of data circulating on WhatsApp."*[138] On 14 August 2023, the then Chief Constable stated, "*We are now confident that the workforce data set is in the hands of Dissident Republicans".*[139]

139. Paragraph 26 of this Penalty Notice sets out the steps taken by the PSNI with the aim of reducing the identifiability of PSNI officers and staff.

[135] PSNI Op Sanukite Update, 18 October 2023 and Internal meeting notes from PSNI visit on 18 October 2023, p. 2.
[136] Detectives investigating criminality linked to freedom of information data breach make arrest | PSNI, 19 October 2023 (accessed 26 September 2024).
[137] Internal meeting notes from PSNI visit on 18 October 2023.
[138] Statement from the Chief Constable on the data breach investigation | PSNI, 10 August 2023 (accessed 26 September 2024).
[139] Update from the Chief Constable on the data breach investigation | PSNI, 14 August 2023 (accessed 26 September 2024).

Those steps involved changing officer and staff identification numbers and reducing their use.

140. The Commissioner is not in a position to assess the effect of these steps on the risks identified at paragraph 69 above (namely, the risk of data subjects being identified as PSNI officers/staff by family and friends, as well as the risk of physical identification by dissident republicans).[140]

141. Paragraph 27 of this Penalty Notice sets out the main steps taken by the PSNI to support officers and staff following the 8 August Incident.

142. The Commissioner does not consider these actions (the removal of the disclosed data from the WhatDoTheyKnow website, the criminal investigation, the steps to reduce the identifiability of officers and staff and the support offered to them), taken collectively, amount to a mitigating factor in his decision on whether to impose a penalty. These actions were all entirely in line with what would reasonably be expected of a police force responding to a personal data breach of this scale and severity.

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

143. A failure to implement appropriate technical or organisational measures is inherent to infringements of Articles 5(1)(f) and 32(1) UK GDPR. The PSNI's responsibility for these infringements is therefore also inherent.

144. The PSNI was the sole controller in respect of the Relevant Processing. The PSNI therefore bears full responsibility for the infringements.

[140]The notice of intent given to the PSNI on 20 May 2024 invited representations in this regard, but none were received.

145. The Commissioner considers that any public authority responding to FOI requests, regardless of size and financial position (i.e. the resources available to it), could be reasonably expected to implement an appropriate security measure which incorporates elements analogous to those set out at paragraph 83 above - even where the nature of the processing is low-risk.

146. The PSNI covers the second largest demographic in the UK and in the financial year 2022-2023, received approximately £840 million in funding from the Northern Ireland Assembly.[141] The Relevant Processing was high risk (see paragraphs 68 to 79 above). It follows even more that the PSNI could have been reasonably expected to have implemented an appropriate security measure.

147. The PSNI's degree of responsibility is therefore an aggravating factor in the Commissioner's decision to impose a penalty.

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

148. 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

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

[141] Police Service of Northern Ireland - Annual Report and Accounts for the year ended 31 March 2023 (psni.police.uk), p. 106, 7 July 2023 (accessed 26 September 2024).

example by responding to requests for information and attending meetings. The Commissioner considers that the ordinary duty of cooperation is required by law (Article 31 UK GDPR) and meeting this standard is therefore not a mitigating factor.

150. The PSNI has responded to requests for information during the Commissioner's investigation in a way that has enabled the enforcement process to be concluded significantly more quickly and effectively. In doing so, the Commissioner's view is that the PSNI has demonstrated good cooperation. This would, however, be reasonably expected of any public authority. The Commissioner therefore 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

151. The infringements became known to the Commissioner as a result of his investigation. That investigation was prompted by the 8 August Incident.

152. Although the Commissioner was notified by the PSNI of the 8 August Incident, that notification, however prompt, was a legal requirement (Article 33 UK GDPR).

