Post-implementation review: Public sector approach trial

September 2024

Information Commissioner's Office

Contents

Executive summary

Purpose of the review and approach

The ICO announced a two-year trial of a revised approach to working with and regulating public organisations in June 2022, which in this report we call the 'Public Sector Approach' (PSA). Its objective was to work more effectively with these organisations to raise data protection standards and ultimately lead to better outcomes for UK citizens. The PSA saw the use of the Commissioner's discretion to reduce the impact of fines on the public sector, coupled with increased engagement, including publicising lessons learned and sharing good practice. To assist in understanding both impact and learning from the trial, a monitoring and review plan was established.

The purpose of this post-implementation review report is to present robust evidence on impact and learning from the trial to inform the ICO's future decisions on regulating public organisations. The ICO's Economic Analysis directorate conducted the review. Although it was done internally, the team was not directly involved in the trial's development or implementation, ensuring objectivity. The overall approach to the review has been theory based and employed mixed methods. This resulted in a broad evidence base to underpin the review's findings, but one that also presented some challenges which should be kept in mind when considering the findings.

The PSA is well aligned with theory, the UK policy context and international approaches; whilst trends in complaints and breach report data have limitations

The PSA is supported by alignment with the theoretical and policy context. The literature finds that fines are an effective regulatory deterrent but have limitations and are not the only tool for promoting compliance. Both monetary and non-monetary incentives play roles, especially in the public sector where motivations differ from the private sector.

The PSA is aligned with UK government goals by promoting best practice for safe data sharing and reducing barriers to data-driven growth. Engaging with public sector organisations helps address perceived data protection barriers and ensures early involvement of the ICO, making data protection laws more enabling.

Internationally, Data Protection Authorities (DPAs) follow a range of approaches to fining public sector organisations. Practice varies amongst European Economic Area (EEA) countries, with over a third imposing no fines, a third imposing reduced fines, and less than a third having no specific rules and applying the same approach to all. Outside of EAA, in other countries, DPAs follow a wide range of approaches on how they impose fines on the public sector, influenced by different legal frameworks and data protection regulations.

Further context for the PSA is provided by ICO data on complaints and personal data breach reports, although for a number of reasons there wasn't an expectation of being able to attribute any trends in these data to the PSA. This proved to be the case.

Reflecting on putting the PSA into practice highlighted novel actions and areas for improvement

Within the ICO, the implementation of the PSA received mixed feedback across different staff levels. Some saw challenges due to a lack of guidance and clear definitions, while others appreciated its flexibility which empowered staff to make decisions based on principles. It was felt that limited engagement with staff prior to introducing the PSA contributed towards misunderstandings early on, and a short lead-in time limited opportunities to consider potential issues and mitigations prior to implementation.

External awareness and understanding of the PSA has varied. Central government engagement took longer than anticipated to set up, but once established it drove greater awareness than in the wider public sector. During the trial period, external coverage was mostly neutral to positive. Some external commentators were critical of the PSA. However, critics of the PSA were divided: some found it too lax, while others believed it should have been applied to the private sector too.

The PSA was perceived as innovative, and it was viewed as positive that the ICO was prepared to trial a different approach so openly. Equally, the approach to monitoring and reporting on the PSA from the outset was noted as novel from an ICO perspective.

Upstream activities have driven change, though this was limited to central government

Awareness of published reprimands and the PSA varied significantly across the public sector, with central government data protection officers (DPOs) being the most aware due to targeted ICO engagement. However, accessibility and presentation of reprimands were seen as areas needing improvement.

Published reprimands were seen as effective deterrents, mainly due to reputational damage, and helped DPOs capture senior leaders' attention. Reprimands were generally viewed as useful for raising data protection standards by sharing best practices and lessons learned, with central government departments citing positive changes and wider effects. However, awareness of reprimands was limited in the broader public sector.

The ICO's increased engagement during the trial was acknowledged. Published reprimands were seen as a useful regulatory tool for raising standards of data protection, through sharing best practice and lessons learned. Central government departments provided examples of this learning, driving change and having wider ripple effects. However, driving change relies on organisations'

awareness of published reprimands which remained limited across the wider public sector.

In terms of impact, around a third of respondents thought that increased engagement had improved data protection compliance, although the same proportion felt there had been no improvement. There was also evidence that upstream activities had raised the profile of data protection amongst senior leaders in central government, particularly the interaction with the Chief Operating Officers (COO) network. However, a recurring theme was that data protection is one of many competing priorities for senior leaders, making it challenging to get traction.

Reduced impact of fines coupled with a notable increase in reprimands, but more to do

During the trial period, approximately 77 reprimands were issued, with 80% targeting the public sector. This marked a significant shift in the ICO's enforcement activity, with a 54% increase in reprimands compared to the previous two-year period. However, the use of other powers like Enforcement Notices and warnings has been limited to date.

Four monetary penalty notices with fines totalling £1.2 million were issued to public organisations during the trial. Without the PSA and the associated increased use of reprimands, fines could have reached £23.2 million, indicating an estimated £22 million difference due to the PSA. There was widespread agreement in the public sector that fines reduce budgets for public services, leading to support for a different regulatory approach, especially among central government DPOs. The wider public sector echoed this sentiment, noting the direct impact of fines on frontline services and disproportionate effects on smaller organisations and devolved administrations' budgets.

However, feedback from some organisations in the wider public sector, including local authorities, was more negative about impact of the PSA. Several DPOs noted that it had made it more challenging to make the case for resources or maintain an interest in compliance with a more limited threat of fines.

Published reprimands a catalyst for change for some, but lack of clarity sees de-prioritisation for others

The impact of the PSA on knowledge and awareness was mixed, but overall sentiment was positive. Data protection professionals, who were the majority of those surveyed, rated their existing knowledge highly. Despite this, the PSA facilitated information and knowledge transfer, with nearly half of central government DPOs reporting new or improved processes due to the PSA. Published reprimands were often cited as catalysts for change, showing how upstream and downstream regulatory activities can synergise to drive improvements.

The impact of the PSA on the status of data protection varied between the wider public sector and central government, likely reflecting the central government focus of the targeted upstream activity. In the wider public sector, there were

concerns about the reduced influence of data protection professionals due to a perceived low threat of ICO enforcement. Conversely, central government DPOs reported increased support from senior leadership and maintained or increased professional influence.

The ICO's reputation benefited from the PSA, being seen as more collaborative and proactive. However, some unintended effects in the wider public sector were highlighted resulting in the de-prioritisation of data protection issues in some instances. Some of these effects may have been exacerbated by a perceived lack of clarity at the outset of the PSA which led some parts of the public sector to believe that the ICO was no longer fining, or even regulating, public bodies. However, feedback received towards the end of the trial suggests this issue had been mitigated.

Trial's outcome isn't a straightforward success or failure, instead, it involves multiple layers

The evidence presented in this review shows that the PSA was an ambitious and challenging trial to deliver over two years with a limited lead-in time. The trial's outcome isn't a straightforward success or failure. Instead, it involves multiple layers: notable achievements, areas with more to do, unexpected challenges, and unintended consequences.

Overall, the PSA has been impactful. It has driven changes that have increased data protection standards, albeit across a smaller population than anticipated. There is clear evidence of how upstream and downstream regulatory activities can work together to drive change. The PSA's effect on the status of data protection varied, likely due to the central government focus of the targeted upstream activities.

The PSA was intended 'not to be a one-way street', with expectations of greater involvement from the public sector, including senior leaders, with investment of time, money and resources in 'ensuring data protection practices remain fit for the future'. While engagement within central government has notably increased, clear evidence of financial and resource investment is less apparent. This reciprocal expectation is less applicable in the wider public sector due to the lack of targeted engagement.

1. Introduction

1.1. Background

In June 2022 the ICO announced[1] and explained[2] a two-year trial of a revised approach to working with and regulating public organisations which in this report we call the 'Public Sector Approach' (PSA). The objective was to work more effectively with these organisations to raise data protection (DP) standards and ultimately lead to better outcomes for UK citizens. The PSA has seen use of the Commissioner's discretion to reduce the impact of fines on the public sector, coupled with increased engagement, including publicising lessons learned and sharing good practice. In June 2024, the two-year trial concluded and the ICO announced[3] that it would review the learning from the trial before making a decision on its future public sector regulatory approach.

1.2. Review of the trial approach

To assist in understanding both the impact and learning from the trial period, a monitoring and review plan was established in conjunction with the launch and implementation of the trial. The plan was underpinned by a theory of change approach and HM Treasury principles (as set out in the Green[4] and Magenta[5] Books) and in line with the ICO's Ex-Post Impact Framework.[6]

The overall purpose of the review is to gain insight into the outcomes and impacts of the trial and assess both the trial itself and the process through which it was delivered. The overall approach to the review has been theory based and employed mixed methods (see Section 2.1 for details of these methods). There were several challenges to measuring the impact of the PSA (see Section 2.2), which should be kept in mind when considering the evidence and findings presented.

---

[1] ICO (2022) *Open letter from UK Information Commissioner John Edwards to public authorities.* Available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/06/open-letter-from-uk-information-commissioner-john-edwards-to-public-authorities/ [Accessed: 18 September 2024].

[2] ICO (2022) *ICO sets out revised approach to public sector enforcement.* Available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/06/ico-sets-out-revised-approach-to-public-sector-enforcement/ [Accessed: 18 September 2024].

[3] ICO (2024) *ICO statement on its public sector approach trial.* Available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/06/ico-statement-on-its-public-sector-approach-trial/ [Accessed: 18 September 2024].

[4] HM Treasury (2022) *The Green Book.* Available at: https://www.gov.uk/government/publications/the-green-book-appraisal-and-evaluation-in-central-government/the-green-book-2020 [Accessed: 18 September 2024].

[5] HM Treasury (2020) *The Magenta Book.* Available at: https://www.gov.uk/government/publications/the-magenta-book [Accessed: 18 September 2024].

[6] ICO (2024) *The ICO's Ex-Post Impact Framework.* Available at: https://ico.org.uk/about-the-ico/our-information/measuring-our-impact/ [Accessed: 18 September 2024].

Key aspects of the monitoring and review plan included:

- A series of quarterly monitoring reports which set out the emerging evidence and sought to identify trends and points of note from a range of evidence activities.
- This post-implementation review report, which brings together and analyses all of the (quantitative and qualitative) evidence streams with reference to the theory of change for the PSA, and presents key insights on impact and thematic learning from implementation of the trial period.

The review has been undertaken by the ICO's Economic Analysis directorate. Whilst it's recognised that this is an internally delivered review, the team were not directly involved in the development or implementation of the trial itself, which helps provide objectivity.

1.3. Purpose and structure of this report

The purpose of this report is to present robust evidence on impact and learning from the trial to inform the ICO's future decisions on regulating public organisations. It is structured as follows:

- Chapter 2 sets out the methodology and sources of evidence for the review;
- Chapter 3 provides the theoretical and policy context, including international benchmarking;
- Chapter 4 explains the process learnings we have found;
- Chapter 5 describes upstream engagement activities and outcomes;
- Chapter 6 describes downstream regulatory activities and outcomes;
- Chapter 7 explores the aggregate level impacts of the PSA; and
- Chapter 8 provides the conclusion and learning points for consideration.

The report is supported by a series of annexes in a separate document:

- A: review approach and methodology;
- B: public sector complaints and data breach report trends;
- C: evidence from international DPAs;
- D: central government DPO survey; and
- E: case studies.

A note on terminology

Throughout this report we use the term Public Sector Approach, or PSA, to refer to the ICO's approach to data protection regulation for public organisations over the trial period June 2022 to June 2024.

Every effort has been made to ensure that the information contained in this report is correct at the time of writing.

2. Review methodology and evidence

The overall approach to the review has been theory based and employed a mixed methods research approach. This chapter explains the research methodology, resulting evidence sources, and some of the methodological challenges. Further details on the review approach can be found in Annex A.

2.1. Research methods and evidence base

The review uses a mixed methods approach, combining both qualitative and quantitative methods to answer the impact and process questions.

As part of the review, over 150 external individuals were engaged (primarily data protection officers (DPOs) and Chief Operating Officers (COOs)), seven internal ICO directorates and over 30 DPAs. Table 1 below outlines the research approaches deployed for the PSA post-implementation review.

Table 1: PSA review inputs

Stakeholder	Research approach	Comments
Central government	Central government DPO survey	Online survey with DPOs in central government and devolved nations, who were contacted at the start and end of the trial period. The survey covered: • awareness and rationale of the PSA; • implementation; • data protection in organisations; and • impacts of the PSA.
	COO Network[7] survey	Online survey with members of the cross-government COO Network. These surveys were conducted at regular intervals throughout the trial period and asked respondents to consider published reprimands and plans they intended to put in place to avoid a similar infringement within their department. The findings of these fed into quarterly monitoring reports.
	COO feedback	The ICO attended a cross-government COO Network in June 2024. This was used to gather

[7] The 11 departments participating in the COO Network are: Cabinet Office, Crown Prosecution Service (CPS), Department for Education (DfE), Department for Health and Social Care (DHSC), Driver and Vehicle Licensing Agency (DVLA), Department for Work and Pensions (DWP), Foreign, Commonwealth and Development Office (FCDO), His Majesty's Revenue and Customs (HMRC), Home Office, Ministry of Defence (MoD), and Ministry of Justice (MoJ).

	from Network meeting	feedback from COOs on the PSA and how it had affected their government department.
	Central government DPO workshop	A virtual workshop with central government DPOs was conducted at the end of the trial. This covered feedback from DPOs on upstream engagement; published reprimands and the impact of fines; overall impacts of the PSA and lessons learned.
	Case-study interviews	Three organisations that fell within scope of the PSA over the trial period were interviewed. Interviewees were asked about mitigating measures their organisation had put in place and their views more widely on the PSA.
Wider public sector	Feedback from public bodies in devolved nations	The ICO attended three network meetings in the devolved nations to gather feedback on the PSA. This included network meetings of Scottish Local Authorities, Welsh Government Executive Agencies and DPOs in the Northern Ireland Executive.
	Intelligence Champions Network	Anecdotal feedback received from DPOs on the impact of the PSA gathered through the ICO's Intelligence Champions Network.
ICO staff	Staff feedback survey	A feedback survey on the PSA was completed by ICO staff at the end of the trial period.
	Internal interviews	A series of internal ICO interviews were held towards the end of the trial to explore learning from how the PSA had been implemented and impacts.
International DPAs	Desk review	Review of EU legislation and online sources (eg legal platforms) comparing approaches across European Economic Area (EEA) countries (those with GDPR).
	Direct consultation	The ICO contacted non-EEA DPAs asking them to share information on their approach to regulating the public sector, including whether administrative fines are permitted.
General	Desk review	Review of:

		• economic academic literature covering aspects of the theory and empirics of effective regulation; • the relevant policy landscape and how it intersects with the PSA; • external commentary on the PSA.
	Monitoring data	Casework data covering data protection complaints and reported personal data breaches.
		Data from investigations directorate on enforcement activity.
		Web analytics data on published reprimands.

Source: ICO analysis.

Table 2 expands on the research approaches outlined in Table 1 to set out the evidence sources that underpin the analysis and synthesis. It is acknowledged that across the evidence base some of the sample sizes are relatively small. However, the central government sample is representative in terms of the central government departmental population, and sample sizes are transparently presented throughout the report.

Table 2: PSA review evidence streams

Research approach	Details	Time period	Sample size
Central government DPO survey	End of trial survey	July 2024	34 responses, (14 central government, 8 devolved administrations, 12 other responses[8])
	Baseline survey	November 2022	28 responses (23 central government, 5 devolved administrations)
COO network survey	Wave 1	May 2023	9 responses
	Wave 2	July 2023	9 responses
	Wave 3	August 2023	11 responses
	Wave 4	January 2024	11 responses
	Wave 5	July 2024	2 responses

[8] Note: 12 responses were received from wider public sector organisations in Wales. These have been excluded from the central government DPO survey analysis but incorporated elsewhere into wider public sector feedback analysis.

COO feedback from network meeting	-	June 2024	21 attendees (including support staff)
Central government DPO workshop	-	July 2024	20 participants
Case study interviews	-	July 2024	3 interviews (DWP, MoD and a public sector organisation in a devolved nation)
Feedback from public bodies in devolved nations	-	June - July 2024	72 attendees across Northern Ireland, Scotland and Wales
Intelligence Champions Network	-	July 2022 - April 2024	Feedback received from 29 DPOs
Staff feedback survey	-	July 2024	10 responses
Internal interviews	-	June - July 2024	7 ICO directorates and 2 members of executive team
International benchmarking	-	July – August 2024	Engagement with 37 DPAs
Casework data covering data protection complaints and reported personal data breaches	-	January 2021 – June 2024	N/A
Data from investigations directorate on enforcement activity	-	July 2018 – July 2024	N/A
Web analytics data on published reprimands	-	April 2023 – June 2024	N/A

Source: ICO analysis.