153. The Commissioner therefore considers this factor to be neutral.

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

154. There are no measures referred to in Article 58(2) UK GDPR which have previously been ordered against the PSNI 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

155. There are no relevant codes of conduct or approved certification mechanisms. 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

156. There are no other aggravating or mitigating factors applicable to the circumstances of the case. This factor is therefore not relevant to the Commissioner's decision.

Conclusion on relevant aggravating and mitigating factors

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

158. 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.

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

Effectiveness, proportionality and dissuasiveness

160. The Commissioner considers 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. The PSNI will continue to have to process personal data when responding to FOI requests, so there is a need to deter the PSNI from infringing the security provisions of the UK GDPR again. There is also a need to deter other public authorities subject to the Freedom of Information Act 2000 from committing such infringements.

161. Taking into account the high degree of seriousness of the infringements (notably the damage suffered by data subjects) and the PSNI's size and financial position, the Commissioner considers that the imposition of a penalty would be proportionate – 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.

C. Conclusion on decision on whether to impose a penalty

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

163. In June 2022, the Commissioner set out a revised approach to public sector enforcement to be trialled over two years.[142] To support this approach, the Commissioner committed to working proactively with

[142] Open letter from UK Information Commissioner John Edwards to public authorities, 30 June 2022. The revised approach (which was trialled for a two-year period ending in June 2024) is currently under review. The revised approach continues to be applied pending the outcome of that review: ICO statement on its public sector approach trial | ICO.

senior leaders in the public sector to encourage compliance, prevent harms before they occur, and learn lessons when things have gone wrong. In practice, this means that for the public sector the Commissioner has committed to increasing the use of public reprimands and enforcement notices, only issuing fines in the most egregious cases.[143]

164. The Commissioner has had regard to the revised public sector approach in reaching his decision to impose a penalty in this case. The Commissioner is satisfied that this case is sufficiently egregious to warrant the imposition of a penalty.

VI. CALCULATION OF PENALTY

165. The Fining Guidance sets out a five-step approach which the Commissioner has applied to calculate the amount of the penalty:

Step 1: Assessment of the seriousness of the infringement.
Step 2: Accounting for turnover.
Step 3: Calculation of the starting point.
Step 4: Adjustment to take into account any aggravating or mitigating factors.
Step 5: Assessment of whether the fine is effective, proportionate and dissuasive.

Following the application of this five-step approach, the Commissioner has gone on to consider the amount of the penalty in light of his revised approach to public sector enforcement.

Statutory maximum penalty

[143] See ICO25 – Our Regulatory Approach, 7 November 2022, p. 7.

166. 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 PSNI's three infringements (of Articles 5(1)(f), 32(1) and 32(2) UK GDPR) were all for the same processing operations (the Relevant Processing). The gravest infringement was that of Article 5(1)(f) UK GDPR.

167. The infringement of Article 5(1)(f) UK GDPR, which is a basic principle for processing, is subject to the statutory maximum of £17.5 million (Article 83(5)(a) UK GDPR).[144] Had the Commissioner imposed a separate penalty for each of the three infringements, the total of those three penalties could not have exceeded £17.5 million.

168. In this case, however, the Commissioner has calculated a single penalty for all three infringements. This is because the three provisions infringed are all of the same nature: they all seek to ensure the security of personal data processing.[145] 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

[144] The turnover-based higher maximum applies only to undertakings with a total worldwide annual turnover exceeding £437.5 million. The PSNI is not an undertaking.

[145] For the avoidance of doubt, the Commissioner considers Articles 5(1)(f) and 32 UK GDPR to be evidently distinct provisions of the UK GDPR (notwithstanding the degree of overlap). 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). In this Penalty Notice, however, the Commissioner has simply calculated a single penalty.

169. 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.

170. In this Penalty Notice (paragraph 132 above), the Commissioner has categorised the infringements as having a high degree of seriousness. This means that the starting point will be between 20% and 100% of the relevant legal maximum (£17.5 million).

171. The Commissioner decides that the infringements warrant a starting point of 80%.

172. A starting point lower than 80% is not warranted for the reasons set out at paragraphs 101 to 132 above. The Commissioner does not repeat those reasons here.

173. A starting point higher than 80% is not warranted for the following reasons:

a) the purpose of the Relevant Processing was to comply with statutory obligations;
b) the Relevant Processing was not extensive;
c) the infringements were not intentional.

B. Step 2: Accounting for turnover

174. Having assessed the seriousness of the infringements, the Commissioner next determines any adjustment to reflect the size of the recipient of the

penalty.[146] This is consistent with the need to ensure the amount of the penalty is effective, proportionate and dissuasive.

175. Where the recipient is an undertaking, the Commissioner will determine the adjustment by reference to the undertaking's turnover. As explained at paragraph 119 of the Fining Guidance, where a recipient is not an undertaking and therefore does not have turnover (as is the case with the PSNI), the Commissioner may instead have regard to other indicators of the recipient's financial position, such as assets, funding or administrative budget.

176. Where a recipient is a public body, the Commissioner's usual practice is to have regard to the recipient's administrative budget or expenditure. The benefit of this approach is twofold: firstly, it acts as an easily understood and standardised comparator; secondly, whilst still correlated with the scale of the public body, it excludes core activities and thus limits any adverse impact on public services.

177. As a measure of administrative expenditure, the Commissioner has used the PSNI's figure for actual expenditure on administrative and industrial staff pay in the financial year 2023/24.[147] This figure was £117 million.[148]

178. As set out in the Fining Guidance, in the case of an undertaking with an annual turnover of between £100 million and £250 million, the Commissioner may apply an adjustment factor of 20% to 50% to the

[146] As set out at paragraph 128 of the Fining Guidance, any such adjustment is discretionary.
[147] Figure obtained from PSNI Finance Report provided to the Commissioner on 11 April 2024. As the financial year 2023/24 had only just ended, the PSNI was only able to provide provisional figures. The PSNI's final audited accounts for the year 2023/24 were laid before the Northern Ireland Assembly on 4 July 2024: Police Service of Northern Ireland - Annual Report and Accounts for the year ended 31st March 2024 (psni.police.uk) (accessed 26 September 2024).
[148] Rounded down from £117,653,000.

starting point. The Commissioner considers this range of adjustment is also appropriate in this case.

179. As he has only taken into account the PSNI's administrative expenditure, the Commissioner considers a figure at the higher end of this range of adjustment is appropriate: the Commissioner decides that an adjustment of 40% is appropriate to reflect the PSNI's size.

C. Step 3: Calculation of the starting point

180. The starting point of the penalty is calculated as follows:
Fixed statutory maximum amount (£17.5 million) x adjustment for seriousness (80%) x turnover adjustment (40%) = £5,600,000 (£5.6 million)

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

181. 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 £5.6 million).

182. One aggravating factor influenced the Commissioner's decision to impose a penalty: the PSNI's degree of responsibility (see paragraphs 143 to 147 above). On this occasion, the Commissioner considers the starting point adequately reflects the PSNI's degree of responsibility and so an adjustment for this aggravating factor is not required. There is therefore no adjustment at Step 4.

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

183. As set out at paragraph 142 of the Fining Guidance, "*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.*"

184. The Commissioner considers that a penalty of £5.6 million will be both effective and dissuasive. A penalty of this amount will have a genuine deterrent effect, taking into account both the specific deterrence to the PSNI and the general deterrence to other organisations.

185. The penalty is specific to the egregious nature of the infringements and reflects the PSNI's economic situation. By adequately reflecting the fact that the PSNI is a public body, the turnover adjustment applied (40%) has ensured that the penalty is proportionate and appropriate to the size and financial position of the PSNI. The penalty is not more than is appropriate or necessary in the circumstances.

F. The Commissioner's revised approach to public sector enforcement

186. As explained at paragraph 163, in June 2022 the Commissioner set out a revised approach to public sector enforcement.[149] Having considered that revised approach, the Commissioner considers that it is appropriate to reduce the amount of the penalty from £5.6 million to **£750,000**.