2.2. Challenges with measuring the impact of the PSA

There are several challenges associated with measuring the impact of the PSA. The primary key challenges and the approaches that have been implemented to try to mitigate these are outlined below.

- **Establishing causality:** Where changes are observed, it can be difficult to assess the extent to which these are related to the PSA, particularly where there are wider external factors that might also influence the outcomes. For example, data protection complaints and personal data breach reports can be time lagged, may or may not relate to infringements of the law and can be influenced by external factors not wholly within an organisation's control. This creates challenges in understanding whether changes in trends can be attributable to the PSA. To help to address this, the review incorporated a range of primary research with both internal and external stakeholders. This included questions on:
    - what external factors have influenced the implementation and functioning of the PSA;
    - the extent to which changes observed are attributable to the PSA;
    - what other factors may have contributed; and
    - what would have happened in the absence of the PSA.
- **Range of stakeholders and the way in which the PSA was implemented during the trial:** The way in which the PSA was implemented meant that fines have been reduced across both central government and the wider public sector while the focus of enhanced regulatory upstream activity has been limited to central government departments for the two-year pilot. This creates challenges for measuring the number of organisations in scope, as well as the impact that upstream regulatory activities have had on compliance. We have tried to mitigate this by including a wide range of research approaches (outlined above), and through targeting a range of stakeholders from central government and the wider public sector to ensure the capture of different perspectives and experiences with the PSA within the review evidence base.
- **Sector definitions:** There are challenges with sector definitions used for the breach reports and complaints data analysed in this report (outlined further in Annex B), as well as the definition of the public sector itself. This is due to the ICO's current data categorisation and the use of subsectors being inconsistent with how they are defined elsewhere (eg the definition of central government used by the ICO differs to how it is categorised by UK government, creating barriers to any benchmarking or comparative analysis). It has not been possible to mitigate this issue.

- **Delivery context**: Following the launch of the PSA, a review plan was developed to assist in understanding the impacts and learnings from the trial period. However, overall progress in delivering the PSA, particularly engagement activity, was more challenging than anticipated and took somewhat longer than initially expected. Given this context, there was a need to update the monitoring and review plan, including changes to some of the milestones, evidence gathering routes and outputs planned. The underlining principles of the original plan remained in place.
- **Baseline**: At the outset there were limited baseline datasets and benchmark indicators to inform the PSA and the development of the review and monitoring plan. The delivery of review and monitoring activities over the PSA trial period helps to establish benchmarks and data for any further interventions in this area.
- **Lagged effects:** The PSA aims to drive behavioural changes, which means that it can take time for the impacts to materialise. At this relatively early stage, given that the PSA has only been in place since June 2022 and with some actions only recently taken, there would not be an expectation of significant evidence of the long-term impacts in the PSA theory of change (see Annex A.3 for further detail on the theory of change). To mitigate this, the route to impact journey was reviewed to assess whether the PSA has driven the expected outputs, whether this is leading to the anticipated intermediate outcomes (ie improved data protection processes), and what this might suggest about future impacts.

3. Theory and policy context

This chapter provides information and context for the PSA by exploring the:

- theoretical background for the imposition of regulatory fines;
- alignment of the PSA trial with the UK policy context;
- trends in public sector data protection complaints and breach reports; and
- comparisons to DP regulation of the public sector in other countries.

The key messages explored in this chapter are summarised below.

Summary of key messages

- In general, fines are a well-established and effective regulatory deterrent to non-compliance. However, they have limits, and **incentives for compliance go beyond penalties, with both monetary and non-monetary factors playing roles,** particularly in the public sector, where regulation requires recognising that incentives and motivations can vary.
- The **UK policy context shows strong alignment with enabling activities under the PSA.** It illustrates how the PSA trial has provided a solid baseline to further contribute to the current government's ambitions in sharing best practice on how to safely share data across government and limiting barriers to data-driven growth.
- Engagement can help alleviate public sector organisations' perceived data protection barriers. Building an enhanced relationship with public sector organisations helps ensure the ICO is brought into conversations early. It also ensures the ICO is given chances to **advocate for data protection compliance by design, allowing data protection laws to work as more of an enabler and less of a constraint**.
- **Complaints and personal data breach reports** may or may not relate to actual infringements of the law. Whilst the root causes of complaints or reported PDBs can often be influenced by the organisation in question, they can also be driven by factors outside an organisation's control. At the outset of the trial there wasn't an expectation of seeing changes in complaint and personal data breach report trends attributable to the PSA.
- **Internationally, DPAs follow a range of approaches to fining public sector organisations.** Practice varies amongst EU/EEA countries that have GDPR. Over a third impose no fines, a third impose reduced fines, and less than a third have no specific rules and apply the same approach to all. In other countries, influenced by different legal frameworks and data protection regulations, DPAs follow a wide range of approaches on how they impose fines on the public sector.

3.1. Theoretical context for the PSA

This section considers the theoretical context for the PSA and surveys the academic and wider literature. We note at the outset that much of the literature referenced in this section considers regulatory intervention from a general position rather than being specific to either data protection or the regulation of the public sector, or both. This reflects the paucity of empirical evidence on these subjects.

3.1.1. Regulatory fines are an established deterrent tool

Fines in a regulatory context serve as a deterrent by discouraging non-compliance and hence promoting adherence to rules and standards. When non-compliant behaviour is punished with adequate frequency and severity, Becker (1968) argues, organisations factor the potential cost of fines into their decision-making. The potential cost of a fine can then deter the organisation from engaging in non-compliant behaviour, where compliance generates higher expected profit than non-compliance.[9,10]

While greater fines provide greater dissuasive effects, there are limits to this mechanism. Fines must also be proportionate to provide 'marginal deterrence' and avoid creating perverse incentives to commit more harmful offenses. Stigler (1970) considers the incentives of a potential offender, using the example that if an offender will receive the same punishment for a minor assault and for murder, then there is no marginal deterrence to murder.[11]

In addition, Veljanovski (2020) warns of the possibility of over-deterrence, which occurs "when the expected penalty is set so high that it […] deters otherwise efficient behaviour or has a chilling effect on the behaviour of firms".[12]

3.1.2. Fines have good deterrent effects but so do other tools

Fines have deterrent effects on the organisations that they apply to, but also wider "spillover" deterrent effects on other organisations.[13] Research from Evans et al (2015) analyses how fines handed down by an environmental regulator to non-compliant firms creates positive spillover effects for other firms. The authors show that enforcement action strengthens the regulator's reputation, having a

[9] Becker, G. (1968) Crime and punishment: an economic approach. Available at: https://www.jstor.org/stable/1830482 [Accessed 5 September 2024].
[10] Baldwin, R., M. Cave and M. Lodge (2010) The Oxford handbook of regulation. Oxford University Press.
[11] Stigler, G. (1970) The optimum enforcement of laws. Available at: https://www.jstor.org/stable/1829647 [Accessed 5 September 2024].
[12] Veljanovski, C (2020) The effectiveness of European antitrust fines. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3730361 [Accessed 7 August 2024].
[13] In economics, a scenario where an interaction between two parties impacts other parties not directly involved in the interaction is said to create an externality, or "spillover" effect. In the context of fines, this spillover is sometimes referred to as a 'general deterrence' effect, as opposed to the 'specific deterrence' effect on the organisation found to be in breach.

positive effect on the compliance of other organisations. Fines that can leverage spillover effects will therefore have a broader dissuasive effect, helping resource constrained regulators to achieve their priorities.[14]

Positive spillover effects from regulatory fines also have a positive impact on economic growth and competition. Enforcement, and the greater compliance that it fosters, mean that the interests of legitimate businesses are not harmed by being at a disadvantage to non-compliant firms. Removing this harm can help to address competitive distortions and disincentives to invest in compliance, and aligns strongly with the ICO's economic growth duty.[15]

However, these positive spillover effects are not exclusive to fines. A recent evaluation of the ICO's FOI Upstream initiative showed early evidence of spillover effects for enforcement notices and later in this report evidence of similar effects linked to reprimand lesson learning are highlighted.[16] Relatedly, a trend amongst European Data Protection Authorities towards the use of reprimands in conjunction with other regulatory tools has been noted.[17]

At the same time, evidence from other regulatory fields suggests that in some circumstances other tools can be more effective than fines. A case study looking at occupational safety in Britain, Germany and France between 2008 and 2014 found no link between having frequent sanctions and fewer fatal occupational accidents. Instead, targeting, differentiation, engagement and prevention seemed to yield better results in improving occupational safety.[18]

Finally, it has been noted that fines have the effect of providing relatively strong incentives to meet a specified minimum level of quality but provide no incentive to outperform the minimum standard. Trémolet and Binderre (2010) argue that it is often better to encourage positive behaviour than punish negative behaviour.[19]

---

[14] Evans, M., S. Gilpatric and J. Shimshack (2015) Enforcement spillovers: lessons from strategic interactions in regulation and product markets. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2664765 [Accessed 5 September 2024].
[15] DBT (2015). *Growth duty: statutory guidance – refresh*. Available at: https://assets.publishing.service.gov.uk/media/66476caebd01f5ed32793e09/final_growth_duty_statutory_guidance_2024.pdf [Accessed 5 September 2024].
[16] ICO (2024) FOI Upstream Evaluation: Interim Findings. Available at: https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/impact-and-evaluation/evaluations/foi-upstream-evaluation-july-2024/ [Accessed 12 September 2024].
[17] Arthur Cox (2023) GDPR Enforcement: The Use of Reprimands by the Data Protection Commission. Available at: https://www.arthurcox.com/knowledge/gdpr-enforcement-the-use-of-reprimands-by-the-data-protection-commission/ [Accessed 12 September 2024].
[18] Blanc, F. (2022) Effective enforcement of privacy regulation – what can be learned from other regulatory areas? Presented at CIPL GPA closed session, Istanbul 28/10/2022.
[19] Trémolet, S. and D. Binderre (2010) Penalties for non-compliance – What penalties are most effective when the operator is in non-compliance with regulatory rules (e.g. for providing data, setting prices, or meeting targets)? Available at: https://regulationbodyofknowledge.org/faq/price-level-and-tariff-design/penalties-for-non-compliance-what-penalties-are-most-effective-when-the-operator-is-in-non-compliance-with-regulatory-rules-e-g-for-providing-data-setting-prices-or-meeting-targets/ [Accessed 10 September 2024].

3.1.3. Incentives for compliance go beyond fines

One of the implications of Becker's framework is that there is economically rational non-compliance with the law, where the costs of compliance exceed the expected costs of non-compliance. Factors that organisations would take into account when making a decision to comply include the costs of compliance, the risk of being caught and successfully enforced against, and the costs that any enforcement action creates (including fines, legal costs and reputational damage). This thinking has been extended and applied in a wide range of contexts.

In a notable example, Harrington (1988) develops a model to seek to explain why the empirical evidence shows generally good compliance with environmental regulation despite limited surveillance and fines. He finds that firms are highly likely to comply when the costs of doing so are low, supporting a focus on reducing regulatory burdens to generate greater compliance. Harrington also observes that even when compliance costs are higher than potential regulatory fines, it's possible that non-monetary factors also incentivise compliance, such as reputational damage from poor publicity. To have this effect, regulators need to promptly spot breaches and communicate enforcement action effectively.[20]

Harrington's findings are reflected in general guidance on good regulation. For example, the OECD (2000) considers that explanations for regulatory non-compliance depend on the extents to which regulated entities:

- know of and comprehend the rules;
- are willing to comply (whether because of economic incentives, good citizenship, acceptance of policy goals or enforcement pressure); and
- are able to comply with the rules.[21]

It follows that compliance can be fostered by improving understanding of the law, and ensuring there are incentives and ability to comply, as well as effective enforcement.

3.1.4. Recognising incentives within public organisations

In regulating the public sector it is important to recognise that public organisations and people in public service have different motivations to those in the private sector. While some public sector organisations carry out commercial functions, most aren't motivated by profit and hence aren't as deterred by potential fines as private sector counterparts. Most commonly, the aim of public sector organisations is to provide services that serve the public interest. Public sector organisations respond to factors such as political influence, budget-setting

[20] Harrington, W. (1988) Enforcement leverage when penalties are restricted. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0047272798001066 [Accessed 23 September 2024].
[21] OECD (2000) *Reducing the risk of policy failure: challenges for regulatory compliance*. Available at: https://one.oecd.org/document/PUMA(2000)4/en/pdf [Accessed 5 September 2024].

and bureaucratic management, and therefore approaches other than financial sanctions should be considered to influence decision making. Mulgun and Albery (2003) argue that "a sense of pride and contribution to public service and the creation of public value" are more powerful incentives in the public sector than monetary factors.[22]

In the UK the Civil Service is expected to display four core values: integrity, honesty, objectivity, and impartiality.[23] Linked to these values is accountability. Accountability in public bodies is vital for ensuring effective governance and public trust. Ministers are ultimately accountable for what happens throughout government, including in public bodies. As the ministerial code states, ministers "have a duty to Parliament to account, and be held to account, for the policies, decisions and actions of their departments and agencies."[24] Accountability in public bodies not only ensures that they are answerable for their actions but also enhances transparency, efficiency, and public trust. For example, accountability influences how voters perceive their elected representatives. Robust accountability frameworks lead to healthier democracies and more responsive governance. In this context, reputation can be a powerful behavioural incentive for public sector bodies. Public sector bodies are ultimately accountable to the public, must operate with a high degree of transparency and act in the public interest.

Applying this thinking to fines, it's possible that their effectiveness varies between the public and private sectors due to differences in their operational goals, accountability structures, and motivations. The evidence here is limited, as there have been few published empirical studies of the effects of sanctions and rewards in the public sector, and those that have been done focus on US institutions.[25] In the context of the infrastructure regulation, for example, it was found that fines are generally effective for private operators if enforced, but "there is a serious question about whether fines are a deterrent for public

[22] Mulgan, G. and D. Albury (2003) *Innovation in the public sector*. Available at: http://www.sba.oakland.edu/FACULTY/MATHIESON/MIS524/RESOURCES/READINGS/INNOVATION/INNOVATION_IN_THE_PUBLIC_SECTOR.PDF [Accessed 7 August 2024].
[23] Civil Service (2015*) The Civil Service code*. Available at: https://www.gov.uk/government/publications/civil-service-code/the-civil-service-code [Accessed 9 August 2024].
[24] Cabinet Office (2010), Ministerial Code, Gov.uk. Available at: www.gov.uk/government/publications/ministerial-code [Accessed 10 September 2024].
[25] NAO (2008) *The use of sanctions and rewards in the public sector.* Available at: https://www.nao.org.uk/wp-content/uploads/2008/09/sanctions_rewards_public_sector.pdf [Accessed 12 September 2024].

enterprises because it is the public that ultimately pays the penalty".[26] This point is supported by literature from the legal and public administration literature.[27,28]

Generally the differing variations between motivations and incentives in regulating the public and private sector can be summarised as:

- In the private sector, financial penalties are a significant deterrent as they directly impact profitability and shareholder value. Fines can damage a company's reputation, affecting customer trust and market position. Companies are motivated to comply with regulations to avoid fines that could give competitors an advantage.
- In the public sector, non-monetary penalties such as reputational damage, loss of public trust, and administrative sanctions can be more impactful than fines. Public sector entities are accountable to the public and elected officials, so penalties often focus on transparency, accountability, and maintaining public trust.

3.2. UK policy context alignment

This section explores how the PSA fits with the wider UK policy context and whether there is alignment.

Specifically in relation to fines, Article 83(7) GDPR (as it was introduced in the UK in 2016) allowed the UK government to make rules about the use of fines against public authorities. Parliament took a positive decision to allow the use of fines, in contrast to some other countries (as explained in Section 3.4 below).

More broadly, the National Data Strategy was introduced in 2019 with the aim of making the UK a world-leading data economy, and ultimately creating data-driven growth. One of its missions was to "transform[…] government's use of data to drive efficiency and improve public services":

> "[T]he government will undertake an ambitious and radical transformation of its own approach, driving major improvements in the way information is efficiently managed, used and shared across government. To succeed, we need a whole-government approach that ensures alignment around the best practice and

[26] Body of Knowledge on Infrastructure Regulation (2012) *Regulating Public vs. Private Operators.* Available at: https://regulationbodyofknowledge.org/general-concepts/regulating-public-versus-private-operators/ [Accessed 10 September 2024].
[27] Graux, H. (2021) *No GDPR fines for public sector bodies at all? No discrimination, and no problem!* Available at: https://inplp.com/latest-news/article/no-gdpr-fines-for-public-sector-bodies-at-all-no-discrimination-and-no-problem/ [Accessed 7 August 2024].
[28] Larson, P. (1998) Public and private values at odds: can private sector values be transplanted into public sector institutions. Public Administration and Development, vol. 17 no. 1.

standards needed to drive value and insights from data".[29]

The emphasis on data sharing is likely to continue under the new Labour government. The Labour manifesto placed significant emphasis on digital and data transformation, which are important enablers of the new government's five missions. In particular, Labour's manifesto committed to "improv[ing] data sharing" across public services to "better support children and families", and to create a National Data Library that can bring together existing research programmes and "help deliver data-driven public services".[30]

Efficient and safe data sharing across government is also an enabler for one of the priorities of Department for Science, Innovation and Technology (DSIT). It aims to "[d]rive forward a modern digital government which gives citizens a more satisfying experience and their time back".[31]

The enabling aspects of the PSA show strong alignment with this wider policy context. The ICO's trial provides a starting point to further contribute to the government-wide effort in sharing best practice on how to safely share data across government, and by removing barriers to data-driven growth.

More broadly in terms of the UK context, recent research with data controllers has shown a need for upstream style support for public organisations aligning with the PSA. For example, 31% of respondents from public bodies said that they faced difficulties in understanding how to share data with other organisations.[32] These public bodies are likely to benefit from an increased emphasis on upstream regulatory tools that provides clarity and helps them overcome this challenge.

This would suggest that an enhanced upstream approach to regulation rather than a deterrent approach to regulation (for example by imposing fines without corresponding engagement) could enhance the ability of data protection to be an enabler of innovation rather than be perceived as one of the many barriers to innovation.

This need is reinforced by the most recent State of the Statistics System report published by the Office for Statistics Regulation, which found that "despite welcome pockets of innovation over the last twelve months, overall there continues to be a failure to deliver on data sharing and linkage across

[29] DCMS (2020). *National Data Strategy* Available at: https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy [Accessed 7 August 2024].
[30] Labour Manifesto 2024. Available at: https://labour.org.uk/change/ [Accessed 7 August 2024].
[31] DSIT – About us. Available at: https://www.gov.uk/government/organisations/department-for-science-innovation-and-technology/about [Accessed 7 August 2024].
[32] ICO (2024) *Data controller study*. Available at: https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/data-controller-study/ [Accessed 12 September 2024].

government".[33] The report noted that "[t]he conversation around data sharing and linkage continues to focus on the risks – from the individual privacy risks to the reputational risks to data owners and government departments", highlighting how the potential benefits for the public good are too often missing from the conversation across government.

3.2.1. Policy context and innovation

In 2020, central government conducted a review of regulatory types and their impacts on innovation. It found that data protection regulation has a mixed effect on innovation:[34]

- it could reduce incentives to innovate in ways that involve personal data, through increased operational and compliance costs (including possible fines); and
- it could help incentivise innovation, by contributing to consumer confidence in new products and by helping create a level playing field across organisations.

Recent research into data controllers confirms that data protection laws are both a constraint and an enabler, depending on the circumstances: 68% of respondents from public bodies said that data protection laws were an enabler, while 45% said that data protection laws were a constraint to at least some extent. The public sector respondents that found data protection laws to be a constraint indicated that it was a barrier due to:[35]

- lack of clarity about data protection law requirements (54% of public-sector respondents who found it a constraint);
- uncertainty about adopting an innovative product or service with unclear compliance assurance (38%);
- costs involved with data protection compliance were too high (32%);
- identifying new processes that restrict innovation (23%);
- making trading with other businesses challenging (17%); and
- making them unable to implement new or improved product or business model (16%).

[33] Office for Statistics Regulation (2024) *The UK's statistical system: OSR's latest views on innovation, challenges and unlocking the power of data through sharing and linkage.* Available at: https://osr.statisticsauthority.gov.uk/news/the-uk-statistical-system-osrs-latest-views-on-innovation-challenges-and-unlocking-the-power-of-data-through-sharing-and-linkage/ [Accessed 7 August 2024].
[34] BEIS (2020) *Taxonomy of regulatory types and their impacts on innovation.* Available at: https://assets.publishing.service.gov.uk/media/5e2f1540e5274a6c45d9e6ef/taxonomy-regulatory-types-their-impacts-innovation.pdf [Accessed 7 August 2024].
[35] ICO (2024) *Data controller study*. Available at: https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/data-controller-study/ [Accessed 12 September 2024].

The PSA helps to alleviate these barriers. By building a relationship with public sector bodies it helps to enhance the likelihood that the ICO is brought into strategic conversations earlier and is given chances to advocate for data protection compliance from design, allowing data protection laws to work as more of an enabler and less of a constraint.

Fines, on the other hand, can reduce funding available for innovation in these organisations, by adding pressure onto public sector organisations' budgets. This is particularly relevant for mission-oriented innovation, which targets grand societal challenges and creates public value to society. Evidence shows that availability of funding is a key factor enabling mission-oriented innovation in the public sector. This is alongside institutional entrepreneurship and mission governance that enable collaboration and experimentation, and the adoption of outcome-based procurement.[36] It is therefore possible that reduced use of or levels of fines, or both, could be an enabler for innovation.

3.3. Trends in DP complaints and personal data breach reports

Monitoring and understanding trends in both public sector data protection complaints and personal data breach (PDB) reports provides further context to the trial approach. As such, monitoring of both was conducted throughout the trial and the findings were included in quarterly monitoring reports. Table 3 provides a summary of key trends from the analysis of complaints and personal breach report data, with full details provided in Annex B.

Table 3: Summary of key trends in public sector data protection complaints and breach reports

Public sector complaints	Public sector PDB reports
• In the first year of the trial, the number of public sector complaints fell by 3% compared to the year preceding the trial's introduction before increasing sharply in year two (up 20% compared to the previous year, and 17% on the year preceding the trial's introduction). These changes highlight the volatile nature of the data, and may reflect lags in the timing of complaints. • Over the lifetime of the trial (Q3 2022 – Q2 2024), health saw the highest number of complaints (at around 8,000, 30% of the total of the trial	• Reported PDBs across the wider public sector have increased since the implementation of the PSA. In the first year of the trial (July 2022-June 2023), reported breaches across the wider public sector increased by 5% compared to the prior year and continued to grow by a further 19% in year two. All public sectors except central government saw an increase in both years of the trial. • Over the lifetime of the trial (Q3 2022 – Q4 2024), health saw the highest number of reported breaches (4,100, 40% of the total reports during the

[36] OECD-OPSI (2021) *Public sector innovation facets – Mission-oriented innovation.* Available at: https://oecd-opsi.org/wp-content/uploads/2021/10/OECD-Innovation-Facets-Brief-Mission-Oriented-Innovation-2021.pdf [Accessed 7 August 2024].

period) followed by local government (around 6,400, 24%) and central government (4,200, 16%).	trial period) followed by education and childcare (around 3,100, 31%) and local government (2,100, 21%).
• Across the wider public sector, the average number of quarterly complaints increased by 8% following the introduction of the PSA. All sectors, except for regulators, saw an increase, the largest being in justice (21%), followed by health (12%) and local government (6%).	• Between Q1 2021 and Q2 2024, an average of 404 wider public sector personal data breach reports were reported each month. The data remains highly volatile, with monthly PDB reports ranging from a low of 265 in August 2021 to a high of 524 in June 2023.
• The most complained about department in every year was the Ministry of Justice (MoJ, 24% - 28% of central government complaints) followed by the Department for Work and Pensions (DWP, 13%-16% of central government complaints).	• Between Q1 2021 and Q2 2024, the departments that reported the most personal data breach reports were HMRC (82 reports, 11% of total central government breaches) followed by the Crown Prosecution Service (59 reports, 8%) and the Department for Work and Pensions (52 breaches, 7%).

Source: ICO analysis.

The trends noted in Table 3 illustrate how complaints and personal data breach reports fluctuate considerably, and it is likely that this is driven by a range of factors. Fundamentally, complaints or reported PDBs may or may not relate to actual infringements of the law. Whilst the root causes of complaints or reported PDBs can often be influenced by the organisation in question, they can also be driven by factors outside an organisations' control. For example, an organisation could take all reasonable steps to ensure compliance and yet still be the subject of a cyber incident. Or a breach of the law by a non-public sector organisation might trigger complaints or breach reports against a public sector organisation. This makes it challenging to discern thematic trends in the data.

Questions about timings also contribute to this challenge. For example, the points of time at which the cause of an event occurs, the event itself occurs, the event is detected by the organisation, the event becomes known to the ICO and the ICO reports the event are not the same. It is often the case that large events which are reported in one year actually happened in previous years, and the current record will change as more becomes known and reported.

In any case, changed trends in complaints and personal data breach reports are considered a 'longitudinal impact' in terms of theory of change principles and the focus of trial activities, and would likely only be observed in the long-term. Therefore, from the outset of the trial, there wasn't an expectation of seeing changes in these trends attributable to the PSA during the two-year trial period.

Before this type of long-term benefit can be observed in the data, progress will first need to be made against shorter term outputs and intermediate outcomes,

by improved data protection processes. For example, enhanced upstream regulatory activity is critical to developing awareness of data protection issues in central government. This would be expected to lead to improved processes, an important factor in driving compliance. Over the long-term this may contribute to a reduction in complaints and personal data breach reporting and increased public confidence in handling personal data.

3.4. International perspective to regulating the public sector

This section reviews the approach taken by other DPAs to regulating the public sector, both in EU and EEA member states, which have GDPR,[37] and other countries.

In EU and EEA member states, administrative fines for infringement of the GDPR are calculated following the guidelines issued by the European Data Protection Board. These guidelines outline the starting points and the methodology used to calculate a fine, aiming to harmonise the process across DPAs. The guidelines apply to calculating administrative fines to be imposed on public authorities and bodies, except the steps that relate to turnover and corporate liability. However, as the guidelines note, not all DPAs have the power to issue administrative fines on the basis of national law.[38]

> "According to Article 83(7) GDPR, each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State*".*

It was reported in 2023 that DPAs from 24 different GDPR countries (+2 from 2022) had imposed a total of 191 fines (+55 from 2022) on representatives of local governments (such as mayors), police officers, schools, universities and other public bodies or educational institutions. These fines amounted to a total of more than €24 million (+9.9 million from 2022).[39] It was noted that "DPAs appear to have increased scrutiny of the public and education sector since […] 2020 […], in particular in connection with the use of technology".[40]

It was also found that fines in the public and education sector were most commonly related to insufficient legal bases for data processing (38% of fines in the public and education sector), and insufficient technical and organisational

[37] The GDPR (Regulation (EU) 2016/679) was adopted in 2016 and became effective in 2018. It regulates information privacy in the European Union (EU) and the European Economic Area (EEA) countries.
[38] European Data Protection Board (2023) *Guidelines 04/2022 on the calculation of administrative fines under the GDPR.* Available at: https://www.edpb.europa.eu/system/files/2023-06/edpb_guidelines_042022_calculationofadministrativefines_en.pdf [Accessed 7 August 2024].
[39] CMS (2023) *GDPR Enforcement Tracker Report.* Available at: https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report-2023 [Accessed 7 August 2024].
[40] Ibid.

measures (30%). Non-compliance with general data processing principles was less relevant in the public sector and in education compared to all GDPR violations (15% vs 24%).[41]

Highest GDPR fine to public sector

The highest fine in the public and education sector as of 2023[42] was issued by the Portuguese DPA in the same year. It sanctioned the Portuguese National Statistical Institute with a fine of **€4.3 million** for numerous violations of several general data processing principles of the GDPR in connection with the 2021 census in Portugal. The controller did not inform the data subjects about the voluntary nature of providing their religious and health data. Further, the controller had failed to exercise due diligence in selecting its processor, contrary to its obligation under article 28 of the EU GDPR, and had permitted the transfer of personal data outside the EEA without providing for additional security measures besides the European Commission's SCCS, as required under the Schrems II ruling. The DPA considered this to be a breach of article 44 of the EU GDPR and article 46 (2) of the EU GDPR. Finally, no data protection impact assessment was carried out for the census.

When it comes to administrative fines for public authorities in GDPR countries:

- 37% of DPAs impose no fines;
- 33% of DPAs impose reduced fines; and
- 27% of DPAs have no specific rules for public authorities, and impose the same fines to all.

A more detailed review of the approach followed by each country with GDPR can be found in Annex C.1.

Internationally, outside of the EEA, countries have different legal frameworks and data protection regulations. These differences affect how DPAs are set up, their remits, and how they operate, including how they regulate public authorities and whether they fine them. A more detailed review of the approaches taken to regulating the public sector internationally can be found in Annex C.2.

Table 4 combines findings (both EEA and internationally) detailed in Annex C, showing which countries have different penalties for the public sector, either because of specific provisions put in place or because of the legal framework, and which ones don’t.

[41] Ibid.
[42] CMS, ibid.

Table 4: Global comparison of approaches towards public sector

Data protection legal framework	Different penalties for public sector	Same as private sector	Comparison not possible
GDPR	Austria Belgium Croatia Cyprus Czech Republic Denmark Estonia Finland France Germany Greece Hungary Ireland Liechtenstein Lithuania Luxembourg Malta Poland Romania Spain Sweden	Bulgaria Iceland Italy Latvia Netherlands Norway Portugal Slovakia Slovenia	
National law(s) other than GDPR	Andorra Bosnia-Herzegovina Japan Jersey New Zealand	Canada Guernsey Hong Kong Jersey Mauritius Switzerland (federal) Switzerland, Cantone Ticino Switzerland, Zurich	Australia Australia, New South Wales Australia, Northern Territories Australia, Victoria Switzerland, Kanton Berne USA

Sources: ICO analysis.

The review found no clear patterns in how different countries and their DPAs decide to regulate data protection in the public sector. Legal systems, historic patterns of regulation and other factors interact to create each country’s position, resulting in a wide range of approaches to using data protection fines in the public sector.

4. Putting the PSA into practice - process learning

This chapter presents the lessons that can be learned from understanding how the PSA was put into practice, how it operated to achieve its intended outcomes, and the factors that influenced these processes. Process evidence adds value by generating structured information and recommendations that help to improve the future effectiveness and efficiency of activities and wider learning in the ICO.

It draws on primary evidence collected through internal interviews, surveys, and external commentary (further details on methodology and sources of evidence provided in Chapter 2). The key messages from putting the PSA into practice are summarised below.

Summary of key messages

• Within the ICO there were **mixed views at different management levels on the way the PSA was implemented**. Some highlighted that challenges stemmed from a lack of guidance on the practical application of the PSA and definitions of key terminology. Others highlighted that its flexibility should be seen as beneficial in enabling staff to be empowered to make decisions via a principles-based approach. It was felt that limited engagement with staff prior to introducing the PSA contributed towards misunderstandings early on, and a short lead-in time limited opportunities to consider potential issues and mitigations prior to implementation.

• While initial external communication was considered clear and was reported to have landed quite strongly, **levels of awareness and understanding of the PSA have been mixed. Central government consultees tended to have greater awareness than those in the wider public sector**, which may reflect increased levels of upstream engagement with central government, once this was established. During the trial period, external coverage of the PSA was described as overall 'neutral, verging on positive'.

• The PSA trial was perceived as novel, and it was viewed as positive that the ICO was prepared to **trial a different approach so openly**. Similarly, the **approach to reviewing, monitoring, and reporting on the PSA from the outset** was quite distinctive from existing ICO practices and was considered good practice in regulatory policy making.

• Some **external commentators were critical of the PSA**. However, their criticisms were divided: some critics found it too lax, while others believed it should have been applied to the private sector too.

4.1. Implementation of the PSA

Table 5 provides a summary of the learning points related to the way in which the PSA was implemented and communicated to relevant stakeholders.

Table 5: Process learning on the implementation of the PSA

Topic	Detail
Developing the PSA	Internal feedback highlighted the importance of following the ICO's policy methodology[43] to ensure policy development is evidence-based, documented and transparent. There could have been greater levels of internal and external consultation prior to introducing the PSA, to provide an opportunity to consider how the policy would be applied in practice and issues that might arise so that these could be mitigated from the outset. The approach to review, monitoring, and reporting on the PSA from the outset was thought to be novel in terms of existing ICO practices and was considered to be an example of good practice in regulatory policy making.
Inputs (time and resources)	Some aspects of the ICO's regulatory delivery were more challenging or required more time due to the PSA. However, this did not directly result in a need to recruit any additional staff. Where tasks were more time-consuming due to the PSA, this tended to be linked to the lack of written guidance for how the PSA should be applied in practice, and the speed at which the PSA was rolled out.
Communication of the PSA internally	Understanding of the PSA was limited early on, which was linked to the limited internal engagement and consultation with staff prior to introducing the PSA. Internal feedback suggests that initially the predominant interpretation of the PSA was that the ICO would no longer be fining the public sector. The focus on increasing upstream engagement and use of a wider range of regulatory tools was not understood universally until later on.
Challenges in implementing the PSA	As already noted in Section 2.2, the upstream engagement activities took longer to establish than was originally anticipated. Challenges in implementing the downstream aspects of the PSA tended to stem from the lack of guidance on the practical application of the PSA and definitions of key

[43] ICO (2024) *Policy Methodology*. Available at: https://ico.org.uk/media/about-the-ico/policies-and-procedures/4028535/policy-methodology.pdf [Accessed: 18 September 2024].

	terminology. Some staff highlighted that further guidance would be useful in the following areas: • procedural steps for implementation and clarification on how the PSA fits into the ICO's fining guidance; • the level of detail, length and processes for publication of reprimands to increase consistency and certainty; and • key terminology (eg clear definitions of 'egregious' and of the types of organisations considered in scope). However, feedback on these points varied at different management levels. Some felt that not having strict definitions allowed flexibility, where staff could be empowered to make their own decisions and that a principle-based approach should be applied for key terminology like 'egregious', building on case law and precedence.
Governance and accountability	The governance and accountability of the PSA has evolved over time and there has been learning around the importance of accountability lines for the work to ensure the whole vision was progressed. In terms of downstream interventions, there were challenges in terms of the need for changes to existing processes and their consistent application.

Source: ICO analysis.

4.2. How the PSA was delivered and received externally

Initial messaging in external communications was reported by internal consultees to be clear and to have landed strongly. However, levels of awareness of the PSA reported by external consultees varied. This may be linked to levels of engagement with public sector bodies.

- Internal feedback indicated that there had been increased engagement with central government, but there was less certainty about whether levels of upstream engagement had changed with other public sector bodies as a result of the PSA.
- It was felt that the dial was shifting on the relationship with central government, but it needed to move further, and that there would be an opportunity to be a facilitator with the new government and its ambition for better use of data.

Public sector bodies often referenced the PSA early in conversations regarding data protection breaches (ie that they would not be fined due to the PSA). This suggests a need to greater publicise the wider regulatory tools in use and correct any misconceptions about the PSA being about not fining. Internal feedback also

suggested that there is an opportunity to better publicise and communicate the proactive engagement delivered through the PSA. This includes telling the story of how the ICO is working with organisations that have come into scope of the PSA, and the changes these organisations are making as a result of this.

While views from the general public have been mixed, it was reported that on the whole, coverage of the PSA externally tended to be 'neutral, verging on positive'. With regards to fines that have been issued, external reporting had often been quite neutral or factual. Some consultees highlighted that the PSA was perceived as quite novel externally, and that it is positive to demonstrate that the ICO is prepared to trial different approaches so openly:

"Publicly, the public sector approach has been perceived as different. If sat in a public sector organisation, even if you might not change your compliance behaviour, you might see ICO as an organisation that is prepared to try things out and experiment".

4.2.1. External commentary on the PSA

Early commentary on the PSA from the legal sector highlighted that, despite the PSA being "based on a practical, proportionate, risk based and outcomes-focused approach", consistent application of data protection enforcement principles was key to its effectiveness. It was recognised that the use of a wider range of enforcement measures other than fines "may have significant implications for [data controllers and their organisations], albeit in a different way to monetary penalties. […] Public reprimands may also potentially expose data controllers to significant reputational risks".[44]

Another article from the legal sector also discussed the reputational effect of reprimands, and added on potential risks for organisations:

"By publishing reprimands, the ICO encourages compliance and highlights lessons for controllers. However, there is a concern that reprimands can lead to reputational harm (and potentially provide the basis for follow-on claims) without the organisation being given the chance to make representations to the ICO (as is provided for in the case of a fine) and, perhaps even more importantly, without the possibility of appeal".[45]

[44] Ropes & Gray (2022) *ICO highlights new strategic approach to regulatory action.* Available at: https://www.ropesgray.com/en/insights/viewpoints/102i27w/ico-highlights-new-strategic-approach-to-regulatory-action [Accessed 7 August 2024].
[45] Slaughter & May (2023) *Key developments in contentious DP in 2023.* Available at: https://www.slaughterandmay.com/insights/importedcontent/key-developments-in-contentious-dp-in-2023/ [Accessed 7 August 2024]. Note that organisations are given the opportunity to make representations on a notice of intent to impose a reprimand. This point will be made clear publicly

Other commentary warned against light-touch regulation, which has historically been less effective at preventing harms,[46] and about an inconsistent approach to fining public sector bodies across regulators.[47] Critics of the PSA were divided: some found it too lax,[48] while others believed it should have been applied to the private sector too.[49] For example, one commentator noted that even for businesses, deterrence may not be a key mechanism to achieve greater compliance: avoiding a fine is the primary motivation for compliance for one fifth (19%) of businesses who responded to their research, compared to the third who named remaining competitive (34%) or increasing customer demand (34%).[50]

when the ICO consults on the Data protection procedural guidance. Although there is no statutory right of appeal to the Tribunal in respect of reprimands, organisations can seek judicial review.

[46] Campaign for Records (2024) *Undoing 40 years of progress on information rights.* Available at: https://www.campaignforrecords.org/blog/undoing-40-years-of-progress-on-information-rights [Accessed 7 August 2024].

[47] Society for Computers & Law (2023) *Data breaches: why shouldn't public bodies be fined?* Available at: https://www.scl.org/12989-data-breaches-why-shouldn-t-public-bodies-be-fined/ [Accessed 9 August 2024].

[48] Mishcon de Reya (2023*) ICO's regulatory use of reprimands: does it need a rethink?* Available at: https://www.mishcon.com/news/icos-regulatory-use-of-reprimands-does-it-need-a-rethink [Accessed 7 August 2024].

[49] Farrer & CO (2022) *Is the ICO going soft on fines?* Available at: https://www.farrer.co.uk/news-and-insights/is-the-ico-going-soft-on-fines/ [Accessed 7 August 2024].

[50] ISMS.online (2024) *The ICO is reviewing its approach to public sector fines: what should it decide?* Available at: https://www.isms.online/information-security/the-ico-is-reviewing-its-approach-to-public-sector-fines-what-should-it-decide/ [Accessed 23 August 2024].

5. Upstream regulatory activities in focus

This chapter explores the impact and effectiveness of the ICO's upstream regulatory activities under the PSA. The evidence in this section is largely based on the findings of a survey of central government DPOs. This also draws on feedback received during workshops and interviews with central government departments.

Summary of key messages

- **Awareness of published reprimands and the PSA varied widely across the public sector**. Awareness was greatest amongst central government DPOs, correlating with the targeting of central government as part of the ICO's upstream engagement. However, some **barriers were highlighted in terms of the accessibility and presentation of published reprimands, with improvements suggested**.
- **Published reprimands were viewed as an effective deterrent, primarily due to the negative impacts of reputational damage**. DPOs found reprimands an effective tool to get the attention of senior leaders.
- Generally, **published reprimands were seen as a useful regulatory tool for raising standards of data protection**, through sharing best practice and lessons learned. Central government departments provided examples of this learning **driving change and having wider ripple effects.** However, driving change relies on organisations' **awareness of published reprimands which remains limited across the wider public sector.**
- There was **agreement that the ICO had increased engagement over the trial. However, attribution was mixed** with only two in five respondents believing this was linked to the PSA.
- In terms of impact, around a third of respondents thought that increased engagement had improved data protection standards and compliance, although the same proportion saw no difference. There was **evidence that upstream activities had raised the profile of data protection amongst senior leaders in central government. In particular, the interaction with the COO network had provided DPOs with opportunities for dialogue and briefing with senior leaders**. It was noted all the upstream factors fed into improvements that 'started with the ICO being more available.'
- A recurring theme was that **data protection was one of many competing priorities for senior leaders, making it challenging to get traction**.

5.1. Upstream in context

In terms of upstream regulatory activities, these can be thought of as enabling and softer regulatory tools, such as education, engagement, influence, advice and guidance. A key aspect of the PSA is to work in partnership with public organisations and to adopt a more proactive approach to raise data protection standards. As set out in the Commissioner's open letter at the outset of the trial:[51]

> "I also have a responsibility as a regulator to enforce the law around compliance issues that continue to happen. The powers I hold are there to act as a remedy and deterrent to data breaches, not, as is often thought, to act only as a punishment".

This involves:

> "Working proactively with senior leaders across the public sector to encourage compliance, prevent harms before they occur and learn lessons when things have gone wrong".

In practice this has been primarily delivered through enabling a lessons learned approach via the publication of reprimands; and increasing ICO engagement with central government departments at both a chief operating officer (COO) and DPO level, through the cross-Whitehall Chief Operating Officers' (COO) network[52] where activities included:

- regular ICO speaking slots at COO network meetings where the Commissioner engaged with members;
- surveys to understand data protection practices and needs; and
- use of lesson learning tools to put the published reprimands into context.

These activities have been supplemented with ad-hoc blogs[53] to share thematic learning and a session on reprimands at the Data protection practitioners' conference (DPPC) 2023. There is also ongoing engagement with central government and devolved administration DPOs as part of business as usual,

[51] ICO (2022) *Open letter from UK Information Commissioner John Edwards to public authorities.* Available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/06/open-letter-from-uk-information-commissioner-john-edwards-to-public-authorities/ [Accessed: 18 September 2024].
[52] The 11 departments participating in the COO Network are: Cabinet Office, CPS, DfE, DHSC, DVLA, DWP, FCDO, HMRC, Home Office, MoD and MoJ.
[53] For example: ICO (2024) *Lessons learnt from reprimands.* Available at: https://ico.org.uk/action-weve-taken/lessons-learned-from-reprimands/ [Accessed 18 September 2024].

including via attendance at monthly meetings of the Central Government Data Protection Committee (CGDPC), which reinforces the PSA.

As noted in Section 2.2, upstream engagement activities took longer to establish than was originally anticipated. In the remainder of this chapter these activities and their impacts are explored.

5.2. Enabling lessons learned via the publication of reprimands

A total of 77 reprimands were issued by the ICO during the trial period, and at the time of drafting 70 have been published.[54] From the total, 60 were issued to public sector organisations. The focus of this section is on how these reprimands were used for lesson learning. Further details on these reprimands is provided in Section 6.2 from an enforcement perspective.

5.2.1. Role of engagement in enabling impact

The delivery of behavioural changes and impacts, as set out in the theory of change (see Annex A.3), is contingent on public sector engagement with published reprimands. This, to a large extent, depends on organisations' awareness of reprimands and more generally of the PSA. Generally, feedback suggested that awareness of published reprimands and the PSA varied widely across the public sector, as detailed in the following. In response to the DPO surveys at the end of the trial:

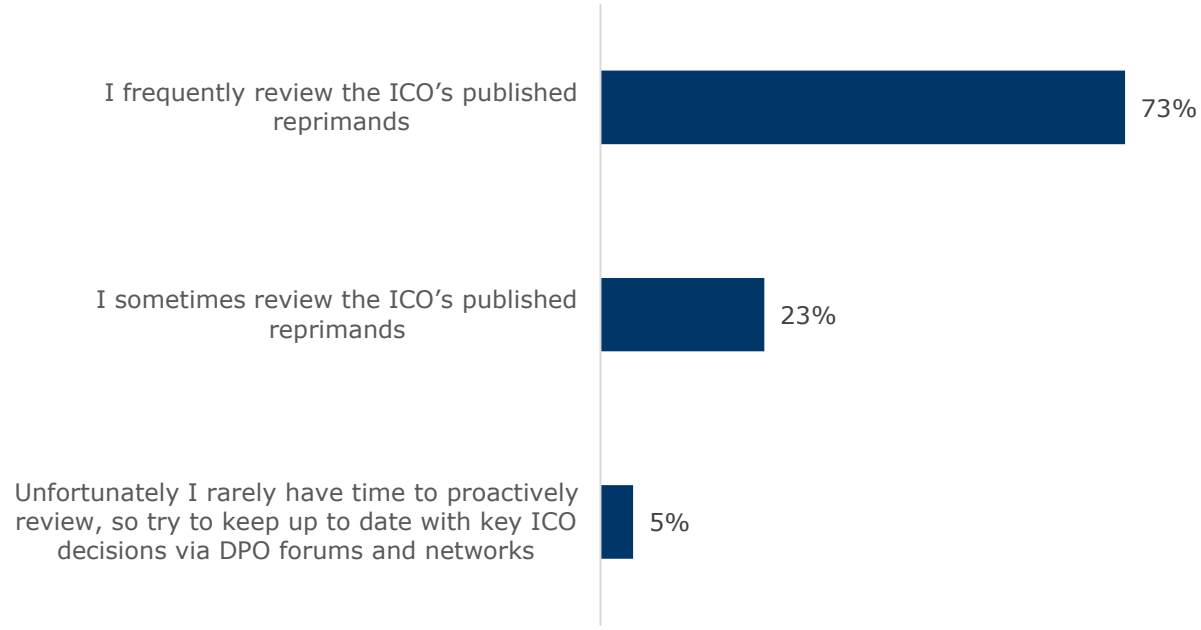
- All respondents to the central government DPO survey were aware that the ICO regularly publishes reprimands: 86% (19 respondents) were "fully aware" and 14% (three respondents) had "some general awareness but did not know any detail".
- Across wider public sector networks, awareness was varied, with around two thirds of respondents having some awareness or being fully aware of the PSA.
- One organisation that had received a reprimand under the PSA had not been aware of a change in the ICO's approach.

The relatively greater level of awareness in central government likely reflected the increased engagement focus with central government departments during the trial period. It also highlighted the challenges associated with ensuring that messages of best practice reach the wider public sector.

Reported levels of engagement with published reprimands amongst central government DPOs are shown in Figure 1. The majority of respondents (73%, 16 respondents) review published reprimands on a regular basis.

[54] It should be noted in some cases there is a lag between reprimands being issued and published on the ICO website, as discussed further in Section 6.2.

Figure 1: Respondents' engagement with published reprimands



Source: ICO analysis (n=22).

Across the wider public sector, organisations highlighted a number of barriers to engaging with published reprimands. Several DPOs noted:

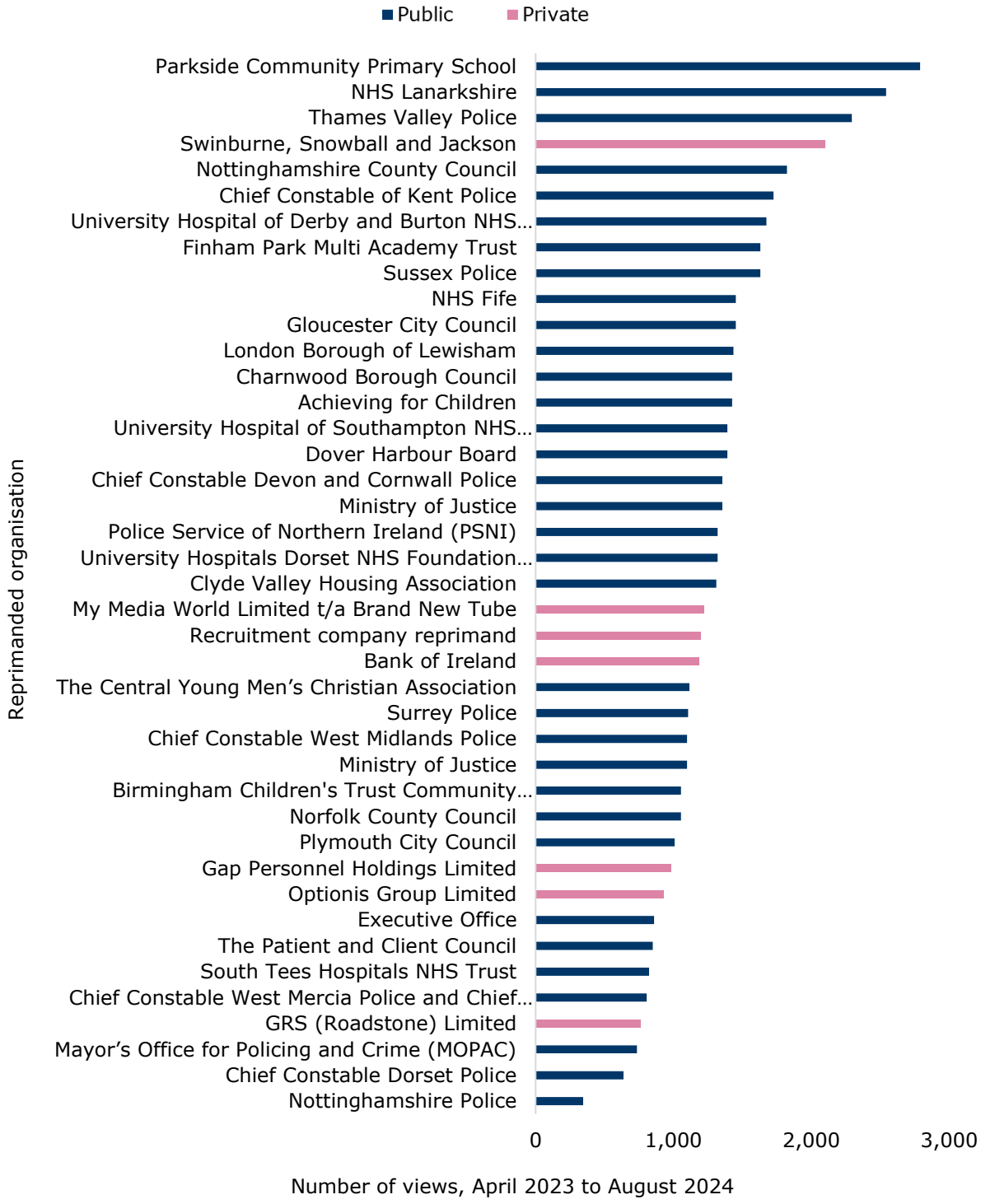
- improvements could be made to the ways in which reprimands, cases and decision notices are shared. One DPO noted that it can be difficult to find and search reprimands by topic or key term, or both, and queried whether improvements could be made to the ICO website to facilitate this. While another indicated that proactively sending out materials to DPOs may be more helpful (eg detail of breaches and trends the ICO is seeing); and
- a need for the ICO to better understand that public organisations are often working with very limited resources and in some cases have limited capacity to tease out and respond to reprimand learning. To respond to this, it was suggested that the ICO could link to guidance and support related to the issue in the reprimand to help organisations avoid breaches.

5.2.2. Engagement with reprimands published on the ICO website

Figure 2 shows the number of views of reprimands published on the ICO website between April 2023 and June 2024.[55] During this period, 41 reprimands were published, of which 34 related to organisations in the public sector and seven to organisations in the private sector.[56]

[55] Comparable web analytics are only available from April 2023. Note that not all of these views will have been by employees of public sector organisations, and it is not possible to exclude views by ICO staff from these figures.
[56] It should be noted that reprimands were published at different times so, for example, those available for longer may have more views. The number of views also likely reflects the level of media interest in certain breaches rather than engagement from any particular sector.

Figure 2: Number of website views for reprimands



Note: Comparable web analytics are only available from April 2023. Whilst this chart shows reprimands published between April 2023 and June 2024, the viewing period runs to the end of August 2024 to allow reprimands published later in the trial period to have viewing data. Source: ICO analysis.

The reprimand to Parkside Community Primary School received the most views (2,790 views) whereas the reprimand for Nottinghamshire Police received the fewest (345 views). Reprimands to organisations in the public sector tended to receive more views with one exception.

5.2.3. Reprimands viewed as a deterrent in the public sector

There was general support for the view that published reprimands are an effective deterrent amongst public sector organisations. Support for this view was strong amongst central government DPOs, where:

- the majority of respondents to the DPO survey agreed that published reprimands are an effective deterrent. Responses commonly cited the negative impact of reputational damage which is effective in getting the attention of senior stakeholders; and
- a number of respondents agreed that reprimands were an effective deterrent, but only to a limited extent. In so far as further detail was provided, reasons included limited coverage of reprimands in the media.

The reputational damage associated with published reprimands was frequently cited as a deterrent across the public sector, as highlighted by comments at the central government DPO workshop:

"The gravity of having something publicly saying you are not doing something satisfactorily when benchmarked against other organisations – that's much more significant than a fine".

"Senior managers don't want to be named and shamed in reprimands and take these seriously. It has also been helpful that some bodies have been fined so that this risk of fine is still there".

"The publishing of reprimands are a valuable resource, even if their department are not directly affected. Knowing what the fine would be helps with communicating that across the businesses, where it would have otherwise been abstract. Before I could say that we might get a fine but couldn't say how much – now there are many tangible examples they can highlight to business areas".

"No central government body wants the reputational damage associated with a fine or reprimand".

"They (reprimands) can be used to draw senior management attention to the potential negative outcomes of non-compliance".

5.2.4. Impact on knowledge and awareness resulting in changes

Across the whole public sector there was strong support for the view that reprimands are a useful regulatory tool for raising standards of data protection.

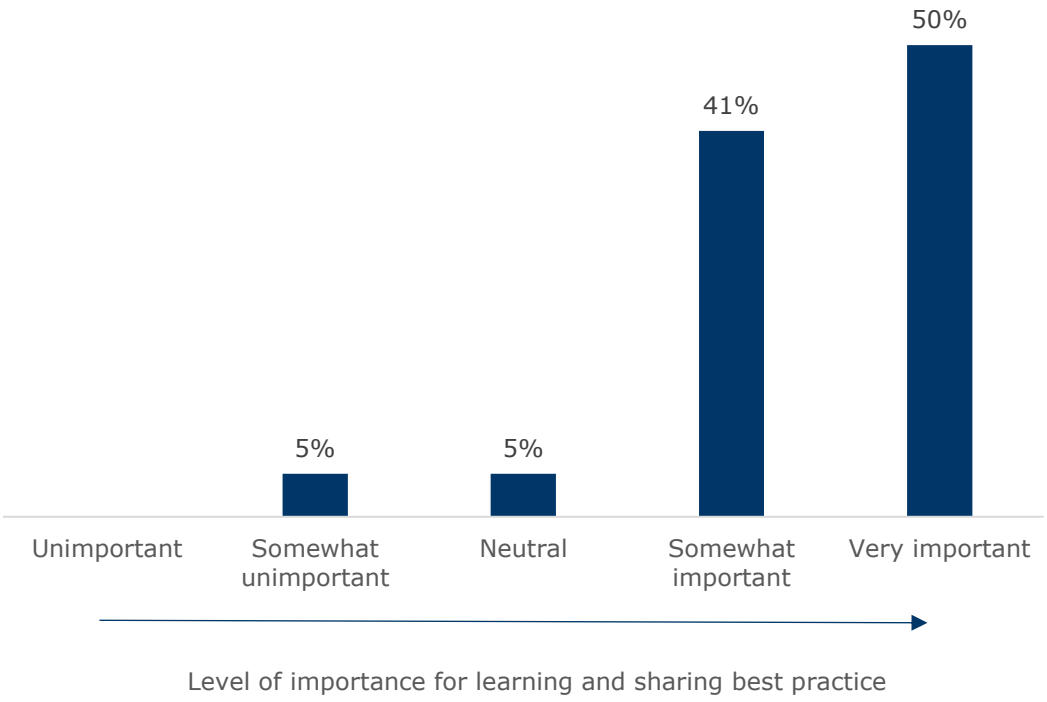
Amongst central government DPOs:

- The majority of respondents to the DPO survey agreed that published reprimands are useful for taking a lessons learned approach. Central government DPOs highlight that they are useful for:

  - encouraging organisations to reflect on their own data protection practices;
  - assessing the likelihood of similar breaches occurring in their own department; and
  - putting in place mitigating measures should these be required.
- One DPO felt however that reprimands are of limited use due to difficulties in getting senior leaders to engage with them.

The majority of respondents to the same survey *(*91%, 20 respondents*)* agreed that published reprimands were important for learning and sharing best practice within their department, as shown in Figure 3 below.

Figure 3: Views on the importance of published reprimands for sharing best practice



Source: ICO analysis (n=22).

Individual responses highlight that published reprimands have been used as case studies for training activities, to inform internal guidance notes to staff and for discussion at data protection forum meetings where business units reflect on the risk of a similar breach occurring.

Within central government, DWP highlighted (see case study in Annex E.3) that it had made specific enhancements to data protection processes in response to a data breach at a different public organisation that had been reported on by the ICO. DWP noted that some of these changes to data protection practices *"were*

used as a model for other departments" illustrating the ripple effects and wider learning that often accompany actions of this nature.

Elsewhere in the wider public sector, DPOs noted the following impacts linked to reprimands:

"The publication and rhythm (of published reprimands) has helped in terms of how we prioritise the resources we have and concentrate on where we can be proactive".

"Our department regularly look at published reprimands to see whether we can proactively change anything. This wasn't an approach that was taken prior to the PSA being introduced".

"Our department got a reprimand, which would have been a fine if it weren't for the PSA. This was received more proactively and got them through the lessons learnt and received greater acceptance from senior leadership than would have otherwise been the case".

One organisation that was interviewed for a case study thought that while reprimands are helpful in creating conversation and increasing focus on avoiding the issue occurring again, if overused, they may lose impact over time.

Other comments around the impact of published reprimands noted that:

- although reprimands tend to get less media coverage than fines, some organisations felt they were a useful regulatory tool for getting data protection on the agenda of senior managers at a lower threshold than would be the case for a fine; and
- the reputational impacts that come with reprimands could be damaging for a public organisation, particularly in the context of public trust and any knock-on effects on the public seeking support, particularly the case where sensitive data is being processed.

The latter point needs to be balanced in the context of the enhanced public trust the ICO expects to result from robust and transparent enforcement to protect the rights of members of the public.

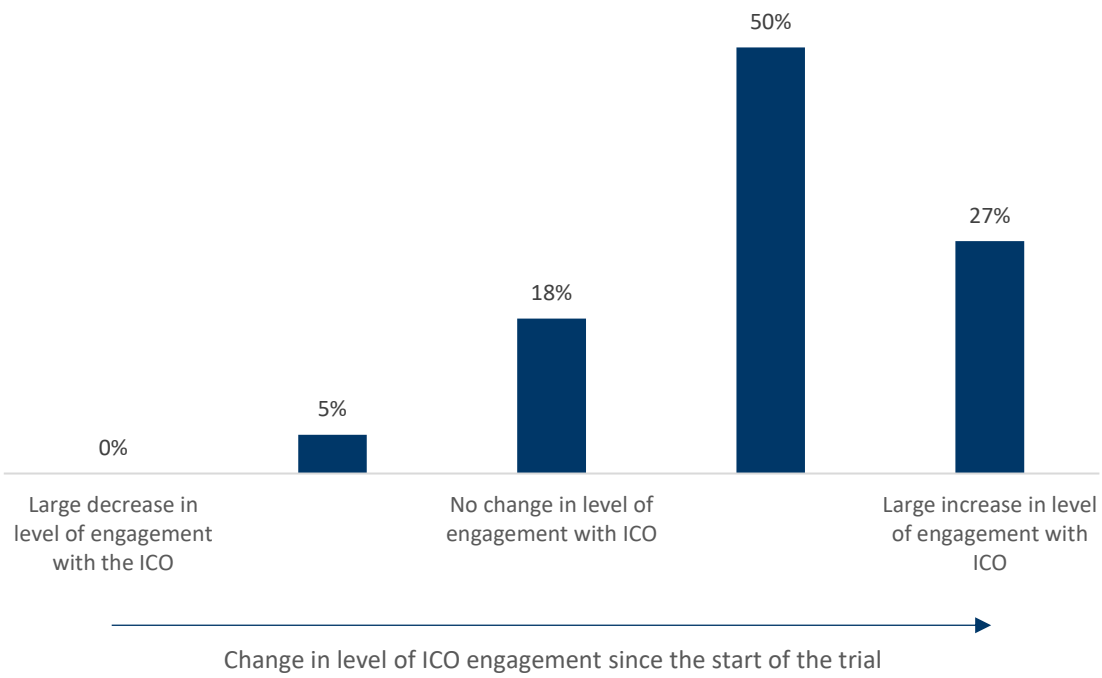
5.3. Enhanced upstream engagement activities

5.3.1. Changed engagement levels

Nearly two thirds of central government DPOs (14 respondents) agreed that the ICO had been working upstream to enhance data protection by design. The remaining third (eight respondents) were either undecided (seven respondents) or disagreed (one respondent).

Over three quarters of central government DPOs (77%, 17 respondents) thought there had been a rise in the level of ICO engagement over the trial period, as shown in Figure 4.

Figure 4: Change in respondents' level of engagement with the ICO over the trial period



Source: ICO analysis (n=22).

When asked to what extent any change in ICO engagement was applicable to the PSA, the levels of attribution were mixed:

- 5% (one respondent) thought this entirely attributable to the ICO's public sector approach;
- 36% (eight respondents) thought this was partially attributable to the approach;
- 27% (six respondents) thought changes in levels of engagement were entirely attributable to factors other than the public sector approach;
- 23% (five respondents) indicated that this was not applicable; and
- 10% (two respondents) explained other factors that had influenced changes in level of ICO engagement, including moving from a part-time to full-time DPO and the department now having more experienced practitioners and complex information access requests.

5.3.2. Impact of upstream engagement

There were mixed views amongst central government DPOs on how engagement had impacted data protection compliance. Around a third (36%, eight respondents) thought it had improved data protection compliance; another third

(36%, eight respondents) noted no change in compliance; and 5% (one respondent) thought that it had led to an increased awareness of data protection in their department.[57]

When asked in the DPO survey about the impact of upstream engagement activities, many central government DPOs noted that this had raised the profile of data protection amongst senior managers.

"The ICO's engagement with COO network has been helpful from a DPO perspective as it's provided more opportunities for dialogue on data protection with senior management. This helps raise profile and consciousness of data protection amongst senior management".

"As the Commissioner attends the COO network, and DPOs regularly provide briefing this has immediately helped in raising awareness of data protection issues at a senior level".

"There was lot of drive to attend cross network meetings as the ICO would also be there, which led to our department being more engaged in cross government networks. This helped to justify using time senior leaders to also attend these meeting. All these factors have fed into improvements and some of it starts with the ICO being more available".

"…the ICO's emphasis on reprimands, attendance at COO network meetings and issuing of surveys based on the reprimands have all helped to raise the profile of data protection".

Despite this, some consultees noted that data protection was only one factor that influences senior decision-making, given the various other priorities and risk mitigations that senior leaders need to balance (see case study in Annex E.2). Also, it was noted that organisations often face challenges in implementing changes aimed at improving compliance (including accountability, resources and culture) as many of the barriers aren't quick fixes and require phased solutions.

[57] Also 36% (four respondents) indicated that this question was not applicable to them and 5% (one respondent) indicated that they were unsure or didn't know.

6. Downstream regulatory activities in focus

This chapter explores evidence on the use, impact and effectiveness of the ICO's downstream regulatory activities under the PSA. This draws on monitoring data, including issued reprimands and monetary penalty notices (MPNs), as well as evidence from a range of surveys, workshops and interviews with organisations from across central government and the wider public sector.

Summary of key messages

- Over the trial period approximately 77 reprimands were issued (July 2022 – June 2024). The majority of these (80%) were issued to the public sector. This **represented a notable shift in terms of the use of reprimands as part of the ICO's enforcement activity**. The trial period represented a 54% uplift in reprimands relative to the previous two-year period. There was however more limited use of other powers than initially expected, such as enforcement notices and warnings.
- Over the course of the trial, four monetary penalty notices were issued totalling £1.2 million. **In total, in the absence of the PSA, the ICO may have delivered fines totalling an estimated £23.2 million. The PSA resulted in a £22 million difference from this counterfactual.**
- Across the public sector, there is **widespread agreement that public sector fines punish the victims of data protection breaches** in the form of reduced budgets for public services. There was broad support for the view that a different regulatory approach is needed for the public sector, especially amongst central government DPOs. The wider public sector shared this sentiment but often for different reasons. They highlighted that fines have a direct impact on the delivery of frontline public services in the wider sector. Also, it was noted that **fines can have a disproportionate impact on smaller organisations and a distinct impact on the budget of devolved administrations**.
- Feedback from some organisations in the wider public sector, including local authorities, was more negative about the impact of the PSA. Several DPOs noted that it had made it **more challenging to make the case for resources or maintain an interest in compliance due to a more limited threat of fines**.

6.1. Downstream in context

In terms of downstream regulatory activities, these should be understood as prescriptive interventions ranging from corrections, such as warnings, to investigations and enforcement. At the outset of the PSA, the Commissioner's ambition in the context of downstream was:[58]

> "…an approach that will see a greater use of my discretion to reduce the impact of fines on the public. In practice this will mean an increase in public reprimands and the use of my wider powers, including enforcement notices, with fines only issued in the most egregious cases. However, the ICO will continue to investigate data breaches in the same way and will follow up with organisations to ensure the required improvements are made".

Over the trial period one of the objectives was to move away from fines as the primary sanction for public organisations. Instead, to see an increased use of reprimands and other regulatory tools to drive improvements in data protection standards. The delivery of this ambition is explored in the remainder of this chapter.

6.2. Enforcement activity during the trial period

6.2.1. Use of reprimands has seen a notable shift

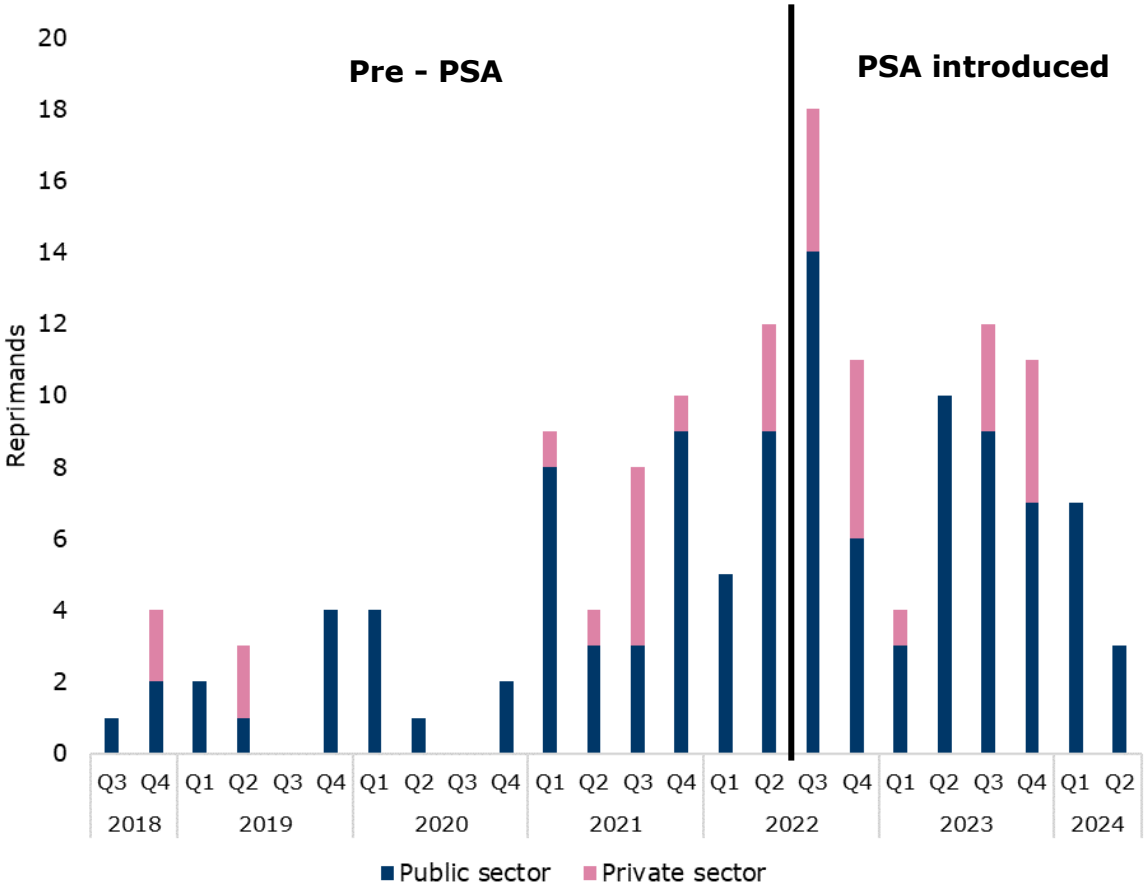
A total of 77 reprimands were issued during the trial period of the PSA. Approximately 80% of these (60 reprimands) were issued to public sector organisations and 17 to private sector organisations, as shown in Figure 5 below.

- In the two-year period prior to the trial (Q3 2020 to Q2 2022), 39 reprimands were issued to public sector organisations; meaning the trial represented a 54% uplift in reprimands relative to the previous two-year period. It is noted, however, that the comparator period will have been impacted by Covid-19.
- Notwithstanding the above Covid-19 point, the period Q3 2018 to Q2 2020 saw 15 reprimands issued to public organisations.

During the trial period, there was therefore a notable shift in terms of using reprimands as part of the ICO's enforcement activity.

[58] ICO (2022) *Open letter from UK Information Commissioner John Edwards to public authorities.* Available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/06/open-letter-from-uk-information-commissioner-john-edwards-to-public-authorities/ [Accessed: 18 September 2024].

Figure 5: Reprimands issued by quarter, Q3 2018 to Q2 2024



Source: ICO analysis.

6.2.2. Thematic trends in reprimands

The most common reason for reprimands to be issued during the trial was the unauthorised disclosure of personal data to a third party (with findings of infringement of articles 5 or 32 of the UK GDPR, or both), totalling 21 instances. This includes four instances in which a reprimand was issued to address shortcomings in organisations' procedures that resulted in carbon copy (CC) emails being sent to a group of recipients, thereby disclosing the personal data of other recipients.

A theme within these examples was cases involving the disclosure of personal data of ex-partners in a family context or in circumstances where parties are potentially in dispute. This perhaps suggests organisations' procedures are not suitably developed to accommodate such circumstances.

Reprimands issued to public sector organisations relating to subject access requests (SARs, with findings of infringements of articles 12 and 15 of the UK GDPR) totalled 13 instances.

The next most common type of infringement (eight reprimands) was in relation to issues concerning the accuracy of personal data held by data controllers. Each

of these infringements concerned data processed for either healthcare or criminal justice purposes and in each case there was an identified risk of harm arising from processing inaccurate personal data.

The unauthorised use of apps for sharing or storing personal data was also a recurring issue for public sector organisations throughout the course of the trial (six reprimands). This may be expected to continue to be challenging for organisations, as messaging apps offer an immediate solution to the issue of relaying information in a timely manner.

6.2.3. Monetary penalty notices impacted by the PSA

Turning to more onerous sanctions, over the course of the trial period, four MPNs were issued to public sector organisations, totalling approximately £1.2 million. Full details are provided in Table 6 below, showing estimates that absent the PSA:

- these four MPNs may have resulted in fines totalling £7.6 million; and
- seven reprimands may have instead been fines totalling £15.7 million.

In total this implies that in the absence of the PSA, the ICO could have delivered fines totalling an estimated £23.2 million.[59] The PSA therefore resulted in an estimated £22 million difference from this counterfactual.

A note on enforcement activity beyond the trial period

Following the end of the PSA trial period in June 2024, a number of investigations which had been ongoing during the trial have concluded, and where relevant are included in Table 6.

Reprimands have been issued to three data controllers within scope of the PSA (London Borough of Hackney, Chelmer Valley High School, The Electoral Commission). Of these, the London Borough of Hackney had initially been considered for a fine (of £1.35 million) but the fine was commuted to a reprimand in light of the PSA.[60] We estimate that The Electoral Commission would have received a fine of around £1 million had the PSA not applied.

In addition, in October 2024 a MPN was issued to the Police Service of Northern Ireland (PSNI) in relation to a data breach that occurred in August 2023.[61] It saw the application of the PSA to reduce the initially proposed fine amount of

[59] We note that these were proposed fines and would have subject to representations and potentially revisions as a result.
[60] The reprimand states that the Commissioner had also withdrawn two of his initial four findings of infringement. See: https://ico.org.uk/media/action-weve-taken/reprimands/4030344/20240705-lboh-updated-reprimand-with-redactions-1.pdf [Accessed 23 September 2024].
[61] This was the first fine to be calculated using the ICO's new Fining guidance. See https://ico.org.uk/about-the-ico/our-information/policies-and-procedures/data-protection-fining-guidance/ [Accessed 23 September 2024].

£5.6 million to £750,000.

On the whole, it has not been possible to observe distinct trends in the behaviour of public sector organisations over the trial period in the context of the data presented in Table 6. This is largely due to similar issues to those affecting complaints and breach reports, as explained in Section 3.3 above.

Additionally, the data in Table 6 should be viewed with consideration of lag effects. The investigations concluded during the trial period may relate to conduct that occurred before the PSA was announced. More generally, there is a time-lag between the occurrence of an infringement and the final regulatory outcomes. Therefore, it is important to note that the data likely shows limited direct cause and effect attributable to the PSA.

6.2.4. Other context to enforcement activity over the trial period

As already highlighted, at the outset of the trial it was intended that downstream activity would see a greater use of the ICO's wider powers, including reprimands and enforcement notices, with fines only issued in the most egregious cases.

In practice, this has led to a notable increase in reprimands but a more limited use of other powers than perhaps initially expected, such as enforcement notices and warnings. This is in part driven by the reactive nature of enforcement activity and the nature of cases coming through the enforcement pipeline. Though some enforcement notices and warnings were issued to public bodies during the trial.[62]

Additionally, it was 18 months into the trial before a MPN was issued illustrating the 'egregious' threshold.[63] This was again driven in part by the reactive nature of enforcement and the circumstances of cases. Once this was issued it served to dispel misconceptions amongst some that the ICO was no longer fining public bodies.

[62] For example see: ICO (2024) *Enforcement Notice and Warning Letter Home Office.* Available at: https://ico.org.uk/action-weve-taken/enforcement/home-office/ [Accessed: 18 September 2024].
[63] ICO (2024) *Ministry of Defence Monetary Penalty Notice.* Available at: https://ico.org.uk/media/action-weve-taken/mpns/4028623/ministry-of-defence-monetary-penalty-notice.pdf [Accessed: 18 September 2024].

Table 6: Monetary Penalty Notices impacted by the Public Sector Approach

Recipient	Circumstances	Reprimand or MPN	Proposed Fine	Final fine (if applicable)
Cabinet Office	Publication of names and addresses of more than 1,000 people announced in the New Year Honours list.	MPN	£500,000	£50,000
The Tavistock & Portman NHS Foundation Trust	CC email error revealing special category data.	MPN	£784,800	£78,400
Department for Education	Access to Learning Records Service database by third party for commercial purposes.	Reprimand	£10,030,000	
NHS Blood and Transplant	Development code released into live environment.	Reprimand	£749,856	
NHS Highland	CC email error revealing special category data.	Reprimand	£35,000	
Sussex Police	Use of an app on work mobile phones to record all incoming and outgoing phone calls.	Reprimand	£1,000,000	
Surrey Police	Use of an app on work mobile phones to record all incoming and outgoing phone calls.	Reprimand	£1,000,000	
Ministry of Defence	Disclosure of email addresses of people eligible for the MOD's ARAP programme.	MPN	£700,000	£350,000
Dover Harbour Board	Use of a social media distribution group for the purpose of combatting vehicle crime.	Reprimand	£500,000	
London Borough of Hackney Council	Cyber incident in 2020 that led to threat actors gaining access to and encrypting 440,000 files.	Reprimand	£1,350,000	
Electoral Commission	Cyber incident in which a threat actor accessed personal data of around 44 million people.	Reprimand	£1,000,000*	
Police Service of Northern Ireland	Spreadsheet error in which personal information of workforce was disclosed in response to an FOI request.	MPN	£5,600,000	£750,000
Total			**£23,249,656**	**£1,228,400**

Source: ICO analysis. Note the comment on timing in the text above. *Estimated.

6.3. Views on the use of monetary penalties in the public sector

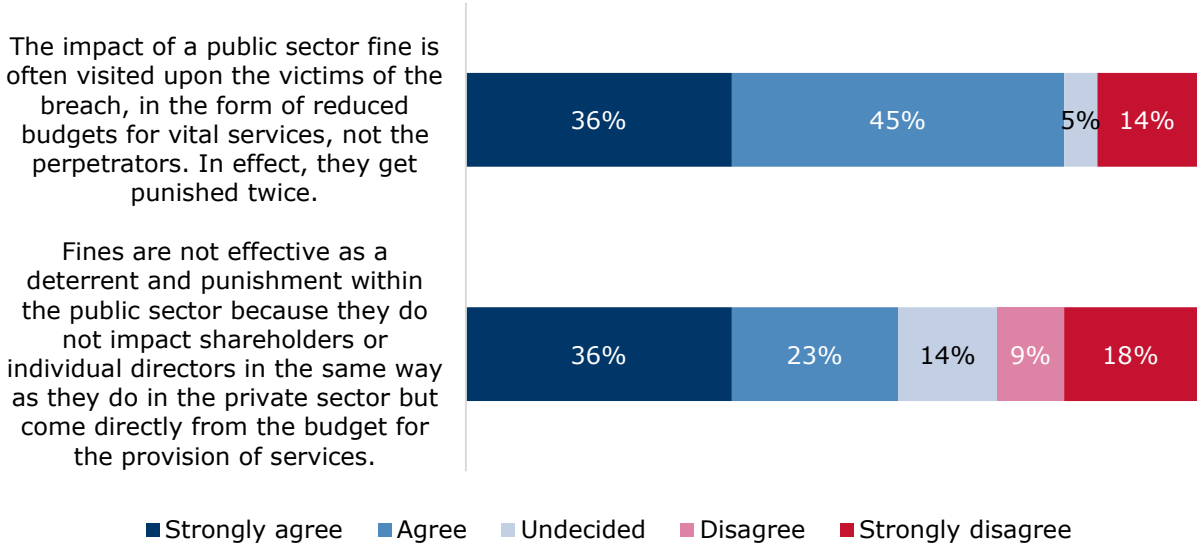
At the outset of the PSA, the Commissioner expressed the following rationale for the reduced focus on monetary penalties:[64]

> *"…impact of a public sector fine is also often visited upon the victims of the breach, in the form of reduced budgets for vital services, not the perpetrators. In effect, people affected by a breach get punished twice".*

There was broad support for the view that a different regulatory approach is needed for the public sector, especially amongst central government DPOs. In the central government DPO survey, as shown in Figure 6:

- around four in five (18 respondents) agreed that public sector fines impact victims of a breach in the form of reduced budgets for vital services; and
- the majority of respondents (59%, 13 respondents) agreed that fines do not impact the public sector in the same way as they do in the private sector but come directly from the budget for provision of services.

Figure 6: Respondents' attitudes to fines



Source: ICO analysis (n=22).

Across the wider public sector, organisations highlighted in the case study interviews and the DPO workshop that fines have a direct impact on the delivery of frontline public services:

[64] ICO (2022) *Open letter from UK Information Commissioner John Edwards to public authorities.* Available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/06/open-letter-from-uk-information-commissioner-john-edwards-to-public-authorities/ [Accessed: 18 September 2024].

"Were a fine applied, this would have to come out of our funding allocation from the department and would have direct implication on services we could provide to the public".

"A fine for us would mean, we could no longer invest in supporting a victim support group or tackle a particular type of crime. We are already tight on budget".

Some public organisations noted that fines could also have a disproportionate impact on smaller organisations, and have the potential to doubly impact people who seek the organisation's services.

Public sector organisations often serve a diverse range of objectives and customers. The impact of fines largely depends on operational context, which varies across public sector bodies. For example, DWP noted (see Annex E.3) that receiving a fine would not have directly impacted on frontline services, as not serving customers would not be an option given its statutory obligations.

"DWP is a demand led organisation. If the number of unemployed or seeking work goes up, our costs go up. This money would need to be found somewhere -- even if it came out of our budget, which ultimately comes from the Treasury. We couldn't not serve our customers".

Evidence from the DPO survey indicated that fines also have a distinct impact on the budget of devolved administrations:

- One DPO felt that fines in devolved administrations take money off public services in that nation, as these are paid to HM Treasury with no ring-fencing for devolved spend.
- This reflects similar feedback provided by the devolved administrations, where another DPO commented that monetary fines on central government departments are 'recycled' back into the government, whereas fines paid by devolved administrations are not and result in reduced budgets.

Some DPOs voiced concerns that limiting the impact of fines could have a detrimental impact on the influence of data protection roles within their organisation, with negative consequences for compliance (discussed further in Section 7.3). However, data protection compliance in the public sector is likely to be affected by a complex landscape of factors, of which downstream regulatory activities is only one part.[65]

[65] For example, spillover or 'general deterrence' effect, as opposed to the 'specific deterrence' effect on the organisation found to be in breach, which early ICO evidence suggests may also arise

6.4. Other impacts from limiting the use of fines

Feedback from some organisations in the wider public sector, including local authorities, was more negative about the impact of the PSA.

- Several DPOs noted that it had made it more challenging to make the case for resources or maintain an interest in compliance due to a more limited threat of fines.
- Some DPOs noted that their resources are very constrained and that limiting the risk of a monetary penalty from the ICO is not necessarily a good thing.
- One DPO indicated that they had not made the approach widely known, as keeping staff thinking they could be fined supports compliance.

Other DPOs commented that:

"Reprimands appeared to be sneered at by expert groups"

"Lack of sufficient resources trumps everything. It is difficult to be proactive in these circumstances".

"I don't think the approach has had a positive impact. There's a logic in not fining public authorities, because we've got no money, and the money only goes back into another area in the same pot. But you've undermined that we're all accountable to the ICO for data protection".

Process suggestions relevant to downstream activities

In addition to the point highlighted above, the following suggestions were made by DPOs:

Holding more informative sessions about the approach to increase awareness of the PSA.

A more tailored approach to communication with public sector bodies: better understanding the nuances of public sector processing (as the approach applied is often generic across the public sector) and providing more direct assistance to public sector bodies.

from reprimand lesson learning. See ICO (2024) FOI Upstream Evaluation: Interim Findings. Available at: https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/impact-and-evaluation/evaluations/foi-upstream-evaluation-july-2024/ [Accessed 12 September 2024].

7. Exploring the impact of the PSA

This chapter explores the main impacts of the PSA trial in terms of changes to:

- levels of knowledge and awareness of data protection;
- changes to data protection processes and procedures;
- the status of the data protection with public sector organisations;
- perceptions of the ICO; and
- other impacts not captured elsewhere.

This builds on the upstream and downstream activity outcomes discussed in the previous two chapters.

Summary of key messages

- Although **net sentiment was positive** there were **mixed views on how the PSA had impacted knowledge and awareness**. However, since the majority of those engaged in the research are data protection professionals, they were likely to score their baseline knowledge relatively high.
- Despite these mixed views, it is clear that **the PSA has led to information and knowledge transfer given that nearly half of the surveyed central government DPOs reported enhanced or new processes and procedures as a result of the PSA**. The sharing of lessons learned through published reprimands was often cited as a catalyst for change. There was tangible impact evidence of how upstream and downstream regulatory activities can work together to drive change.
- The **impact of the PSA on the status of data protection varied between the wider public sector and central government, likely reflecting the central government focus of the targeted upstream activity**. Across the wider public sector, there were concerns around erosion of influence of data protection professionals due to a perceived threat of ICO enforcement as low. In contrast, central government DPOs reported that support from senior leadership had increased with the PSA, and there was a majority view that professional influence had remained the same or increased.
- There were **positive reputational impacts for the ICO**, with the PSA viewed as taking a more collaborative and proactive approach.
- However, some feedback reported **unintended behavioural effects in the wider public sector resulting in the de-prioritisation of data protection issues in some instances**. Some of these effects may have been **exacerbated by a perceived lack of clarity** at the outset which led to the misconception that the ICO was no longer fining, or even regulating, public bodies, which was later mitigated.

7.1. Levels of data protection knowledge and awareness

While the net sentiment was that the PSA had positively impacted knowledge and awareness of data protection in the public sector, views were mixed. The survey of central government DPOs found that:

- nearly half (45%, 10 respondents) reported a positive impact on levels of knowledge and awareness in their department;
- a third (32%, seven respondents) noted no change in levels of knowledge and awareness; and
- 5% (one respondent) noted a negative impact on knowledge and awareness.[66]

This was consistent with feedback received from the wider public sector, where around half of consultees in workshops with organisations in the devolved nations noted that the PSA had not had an impact on levels of knowledge and awareness in their organisation. For many of these respondents, this was due to their organisation already having strong processes and procedures in place. Some of the reasons provided included:

- the organisation already had a good working relationship with their ICO contacts prior to the revised approach;
- there was already good awareness and respect for data protection;
- data protection processes were already established; and
- external factors have had a greater impact than the PSA (eg Brexit, Covid-19, and media attention on data protection issues).

Respondents from across the three devolved networks engaged via the research, provided the following examples of positive impacts that the PSA had on their organisation's knowledge and awareness of data protection:

- the organisation had ingrained data protection principles more widely, with continued training and knowledge updates building on the ICO's upstream activity;
- understanding bad experience in one sector had been helpful for learning in others; and
- increased interaction with the ICO had an impact on the general staff awareness of data protection matters.

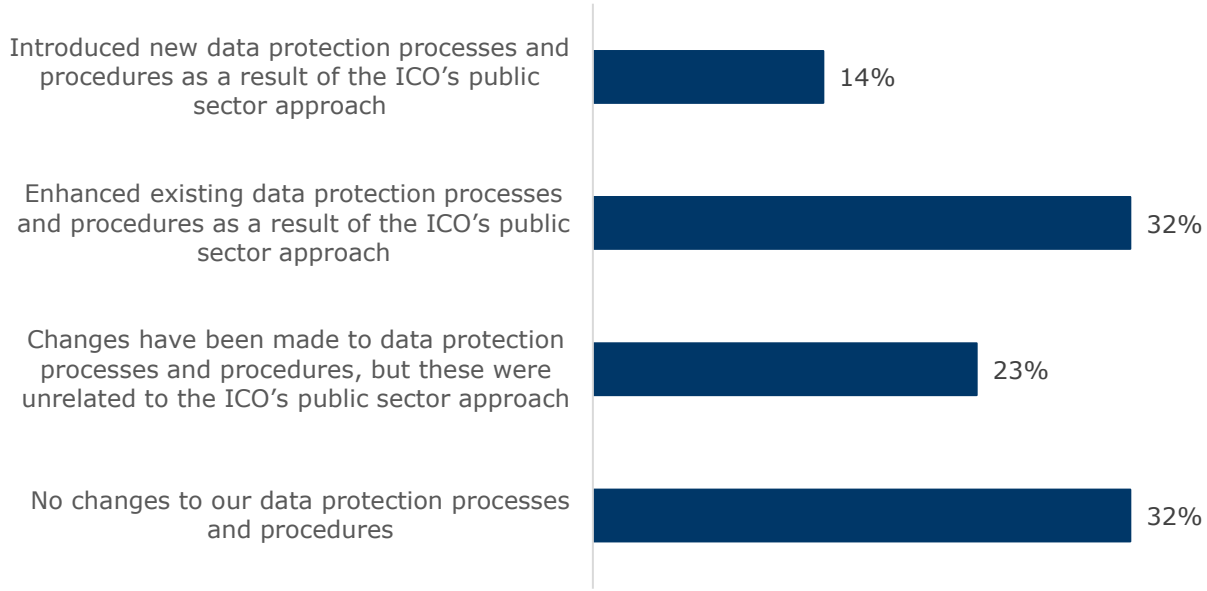
7.2. Changes to data protection processes and procedures

At the end of the trial, central government DPOs were asked whether they had made changes to their departments data protection processes and procedures as a result of the approach. Nearly half of central government DPOs had enhanced

[66] Note that the remaining 18% (four respondents) answered 'don't know' or 'unsure'.

or introduced new data protection processes and procedures as a result of the PSA, as shown in Figure 7 below.

Figure 7: Have you made any changes in your organisation's data protection processes and procedures as a result of the ICO's public sector approach?



Source: ICO analysis (n=22).

In so far as central government DPOs provided further detail, these changes included:

- updates to guidance products in response to published reprimands;
- updates to training activities; and
- regular briefings to their department's COO about data protection activities.

The sharing of lessons learned through published reprimands was often cited as a catalyst for change in central government departments. For example, DWP highlighted they had made specific improvements to processes in response to a data breach at a different public authority that had been reported on by the ICO. They strengthened guidance on redaction and processes around giving out information in response to FOIs. DWP noted that some of these changes to practices "were used as a model for other departments" illustrating the ripple effects and wider learning that often accompanies actions of this nature.

To capitalise on sharing best practice and avoiding similar breaches, published reprimands were discussed in the cross-government COO network. To monitor actions that government departments had taken in response to specific reprimands, a series of surveys were circulated to members of the cross-

government COO network over the trial.[67] These surveys focused on practices in government departments, as well as learnings from published reprimands. A summary of some of the actions taken by departments in response to a reprimand[68] are discussed below. This provides tangible impact evidence of how upstream and downstream regulatory activities can work in synergy to drive change.

Actions taken by COO network members in response to DWP reprimand

In January 2024, members of the cross-government COO network were asked to report on what progress had been made against plans to improve data protection processes. This followed up on a previous issued survey (from July 2023), where departments were asked what plans they intended to implement in response to a DWP reprimand where key information was not redacted, resulting in a data breach. In response to this:

- seven respondents from 10 had made changes to internal data protection processes. Responses highlighted new engagement procedures on the procurement of IT systems; ensuring that data protection staff have oversight of redaction cases and updated departmental policies on redaction;
- four respondents from 10 carried out testing of existing processes. This included a full review of data protection policies; a deep dive into the department's use of redaction technologies and an internal audit of high risk areas;
- four respondents from 10 made updates or changes to DPIA procedures. This included issuing of new templates; the introduction of bite-size training videos and the review of existing DPIAs;
- four respondents from 10 made updates to staff training and carried out awareness-raising activities. This included using reprimands as case studies in training materials; ensuring that staff responsible for redaction undertake additional training and the updating of training materials to reflect departments' redaction policies and
- two respondents from 10 provided no update on plans to improve data protection processes in response to the DWP reprimand.

Interviews were conducted with a number of organisations that had received a reprimand or MPN as a result of a data breach to understand what change measures they had put in place. However, these changes were often described

[67] The 11 departments participating in the COO Network are: Cabinet Office, CPS, DfE, DHSC, DVLA, DWP, FCDO, HMRC, Home Office, MoD and MoJ.
[68] ICO (2022) Reprimand issued to DWP. Available at: https://ico.org.uk/media/action-weve-taken/reprimands/4023126/dwp-reprimand.pdf [Accessed 13 September 2024].

as a direct response to the realisation that they'd had a UK GDPR infringement, rather than being implemented due to the ICO or the PSA, or both.

"We immediately started a lot of work. When we actually received the reprimand, there was very little in the reprimand that we'd not already addressed".

Examples of the types of measures put in place by organisations are explored in the case studies in Annex E. Below is an extract from a case study illustrating how realisation of the infringement primarily drove changes but that there are additionality aspects linked to time and quality attributable to the ICO.

Case study: Ministry of Defence (MoD)

MoD implemented a number of changes in response to the BCC breach in 2021, including:

- **increased focus on information management systems**, more upfront consideration of potential risks and mitigations;
- speaking to staff and **changing internal policies** to raise awareness and that use of the BCC field carries inherent risk of human error;
- **referencing the breach in training** (delivered to staff annually) and lessons the MoD has had to learn from it; and
- **seeking to increase awareness and understanding amongst staff** that data protection and information management is needed and is not optional (or an issue only to be addressed by the data protection team).

MoD also recalled receiving a reprimand for a backlog in responding to SARs and noted that this had been helpful in driving focus in the department and getting the resources in place to resolve the issue. MoD indicated that they were able to invest in a single workflow assessment across the organisation and improve both front and back-end systems as a result. This had also started to drive savings that could be reinvested elsewhere.

MoD highlighted that the ICO was not the only driver for the changes that had been implemented, but that it had been a catalyst for pace and emphasis. MoD noted that *"it focused attention within the department and whole flurry of activity arose as a result of the incident".*

7.3. Impact on the status of data protection within the public sector

There were mixed views around the impact of the PSA on the standing and status of data protection within public sector organisations. This varied widely between the wider public sector and central government.

Across the wider public sector, there were concerns around the erosion of influence of data protection professionals with senior management as a result of the changed focus of downstream regulatory activities. This point regularly came up in feedback from the wider public sector during the trial period. This was often the case in the health and policing sectors where one DPO commented that:

> "[The] consequences of non-compliance are not taken as seriously under the current approach and that…data protection is perceived to have become easier and less important at a senior level…making it harder to push the importance of messaging to senior policing colleagues".

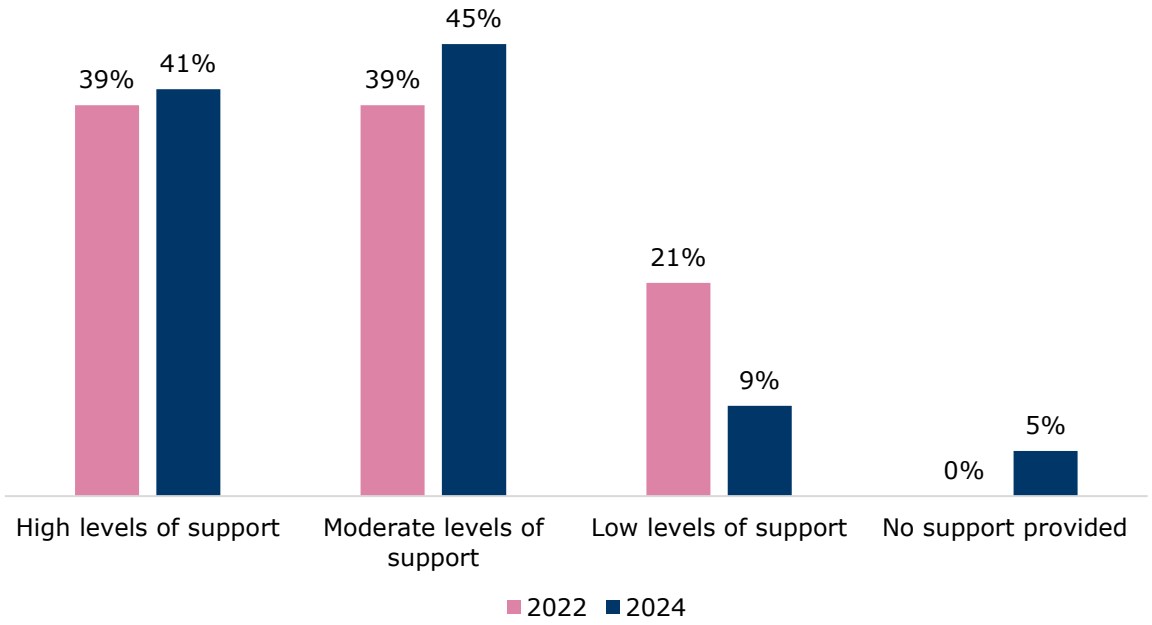
This point also came up in anecdotal feedback, including from a DPO in a central government department. This feedback described internal action on data protection issues as "an uphill battle" and claimed that the department's internal legal advice undermines the PSA by describing the threat of ICO enforcement as low. Feedback from a health trust also suggested that the new approach had done "more harm than good", particularly where staff are under-resourced and deal with high volumes of special category data.

Another DPO commented that:

> "There is more leniency and acceptance, which may have resulted in a decreased sense of urgency when addressing any data protection matters. I feel that although data protection teams are likely to have been less pressured over the past few years, the data protection field has been deprioritised from organisations as a result".

However, this differed from the overall experience of DPOs within central government departments. The central government survey found that (as shown in Figure 8) around 86% of DPOs (19 respondents) reported high or moderate levels of support from senior leadership, relative to 78% in 2022.

Figure 8: Levels of support from senior leadership in driving compliance



Source: ICO analysis (n=22).

The following quotes from the DPO survey illustrate the variety of experiences reported by central government DPOs:

"The work of the DPO is supported right across Director level within the organisation".

"..the DPO is included in a wide range of activities and briefings. Suggested improvements are normally actioned although I don't win every battle".

"I have sufficient support from Perm Sec's to be effective as DPO".

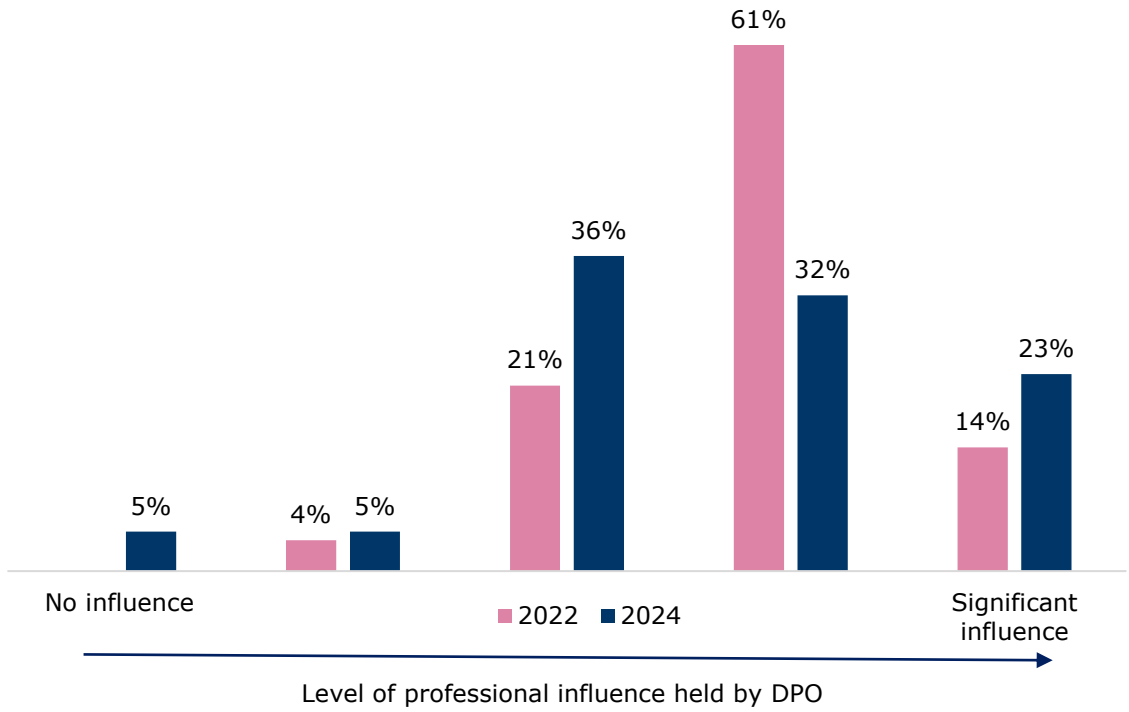
"As part of the SLT, I have good influence but it is still seen as a nuisance by some".

"I am often involved in major projects, but sometimes only after the event".

"The DPO does not weigh in to any business decisions, at a strategic level, and instead is a reactive function to try and mitigate risks once they have escalated so far, other roles in the business don't know how to handle the matters".

Central government DPOs were also asked about the level of professional influence linked to the role of the DPO. The bulk of respondents reported that DPOs have medium to high levels of influence, as illustrated in Figure 9. Whilst those reporting significant influence had increased since 2022, there was a moderate decline overall towards less influence over the trial period.

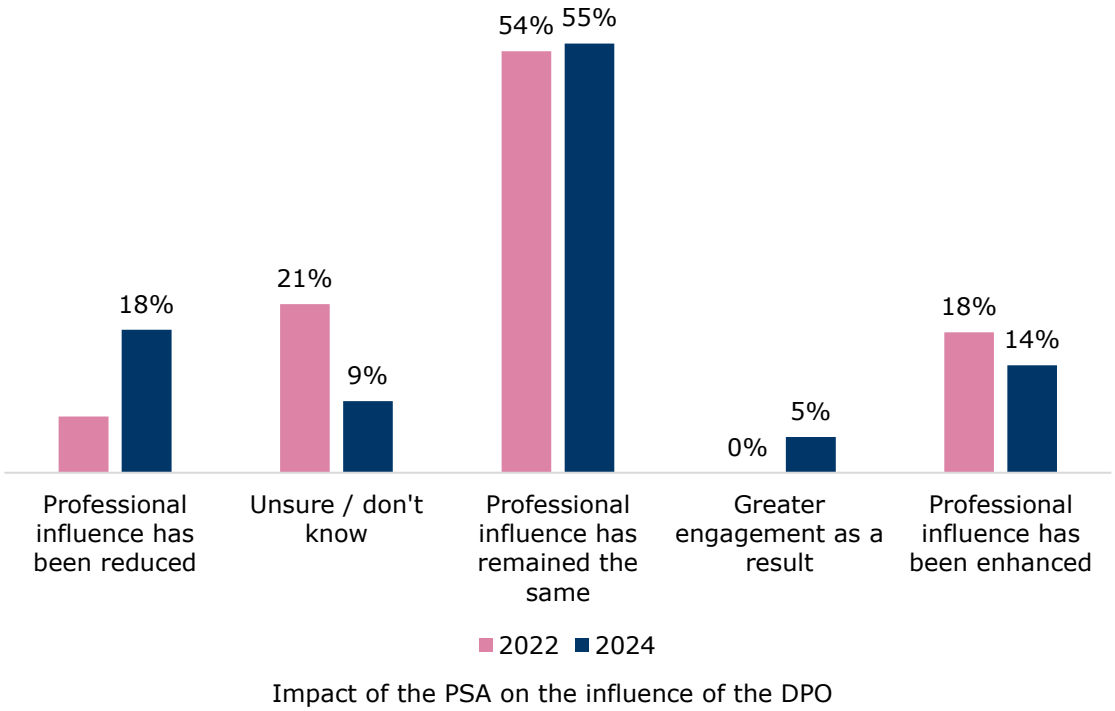
Figure 9: Level of influence of DPOs within central government departments



Source: ICO analysis (n=22).

There were mixed views when central government DPOs were asked how levels of professional influence have been affected by the trial, as shown in Figure 10. Over half of central government DPOs felt that there had been no change in their overall level of professional influence (broadly consistent with expectations when asked in the baseline survey in 2022); 14% felt that their level of professional influence had increased; and 18% felt their influence had been reduced.

Figure 10: Impact of public sector approach on levels of professional influence



Source: ICO analysis (n=22).

7.4. Perceptions of the ICO

Generally, amongst public sector organisations it was perceived that the PSA had resulted in a more collaborative and proactive approach, with positive reputational impacts for the ICO. Amongst central government DPOs:

- 41% (nine respondents) had a more positive view of the ICO;
- 32% (seven respondents) had not changed their view;
- 9% (two respondents) viewed the ICO more negatively; and
- 14% (three respondents) were unsure.

Some of the more positive responses highlighted a more constructive relationship with the ICO around sharing lessons and best practice. Other responses highlighted that the approach "demonstrates that the ICO is responsive to the financial pressures faced by the public sector".

7.5. Impact constraints

Central government DPOs pointed to a range of underlying challenges. The most common challenges highlighted related to resourcing or budget constraints and operational delivery pressures. In some instances, DPOs thought that these pressures had increased the risk of human errors occurring. Other challenges noted by a smaller number of DPOs included issues associated with the management and governance structures for driving change (referenced by three

organisations), understanding of complex compliance requirements (two organisations), and pressure to implement new and developing technologies without fully understanding the associated risk (one organisation). Commenting on these challenges, one DPO stated that:

> "Data protection is complex, hard to understand and therefore burdensome. It is competing with day to day delivery. It is viewed as an obstacle rather than an enabler".

Anecdotal feedback from some DPOs suggests that the interaction of the PSA with these other constraints may have resulted in some unintended behavioural effects in the wider public sector, resulting in the de-prioritisation of data protection issues in some instances.

As noted above, there were mixed views amongst central government DPOs and those in the wider public sector on the impact of the PSA on the standing and status of data protection within public sector organisations. Those in the wider public sector raised some concerns around the erosion of influence of data protection professionals with senior management. The feedback highlighted that this was the result of limiting MPNs, which led senior officials to see the threat of enforcement action from the ICO as low. This could have implications for the compliant use of novel technologies in the wider public sector, as highlighted by one DPO below:

> "In the landscape of tech innovation and novel use of sensitive data in policing there is a particular need to ensure that there is appropriate senior, experienced staff advising on these issues and implementation of technology, and if they are found to not be taking this person's advice or making an individual who is not qualified in data protection issues as the responsible individual that there are consequences".

Some of these issues may have been exacerbated by a lack of clarity on the scope of the PSA and what constitutes an 'egregious' data breach. During the trial this led to a perception in some part of the public sector that the ICO was no longer fining public bodies. However, feedback received towards the end of the trial suggested this issue had largely been resolved due to a number of MPNs been issued to public bodies.

Whilst acknowledging the above point on novel technologies, overall across the evidence base there was limited evidence on the PSA impacting innovation, the adoption of technologies or the compliant sharing of data within the public sector.

Mitigating constraints

To help mitigate and overcome the constraints highlighted, DPOs provided suggestions related to enabling impact. These are summarised below.

Process suggestions around enabling impact

Feedback across the review surveys and workshops suggested that greater consideration should be given to the impact of regulatory activities on different organisations, the nature of their role and how regulatory enforcement can impact on service capacity.

Wide-ranging suggestions were made about alternate ways to hold the public sector to account to improve standards. It is highlighted that both the need for these measures and their feasibility under current legislation may vary. Suggestions included:

- a requirement for public sector bodies to **engage in audits** with the ICO;
- asking accounting officers to appear at Public Account Committee sessions for the most egregious breaches to **explain to the Commissioner what mitigating measures they have put in place**;
- introducing an **annual return for public sector organisations**, signed off by the CEO, to improve accountability and visibility for data protection standards; and
- **reallocating funds from fines to improve data protection practices**: using the pot of funds from fines for grants or funding specifically for data protection resources to help to show that improvements are being made without taking away public resources.

Other suggestions include exploring a two-tier system, where public sector bodies could still be fined unless they could demonstrate that mitigating measures have been put in place.

8. Review conclusion and learnings

8.1. Conclusion

Trial outcome isn't a straightforward success or failure, instead, it involves multiple layers

The evidence presented in this review shows that the PSA was an ambitious and challenging trial to deliver over two years and with a limited lead-in time. The focus of this review was on the impact and learnings from the trial and these are multi-faceted. The trial's outcome isn't a straightforward success or failure. Instead, it involves multiple layers: notable achievements, areas with more to do, unexpected challenges, and unintended consequences.

When the Commissioner announced the trial via an open letter in June 2022, it sent a clear message that the ICO is a modern and forward-thinking regulator, unafraid to innovate transparently. It is easy to stick with the status quo, while investigating and acting on new approaches shows a commitment to pragmatic, proportionate and effective regulation focused on making a difference. Changes of this nature will always be open to criticism, and the review shows that some aspects of these were valid.

The two primary strands of the PSA - raising data protection standards with an enhanced use of influencing and educating regulatory activities (upstream) and enforcing the law using a wider range of regulatory tools and powers (downstream) – have had varied outcomes in different contexts.

Upstream activities have driven change, though this was limited to central government

The upstream activities in a central government context, primarily facilitated by the COO network engagement and the publication of reprimands, have driven real change in terms of enhancing data protection standards. However, beyond central government in the wider public sector the impact has been more limited. This should not be surprising given the focus of upstream activities on central government, but it has likely led to some unintended effects in the wider public sector, which are explored more below.

Given the nature of a trial period involves testing a concept, it was reasonable to concentrate on central government until the trial’s outcomes were clear. However, to better manage expectations, the differing approaches to central government and the wider public sector could have been more clearly communicated at the outset. Although all public sector organisations had access to the published reprimands, awareness was lower in the wider public sector, and challenges regarding access and ease of use were also noted.

Reduced impact of fines coupled with a notable increase in reprimands, but more to do

There has been a shift over the trial period that has seen the ICO enforcing the law using a wider range of regulatory tools and powers. This has involved greater use of the Commissioner's discretion to reduce the impact of fines on the public, resulting in a total of £1.2 million in fines instead of a possible estimate of £23.2 million absent the PSA. In practice, this has led to a notable increase in reprimands but a more limited use of other powers, such as enforcement notices, than initially suggested. This indicates that there is still work to be done in fully utilising the spectrum of regulatory powers and tools.

This strand of the PSA encountered implementation challenges that have likely contributed to this need for more development. These challenges included:

- misinterpretation of the PSA messaging leading to the misconception that it was solely about not fining public organisations;
- slower-than-anticipated adaptation of internal processes and establishment of engagement to support the new approach; and
- an extended time period before it was possible to illustrate the 'egregious' threshold with an example.

Effect on the status of data protection varied with some unintended consequences

Overall, the PSA has been impactful. As already highlighted, it has driven changes that have increased data protection standards, albeit across a smaller population than anticipated. There is clear evidence of how upstream and downstream regulatory activities can work together to drive change and the ICO has experienced positive reputational impacts. The PSA's effect on the status of data protection varied, likely due to the central government focus of the targeted upstream activities. An unintended consequence in the wider public sector was concerns about the erosion of influence among data protection professionals. This stemmed from a perceived low threat of ICO enforcement and fears of possible de-prioritisation of data protection issues in some instances.

Need for accountability to deliver improvements on all sides

At the beginning of the trial, the Commissioner noted the need for accountability to deliver improvements on all sides. The ICO demonstrated this accountability by establishing a monitoring and review programme to accompany the trial. The PSA was intended 'not to be a one-way street', expecting greater involvement from the public sector, including senior leaders, with investment of time, money and resources in 'ensuring data protection practices remain fit for the future'. While engagement within central government has notably increased, clear evidence of financial and resource investment is less apparent. This reciprocal

expectation is less applicable in the wider public sector due to the lack of targeted engagement.

8.2. Learning points for consideration

The learning highlighted here summarises themes presented throughout this review report. This includes some of the suggestions that were captured via the primary research to help to improve the future effectiveness and efficiency of the regulation of public sector organisations and wider learnings for the ICO.

Table 7: PSA learnings for consideration

Topic	Detail
Scope and parameters of the PSA	A need for clarity and clear parameters on the scope of the regulatory approach upstream and downstream. The review also received feedback around amending the scope of the approach to focus on areas that present the highest risk and where the ICO can have the biggest impact.
Utilising the full spectrum of regulatory tools and leveraging greater public sector accountability	Ensure mechanisms are in place to enhance the use of the full spectrum of regulatory tools and powers, where this is appropriate. This includes the potential for greater use of enforcement notices and warnings. Suggestions were received from stakeholders about exploring alternate accountability mechanisms for the public sector which the ICO could investigate further.
A more tailored regulatory approach	The trial was viewed as a one-size-fits-all approach by some and it was felt that greater consideration could be given to the impact of regulatory activities on different organisations, the nature of their role and impacts of enforcement. However, this does need to be balanced against the need for effective enforcement. Recognising the pressures on public sector resources was also a common theme. The need for the ICO to better understand that public sector organisations are trying to do the best they can with limited resources was highlighted. To respond to this, it was suggested that the ICO could offer more guidance and support to help bodies with limited resources avoid breaches.
External communication of the PSA and its supporting tools	To enhance clarity it was suggested having a central resource on the ICO's website about the approach, including its supporting tools. Also holding more information sessions about the approach to increase awareness and mitigate some misconceptions.

	A more tailored approach to communication with wider public sector organisations to allow better understanding of the nuances of public sector processing (as the approach applied is often generic across the public sector) and providing more direct assistance to public sector organisations. Improving access, searchability and retention on the ICO website of published cases and reprimands. It was also suggested that there could be improvements to the ways in which reprimands, cases and decision notices are shared, including accessibility considerations.
Enhanced internal processes to support implementation and insight generation	A lack of guidance on the practical application of the PSA and definitions of key terminology was cited by ICO staff as a key challenge in the implementation of the PSA. Internal consultees highlighted a need for enhanced processes to assist in streamlining the approach: • procedural steps for implementation and clarification on how the PSA fits into the ICO's fining guidance; • the level of detail, length and processes for publication of reprimands to increase consistency and certainty; and • key terminology (eg clear definitions of 'egregious' and of the types of organisations considered in scope). Further enhancements to the categorisation of internal data to allow more efficient generation of insights linked to public sector organisations.
Research to understand public sector organisation perspectives and monitoring	Beyond the research set up to support the monitoring and review activity of the trial, there is a need to continue research with public sector organisations. This is at both a central government and wider public sector level, to allow effective targeting of interventions and to monitor change and impact. It should be explored how this could link to the ICO's Data controller study.

Source: ICO analysis.

ico.

Information Commissioner's Office