[149] Open letter from UK Information Commissioner John Edwards to public authorities, 30 June 2022. The revised approach (which was trialled for a two-year period ending in June 2024) is currently under review. The revised approach continues to be applied pending the outcome of that review: ICO statement on its public sector approach trial | ICO.

G. Conclusion - penalty

187. For the reasons set out above, the Commissioner decides to impose a penalty on the PSNI of £750,000.

H. Financial hardship

188. Paragraph 151 of the Fining Guidance explains that "*In exceptional circumstances, the Commissioner may reduce a fine where an organisation or individual is unable to pay because of their financial position.*"

189. The notice of intent (given to the PSNI on 20 May 2024) indicated that the amount of the penalty the Commissioner proposed to impose was £750,000. The PSNI made a claim of financial hardship in written representations dated 14 June 2024.

190. As explained at paragraph 152 of the Fining Guidance, "*The Commissioner will only grant a reduction for financial hardship on the basis of objective evidence that imposing the proposed fine would irretrievably jeopardise an organisation's economic viability… The Commissioner will not base any reduction on the mere finding of an adverse … financial situation.*"

191. Whilst the Commissioner acknowledges the financial challenges faced by the PSNI, the Commissioner is not convinced, on the basis of the evidence put forward in the written representations, that the PSNI's economic viability would be irretrievably jeopardised as a result of a penalty of £750,000.

192. Whilst the PSNI's representations do not justify a reduction for financial hardship, the Commissioner has considered those representations in relation to the proportionality of the penalty amount as follows:

a) The PSNI's final audited position for the year 2023/24 involves a small resource underspend. This position assumes a penalty of £610,000.[150] The PSNI initially submitted that a penalty of £750,000 would result in the PSNI reporting a 2023/24 resource overspend, "*pushing PSNI into breaching spending limits*" and that this would "*initiate a whole range of other unintended consequences related to financial management, financial reporting and Assembly accountability*."[151] When probed by the Commissioner, however, the PSNI stated that "*If the fine imposed is £750k, the £140k difference between the* [£610,000] *accrual and the fine would be chargeable to the 2024-25 budget."*[152] The financial position for the year 2023/24 would therefore remain unchanged.

b) The PSNI submitted that a penalty of £750,000 would frustrate efforts to allocate additional resources to the improvement of information management within the force. The representations did not include specific proposals as to how funds arising from a penalty reduction would be allocated. In applying the revised approach to public sector enforcement to reduce the penalty amount, the Commissioner has already taken impacts of this nature into account. In any event, the Commissioner must ensure that a penalty is not only proportionate but also a deterrent and an effective sanction for the infringements.

193. The Commissioner has therefore not reduced the penalty amount from £750,000 (the amount indicated in the notice of intent).

[150] PSNI letter to Commissioner, 12 July 2024, p. 1.
[151] PSNI written representations, 14 June 2024, p. 3-4.
[152] PSNI letter to Commissioner, 12 July 2024, p. 2.

VII. PAYMENT OF THE PENALTY

194. The penalty must be paid to the Commissioner's office by BACS transfer or cheque by 25 October 2024.

195. Under paragraph 9(4) of Schedule 16 to the DPA, in Northern Ireland, a penalty is recoverable—
   a) if a county court so orders, as if it were payable under an order of that court;
   b) if the High Court so orders, as if it were payable under an order of that court.

196. Under paragraph 9(1) of Schedule 16 to the DPA, the Commissioner must not take action to recover a penalty unless—
   a) the period for payment specified in this Penalty Notice (by 25 October 2024) has ended,
   b) any appeals against this Penalty Notice have been decided or otherwise ended,
   c) if this Penalty Notice is varied, any appeals against the penalty variation notice have been decided or otherwise ended, and
   d) the period for the PSNI to appeal against the penalty, and any variation of it, has ended.

VIII. RIGHTS OF APPEAL

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

198. 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: 26 September 2024

Stephen Bonner
Deputy Commissioner, Regulatory Supervision
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF