Post-implementation review annexes: Public sector approach trial

September 2024

Information Commissioner's Office

Contents

Annex A: Detail on review approach and methodology

This Annex provides further details on the overall approach to the review, expanding on the information within Section 2 in the main report. This includes providing further detail on the timeline for the review, the key research questions, and the theory of change for the PSA.

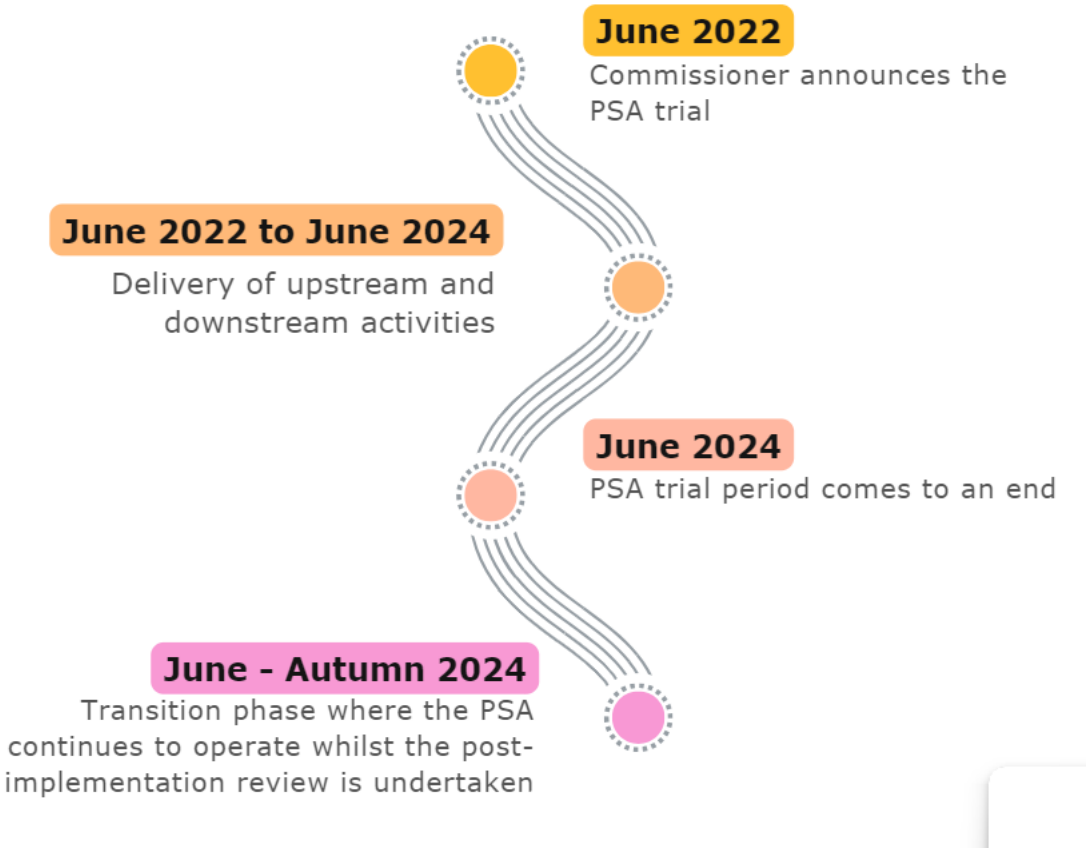
A.1 Review overview and timeline

This post-implementation review follows the standard set by HM Treasury's Magenta Book[1] and Green Book.[2] As set out by HM Treasury, ex-post impact analysis should be useful, credible, proportionate and tailored around the needs of various stakeholders, such as decision makers, users, implementers and the public.

The review has been delivered using both process and impact approaches. This considers design and implementation learning points as well as the difference the PSA has made in terms of impact. The PSA was announced as a two year trial by the Commissioner in June 2022 and came to an end in June 2024. The PSA is currently in a transition phase, continuing to operate as normal whilst the post-implementation review is undertaken [3].

[1] HM Treasury (2020) *Magenta Book*. Available at: https://assets.publishing.service.gov.uk/media/5e96cab9d3bf7f412b2264b1/HMT_Magenta_Book.pdf (Accessed: 12 September 2024).
[2] 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: 12 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: 10 October 2024].

Figure 1: PSA timeline



Source: ICO analysis.

A.2 Review questions

The review questions that we have used are set out in Table 1 below. These were not intended as an exhaustive list but provided an overall guide to our approach.

Table 1: Review questions

Process – what can be learned from how the PSA was delivered?	**Impact – what difference has the PSA made?**
Was the PSA delivered as intended internally and externally?	Did the PSA achieve the expected outcomes/impact? To what extent?
What worked well, or less well, for whom and why? What could be improved?	What would have happened anyway?
What can be learned from the delivery methods used?	To what extent can the impact be attributed to the change? How confident can we be that the PSA caused the observed changes?

Were there any unexpected or unintended issues in the delivery of the PSA?	How has the context and external factors influenced outcomes?
How has the context influenced delivery?	Has the PSA resulted in any unintended outcomes?
How did external factors influence the delivery and functioning of the PSA?	To what extent have different groups been impacted in different ways, how and why?
	What generalisable lessons have we learned about impact?

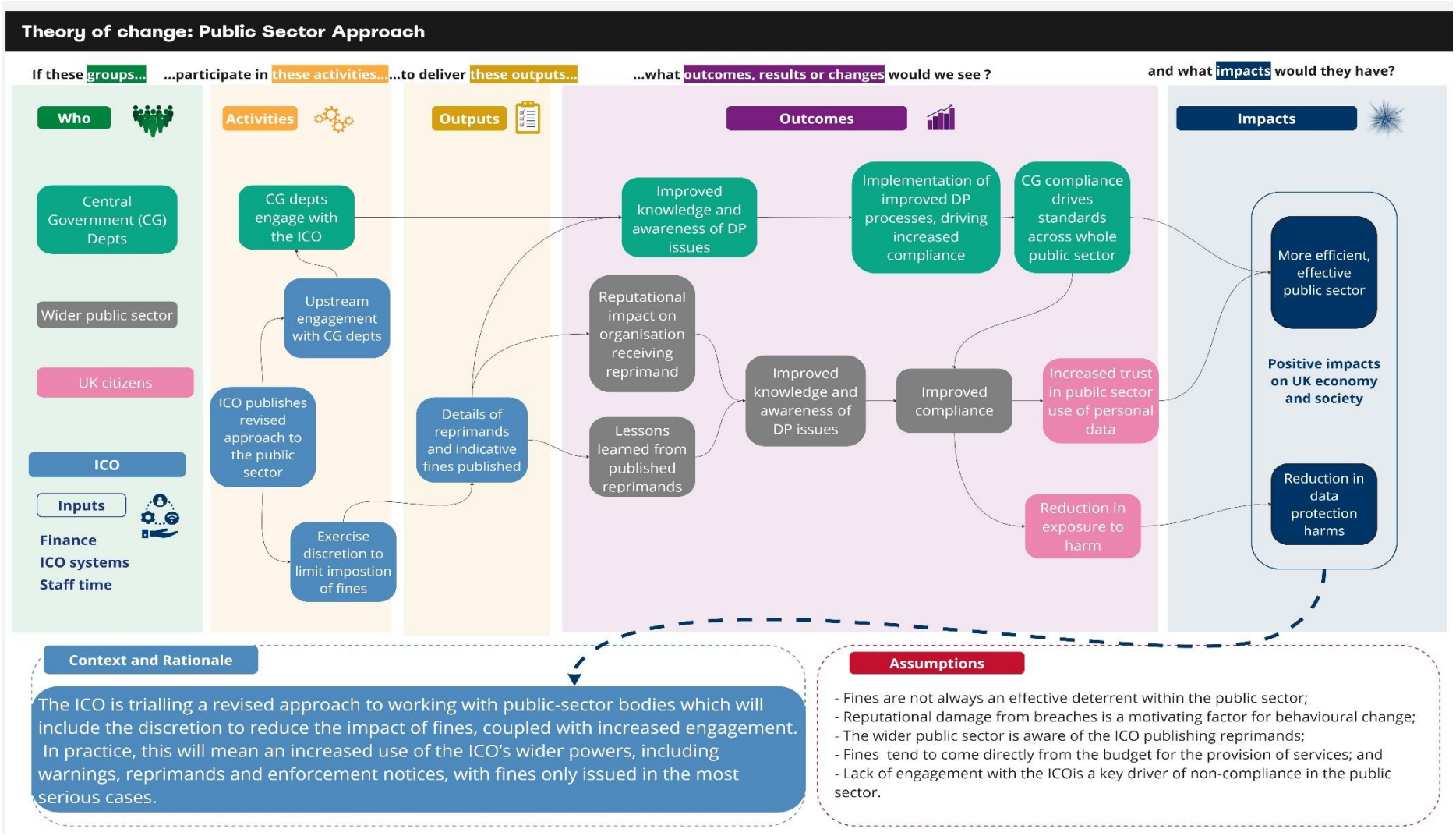
Source: ICO analysis.

A.3 Theory of change

Figure 2 explores the theory of change for the ICO's PSA. A theory of change illustrates how and why the desired change is expected to happen in a particular context. It does this by outlining the assumptions upon which the intervention is based, examining the wider context, setting out all the steps of the intervention, and outlining how these were expected to contribute towards achieving the desired outcomes.

Impact, linked to the rationale for the intervention, is often the most difficult aspect to measure since it will occur over a longer period of time and will be influenced by other external factors. Section 2 in the main report provides further details regarding the challenges in measuring the impact of the PSA and approaches we have deployed to try to mitigate these.

Figure 2: Theory of change for the PSA



Source: ICO analysis.

Annex B: Wider public sector data protection context

This annex chapter provides a summary of trends in data protection activity drawing on evidence on data protection complaints made and personal data breaches reported to the ICO between January 2021 and June 2024.[4]

Summary of key messages

Data protection complaints

- The number of data protection complaints received varied throughout the period from a low of 2,614 in Q4 2022 to a peak of 3,749 in Q2 2024. This variation was seen in all six sectors under consideration.
- The proportion of data protection complaints resulting in no further action remained stable pre and post implementation of the Public Sector Approach (around 60% of data protection complaints). In both periods, almost all other cases ended in informal action (around 40%).
- The top ten most complained about departments accounted for between 74% and 78% of all data protection complaints in each year under consideration.

Personal data breaches

- The number of PDBs reported to the ICO fluctuated over the period, dipping to a low of 1,046 in Q2 2022 and rising to a peak of 1,434 in Q2 of 2024.
- Post implementation of the Public Sector Approach, the average number of reported breaches increased by 11% per quarter.
- The proportion of personal data breaches reported reaching specific outcomes remains similar pre and post implementation of the PSA. In both periods around three-quarters resulted in informal action being taken, just under a tenth resulted in an investigation being pursued while the remainder resulted in no further action.

It is important to note that insights from the data on the impact of PSA are likely to be limited as:

- Complaints and breaches often fluctuate considerably, and it is likely that this is driven by a range of factors. Fundamentally, complaints or reported breaches may or may not relate to actual infringements of the law, and whilst the root causes can often be influenced by the organisation in

[4] The analysis in this paper refers to calendar year quarters. Quarter 1 (Q1) refers to January to March, Quarter 2 (Q2) to April to June, and so on.

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.

- The focus of enhanced regulatory upstream activity was limited to central government departments for the two-year pilot. Impacts are generally long-term in nature. Progress will first need to be made against shorter term outputs and intermediate outcomes, by way of improved data protection processes, before long term benefits can be observed in the data.[5]
- Questions about timings also contribute to the challenge. For example, the timing of when the cause of an event occurs, when the event itself occurs, when the event is detected by the organisation, when the event becomes known to the ICO and when the ICO reports the event are not the same point in time. It is often the case that large events that are reported in one year actually happened in previous years, and the current state will change as more becomes known and reported.
- There are a range of wider data quality issues which should be kept in mind when considering the analysis. These are described in Section 2.2 of the report.

B.1 Sector definitions

Using the available information within the existing ICO databases, we use the following sector definitions for the purposes of the analysis:

- **Central government**: This includes advisory boards and panels, executive agencies, government departments, non-departmental public bodies and ombudsman.
- **Wider public sector**: This includes organisations in the health sector, local government, central government, education and childcare, justice, and regulators.

There are a number of data quality issues which should be considered in the context of the analysis:

- The ICO's current data categorisation infrastructure has no definitive marker for public sector organisations.
- The use of subsectors is inconsistent with how they are defined by the UK Government. For example, the UK Government categorises central

[5] 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 data protection processes, an important factor in driving data protection compliance. Over the long-term, this may contribute to a reduction in data protection harms and increased public confidence in the handling of personal data.

government bodies as Ministerial and Non-Ministerial departments; public bodies and agencies; and public corporations.[6] This differs to how central government is defined by the ICO and creates barriers to any benchmarking or comparative analysis. Ideally, sector definitions should be standardised and align with the UK Government and wider industry SIC codes.

- The definition of the wider public sector we use is also problematic, as it covers elements of the private sector such as private healthcare and pharmaceutical companies[7]. The education and childcare sector also includes elements of private education and private childcare such as childminders and nurseries. Given time and resource these would ideally be excluded from the analysis. However, given their relatively small share this was not considered proportionate.

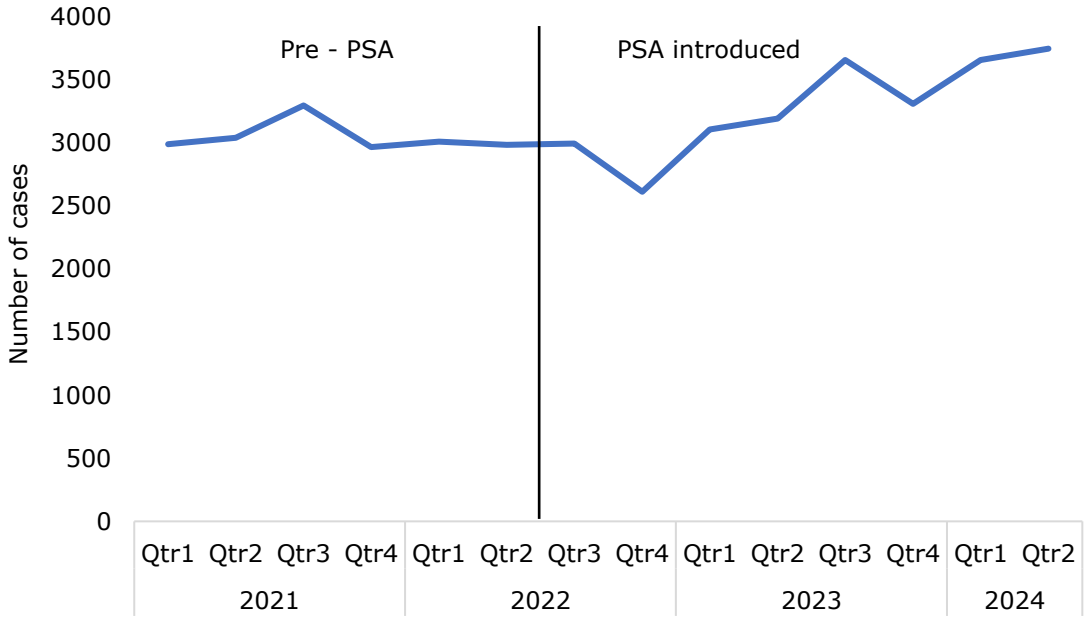
B.2 Trends in data protection complaints

This section describes trends in the number of public sector data protection complaints between Q1 2021 and Q2 2024 ensuring that the baseline prior to the PSA is considered for context.

As shown in Figure 3, the number of complaints received varied throughout the period. Between Q1 2021 and Q3 2022, the number of complaints received remained broadly steady and ranged between 2,970 and 3,300. Following the introduction of the PSA, complaints dropped to a low of 2,614 in Q4 2022 before gradually rising to a peak of 3,749 in Q2 2024.

[6] UK Government (2024) Departments, Agencies and Public Bodies. Available at: www.gov.uk/government/organisations [Accessed 16 October 2024].
[7] These private sector elements make up a relatively small share of the data (10-15%) and don't have a major impact on the overall analysis.

Figure 3: Data protection complaints about public sector organisations, Q1 2021 to Q2 2024



Source: ICO analysis.

Prior to the introduction of the PSA in June 2022, the ICO received an average of around 3,050 complaints per quarter (between Q1 2021 and Q2 2022). In the period following the announcement of the approach (Q3 2022 to Q2 2024), the average number of complaints rose to around 3,300 per quarter, an increase of 8% on the pre-trial period.

Table 2 shows that the number of complaints over the life-time of the PSA. 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 likely linked to the limitations set out earlier in this chapter.[8]

[8] Results are not statistically significant. Comparison of means, t-test to 90% significance.

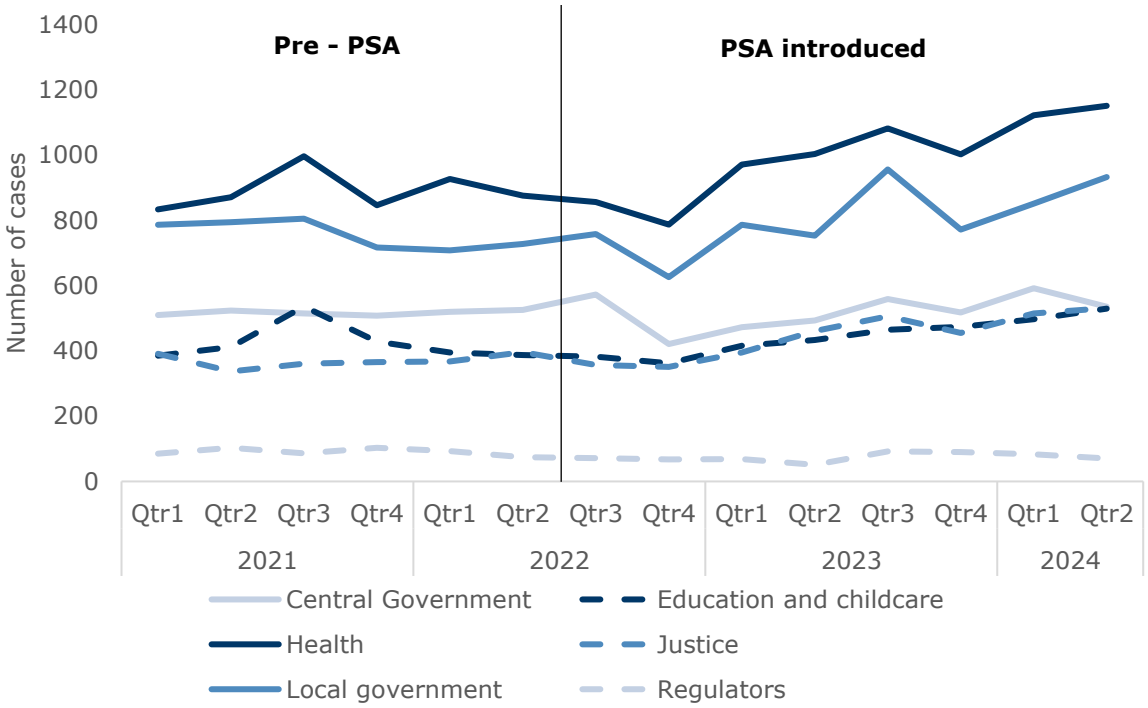
Table 2: Data protection complaints per year, Q3 2021 to Q2 2024[9]

Sector	Pre-Trial (July 2021 to June 2022)	Year 1 of trial (July 2022- June 2023)		Year 2 of trial (July 2023 – June 2024)	
	No. of complaints	No. of complaints	% change on Pre-Trial	No. of complaints	% change on Pre-Trial
Wider public sector	12,265	11,914	-3%	14,380	+17%

Source: ICO analysis.

Figure 4 shows the number of public sector complaints by sector. All sectors, except for regulators, follow a similar trend to that of public sector complaints as a whole. For most sectors, complaints remained largely constant between Q1 2021 to Q3 2022, after which the total number of cases per quarter mostly increased for the remainder of the trial.

Figure 4: Data protection complaints about public sector organisations by sector, Q1 2021 to Q2 2024



Source: ICO analysis.

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 period) followed by local government (around 6,400, 24%) and central government

[9] Data reported here starts in Q3 2021 allow comparison across 12 month periods.

(4,200, 16%). Regulators were subject to significantly fewer complaints (600, 2%).

Table 3 shows the average number of quarterly complaints per sector in the period leading up to the implementation of the PSA and for the duration of the trial. 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 been in justice (21%), followed by health (12%) and local government (6%).

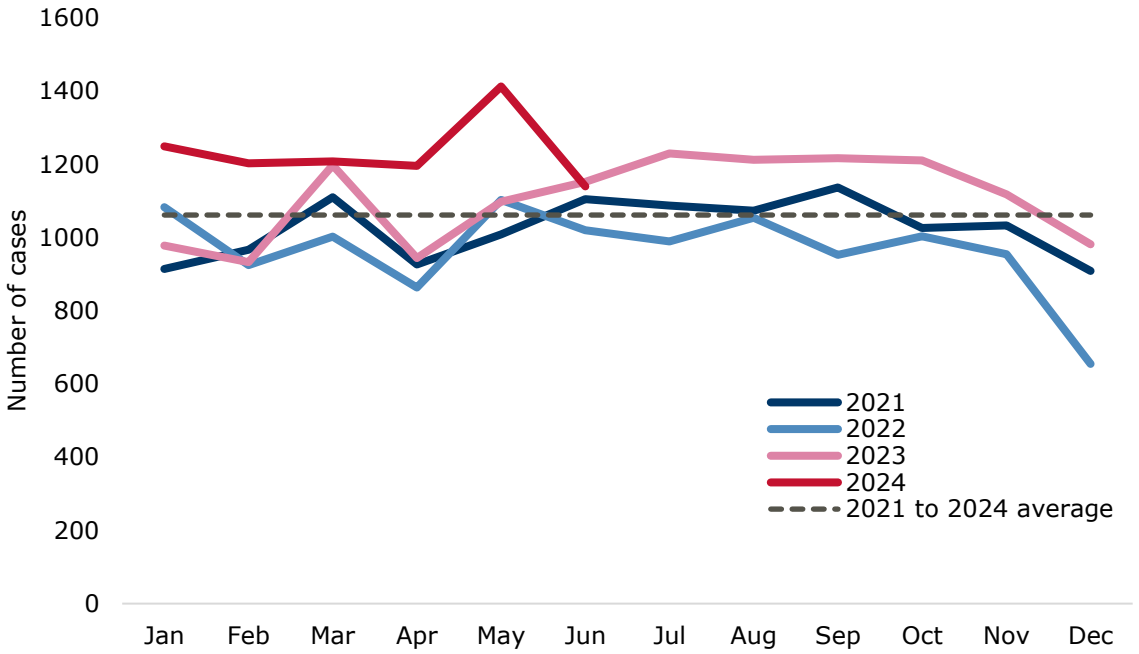
Table 3: Number of complaints per quarter by sector, pre and post PSA

Sector	Mean data protection complaints per quarter		Percentage change (%)
	Pre-Trial Period Q1 2021 to Q2 2022	Trial Period Q3 2022 to Q2 2024	
Central Government	517	521	+1%
Education and childcare	424	445	+5%
Health	892	997	+12%
Justice	370	446	+21%
Local government	756	804	+6%
Regulators	91	74	-18%
Total	**3,050**	**3,287**	**+8%**

Source: ICO analysis.

Between January 2021 and June 2024, an average of 1,062 complaints were received each month about the total wider public sector (as shown in Figure 5). The data remains highly volatile, with monthly complaints ranging from a low of 655 in December 2022 to a high of 1,413 in May 2024.

Figure 5: Data protection complaints by month, Q1 2021 to Q2 2024



Source: ICO analysis.

The proportion of data protection complaints reaching specific outcomes remains similar pre and post implementation of the PSA (as shown in Table 4). The majority of complaints resulted in no further action (around 60% of data protection complaints) whilst almost all other cases ended in informal action (around 40%).

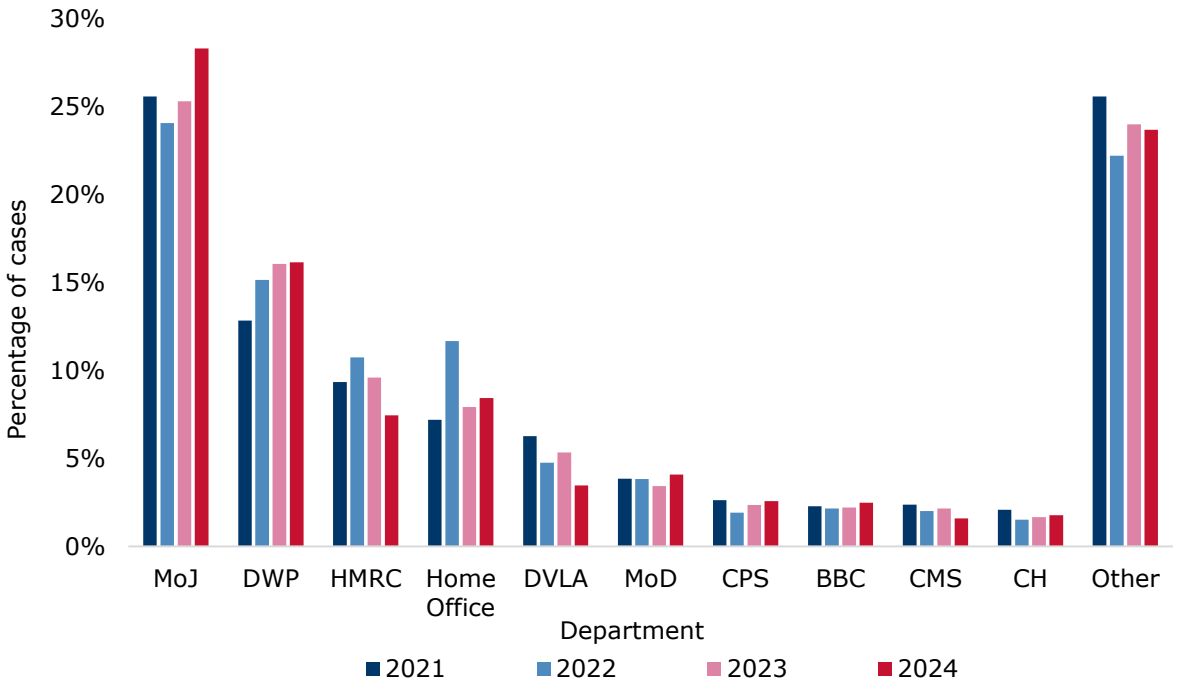
Table 4: Data protection complaint decisions, Q1 2021 to Q4 2023

Decision	Pre-Trial (January 2021 to June 2022)		Trial Period (July 2022 to December 2023*)	
	No. of cases	% of cases	No. of cases	% of cases
Informal action taken	7,386	40%	7,792	41%
Investigation pursued	3	0%	5	0%
No further action	10,906	60%	10,925	58%
Regulatory action taken	1	0%	0	0%
Unassigned	1	0%	163	1%
Total	**18,297**		**18,885**	

Note: Q1 and Q2 2024 removed to facilitate comparison of percentages. A large number of complaints from 2024 remain unassigned.
Source: ICO Economic Analysis.

Since Q1 2021 there have been 7,267 data protection complaints about central government. The top ten most complained about departments accounted for between 74% and 78% of all complaints in each year. 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).

Figure 6: Top ten departments[10] ranked by percentage of central government complaints 2021 to 2024



Source: ICO analysis.

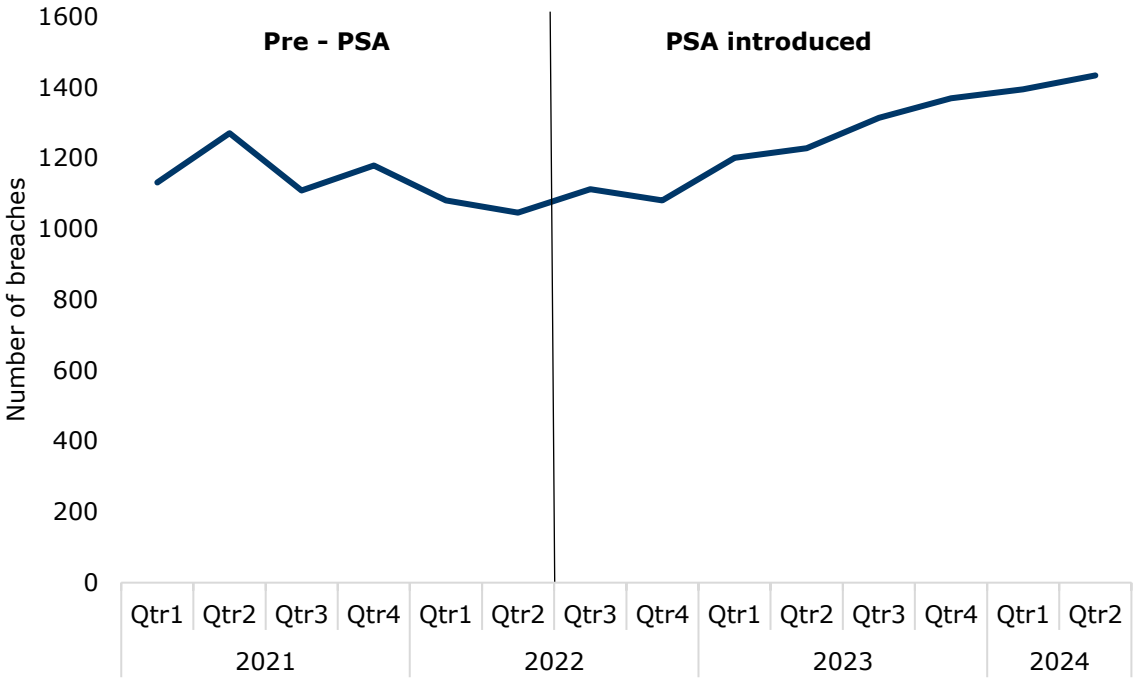
B.3 Personal data breaches

This section describes trends in the number of personal data breaches (PDBs) reported to the ICO by the wider public sector between January 2021 and June 2024.

The number of PDBs reported to the ICO has fluctuated over the period, dipping to a low of 1,046 in Q2 2022 and rising to a peak of 1,434 in Q2 of 2024 (as shown in Figure 7).

[10] MoJ: Ministry of Justice; MoD: Ministry of Defence; CPS: Crown Prosecution Service; CMS: Child Maintenance Services; CH: Companies House.

Figure 7: PDBs reported to ICO by the wider public sector, Q1 2021 to Q4 2024



Source: ICO analysis.

Prior the introduction of the PSA in June 2022, the ICO received an average of 1,136 public sector breaches per quarter (Q1 2021 – Q2 2022). After the implementation of the PSA, the average number of reported breaches increased by 11% to 1,267 per quarter.[11]

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), 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. As shown in Table 5, all sectors except central government saw an increase in both years of the trial.

Table 5: Personal data breaches reported to the ICO, Q3 2021 to Q2 2024

	Pre-Trial (July 2021 to June 2022)	**Year 1 of trial (July 2022- June 2023)**		**Year 2 of trial (July 2023 – June 2024)**	
Sector	No. of Breaches	No. of Breaches	% change on Pre-Trial	No. of Breaches	% change on Pre-Trial
Central Government	220	169	-23%	200	-9%
Wider public sector					

[11] Result is statistically significant using a comparison of means, t-test with 95% significance.

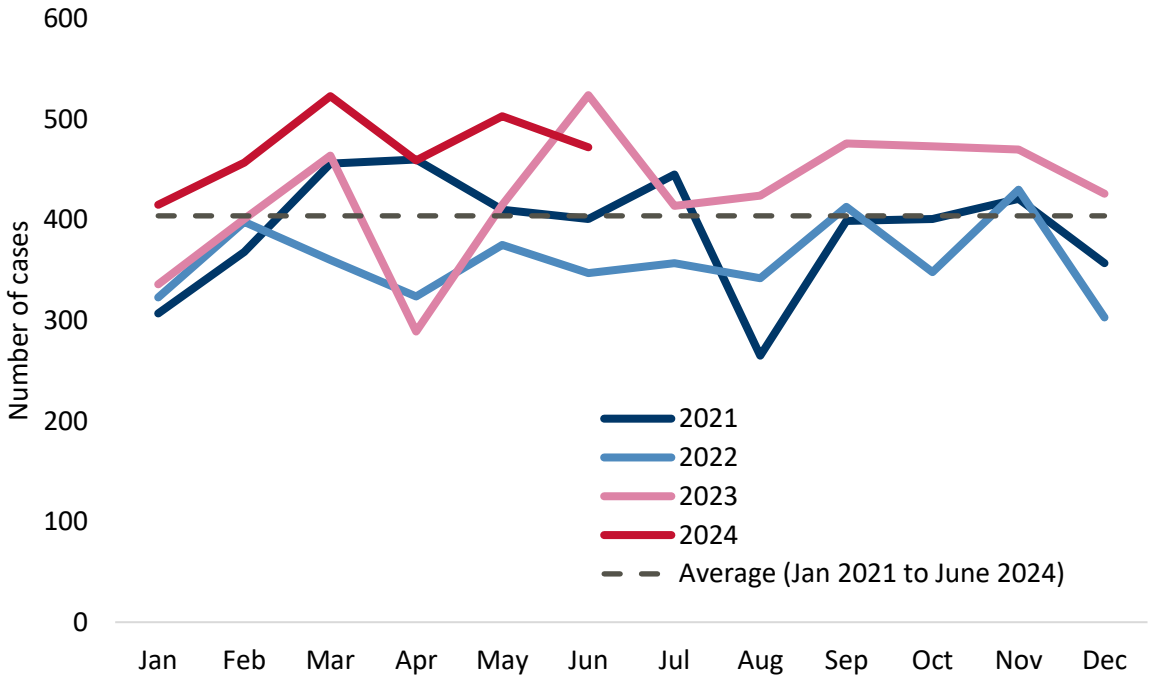
Education and childcare	1,367	1,426	4%	1,718	26%
Health	1,761	1,855	5%	2,216	26%
Justice	136	171	26%	213	57%
Local Government	895	957	7%	1,128	26%
Regulators	36	44	22%	37	3%
Total – wider public sector	**4,415**	**4,622**	**5%**	**5,512**	**25%**

Source: ICO analysis.

Over the lifetime of the trial (Q3 2022 – Q4 2024), health saw the highest number of breaches (4,100, 40% of the total breaches during the trial period) followed by education and childcare (around 3,100, 31%) and local government (2,100, 21%). Regulators were subject to significantly fewer breaches (around 100 breaches, 1%).

Between Q1 2021 and Q2 2024, an average of 404 wider public sector breaches were reported each month (as shown in Figure 8). The data remains highly volatile, with monthly complaints ranging from low of 265 in August 2021 to a high of 524 in June 2023.

Figure 8: Personal data breaches reported by month, Q1 2021 to Q2 2024



Source: ICO analysis.

The proportion of PDBs reported reaching specific outcomes remains similar pre and post implementation of the PSA (as shown in Table 6). The largest proportion of complaints resulted in informal action (around 75% of reported

breaches) with the remaining cases resulting in an investigation being pursued (8-9% of reported breaches) or no further action (14% of reported breaches).

Table 6: Personal data breaches reported, Q1 2021 to Q4 2023

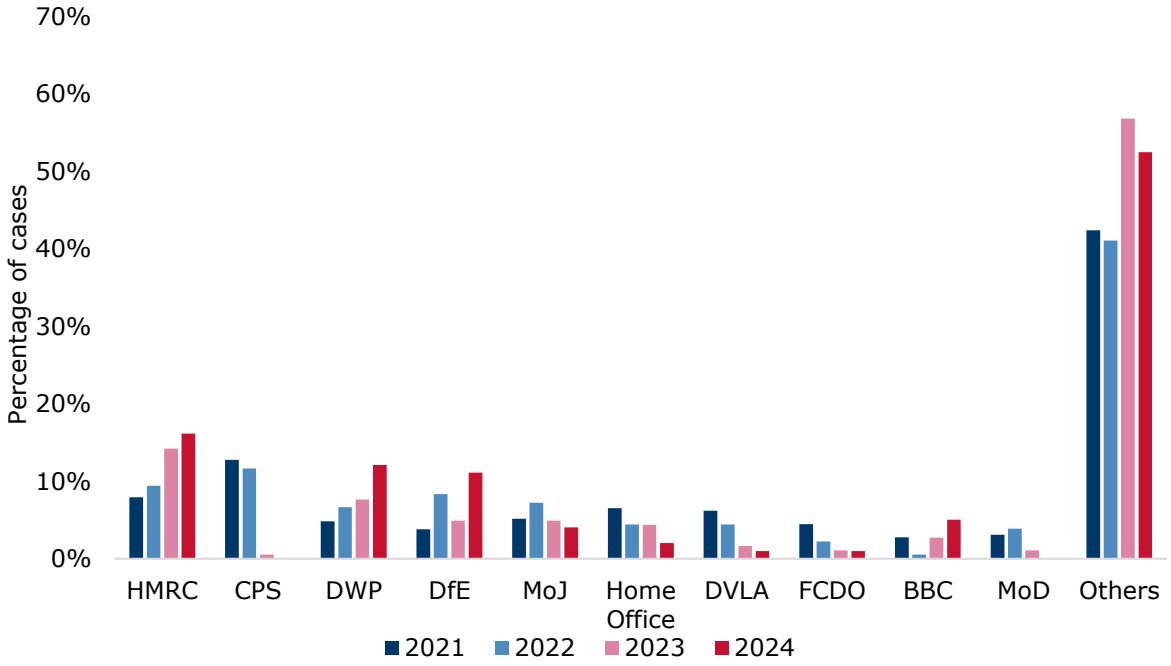
Decision	Pre-Trial (January 2021 to June 2022)		Trial Period (July 2022 to December 2023*)	
	No. of breach reports	% of breach reports	No. of breach reports	% of breach reports
Informal action taken	5,214	76%	5,438	75%
Investigation pursued	624	9%	555	8%
No further action	979	14%	1,022	14%
Unassigned	0	0%	245	0%
Total	**6,817**	**-**	**7,305**	**-**

Note: Q1 and Q2 2024 removed to facilitate comparison of percentages. A large number of reports from 2024 remain unassigned.
Source: ICO Economic Analysis.

Between 2021 and 2024, the top ten organisations in central government accounted for around half of all breaches in the sector *(as* highlighted in Figure 9). The departments that reported the most breaches were HMRC (82 breaches, 11% of total central government breaches) followed by the Crown Prosecution Service (59 breaches, 8%) and the Department for Work and Pensions (52 breaches, 7%). Notably, the Crown Prosecution Service reported just one personal data breach in 2023 and none in 2024, despite having recorded the most of any department in both 2021 (37 breaches, 12%) and 2022 (21 breaches, 11%).

It is worth highlighting that reported breaches for individual departments are often highly volatile linked to some of the factors set out at the beginning of this chapter.

Figure 9: Top ten departments[12] ranked by percentage of personal data breaches reported 2021 to 2024, with equivalent percentage share by year.



Source: ICO analysis.

[12] CPS: Crown Prosecution Service; MoJ: Ministry of Justice; MoD: Ministry of Defence.

Annex C: Evidence from international DPAs

This annex reviews the approach taken by other DPAs to regulating the public sector, both in EU/EEA Member States, which have GDPR,[13] and other countries.

C.1 Countries with GDPR

Countries with GDPR can set their own national rules on if and how they issue administrative fines to public authorities. Table 7 provides a review of the approach followed by each country. As the provision and regulation of public administration is not homogeneous across GDPR countries, the table also specifies who is considered in scope for each country's public sector approach on administrative fines.

Table 7: Comparison of approach to administrative fines in GDPR countries

Country	Maximum fine on public authorities and bodies	Who is subject to these specific rules
Austria	EUR 0	Public authorities and public bodies
Belgium	EUR 0	Government or its servants or agents, except those offering goods or services on the market
Bulgaria	No specific rules for public sector	
Croatia	EUR 0	Public authority
Cyprus	EUR 200,000 (GBP 168,000)	Public authority carrying out not-for-profit activity
Czech Republic	CZK 0	Authorities and public entities
Denmark[14]	DKK 16,000,000[15] (GBP 1,800,000)	Public authorities
Estonia[16]	EUR 0	State authorities
Finland	EUR 0	Public authorities, public bodies, Evangelical Lutheran or Orthodox Church of Finland
France	EUR 0	Public authorities and public entities

[13] 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.
[14] As outlined in the GDPR recitals, the Danish and Estonian legal system don't allow the national DPAs to directly issue administrative fines, which are instead imposed by the competent national courts.
[15] Administrative fines can only be issued in very simple cases where there is clear case law regarding the level of the fine for the relevant type of infringement.
[16] See footnote 12 above.

Germany	EUR 0[17]	Public authorities and public bodies
Greece	EUR 10,000,000 (GBP 8,400,000)	Public authorities
Hungary	HUF 20,000,000 (GBP 43,000)	Public authorities
Iceland	No specific rules for public sector	
Ireland	EUR 1,000,000 (GBP 840,000)	Public authorities and public bodies providing it is not acting as an undertaking within the meaning of the Competition Act 2002
Italy	No specific rules for public sector	
Latvia	No specific rules for public sector	
Liechtenstein	EUR 0	Public authorities and public bodies
Lithuania	EUR 60,000 (GBP 50,000)	Public institutions
Luxembourg	EUR 0	The State or municipalities
Malta	EUR 50,000 (GBP 42,000)	Public authority
Netherlands	No specific rules for public sector	
Norway	No specific rules for public sector	
Poland	PLN 100,000 (GBP 2,000)	Public authorities, research institutes, and the Polish National Bank
Portugal	No specific rules for public sector	
Romania	RON 200,000 (GBP 34,000)	Public authority
Slovakia	No specific rules for public sector	
Slovenia	Unclear – new data protection law introduced in 2023	
Spain	EUR 0	Public entities and other authorities, unless acting in a private capacity
Sweden	SEK 10,000,000 (GBP 728,000)	Public authority

Sources: White & Case,[18] and CMS.[19]

[17] Some exceptions apply, eg depending on the extent public bodies compete in the market as public-sector companies.
[18] White & Case (2019) *GDPR guide to national implementation.* Available at: https://www.whitecase.com/insight-our-thinking/gdpr-guide-national-implementation [Accessed 7 August 2024].
[19] Ibid.

C.2 Other countries

Table 8 shows a review of the approaches taken to regulating the public sector in non-European countries.

Table 8: Comparison of approaches in non-GDPR countries

Country	Specific enforcement rules for public sector	Administrative fines on public sector	Penalty rules for public vs private sector
Andorra	Same as private sector	No (law does not allow)	Law doesn't allow penalties on public authorities
Australia (federal)	Follows approach in their Privacy regulation action policy	Yes: max AUD 3,960 (GBP 2,000) on individuals and AUD 19,800 (GBP 10,000) on bodies corporate	No difference
Australia, New South Wales	Follows approach of their Regulatory Framework	Yes: max AUD 110,000 (GBP 56,000)	Only regulates the public sector, with the exception of some health service providers
Australia, Northern Territories	No role in enforcement	No	Not applicable to jurisdiction
Australia, Victoria	Risk-based approach, guided by principles in their Regulatory Action Policy	Yes: max AUD 118,554 (GBP 61,000) on individuals and AUD 592,770 (GBP 304,000) on body corporates	Only regulates public sector organisations and their contracted service providers
Bosnia-Herzegovina	(No information provided)	Yes: min fine or penalty imposed on employee (BAM 100, GBP 44) and responsible person (BAM 1,000, GBP 440), not on the institution	For public sector it only imposes fines on employee and responsible person, not on institution. Can initiate misdemeanours before the Court, which can fine up

			to BAM 100,000 (GBP 44,000)
Canada	Privacy Commissioner can receive or initiate complaints and, following an investigation, issue findings and recommendations to public authorities; fines up to CAD 1,000 (GBP 570) for obstruction	No (law does not allow)	No difference: has no authority to issue fines or orders over public or private sector organisations
Guernsey	Same as private sector	Yes: max based on around global annual turnover or global gross income ("essentially equivalent" to GDPR)	No difference
Hong Kong	Same as private sector	No	No difference
Japan	Follows approach set out in guidelines for administrative entities	No (law does not allow)	Different penalties can be imposed on public and private sector depending on the type of infringement.
Jersey	Same as private sector	No (law does not allow)	Law doesn't allow penalties on public authorities
Mauritius	Same as private sector	No (all violations are considered criminal offences)	No difference: max MUR 200,000 (GBP 3,300) for both public and private sectors
New Zealand	Same as private sector	No	No difference: limited criminal penalties available but no

			administrative penalties
Switzerland (federal)	Acts in supervisory role (advising the federal administration and taking position on the confederation's legislative projects), not a sanction authority. Can issue an injunction, which opens the possibility to further legal action	No (law does not allow)	Law doesn't allow penalties on public authorities
Switzerland, Cantone Ticino	Can refer matters to the Court, and appeal against decisions	No (law does not allow) but Court can sanction to max CHF 10,000 (GBP 9,100)	Law doesn't allow penalties on public authorities
South Korea	Follows regulation framework	Yes: max KRW 50 mil (GBP 28,500)	No difference: same penalties regulations. Law was amended to increase the upper limit of the penalty surcharge for public institutions without revenue to KRW 2 bil (GBP 1.1 mil). Public officials who intentionally leak personal information causing significant secondary damage are removed from the public office, even for first time offenders.
Switzerland, Kanton Berne	Follows Data Protection Act	No (law does not allow)	DPA only applicable to public authorities, doesn't

	(2006), currently under review		regulate private entities
Switzerland, Zurich	Can only issue injunctions for public sector	No (law does not allow)	Law doesn't allow penalties on public authorities
USA	Federal Trade Commission has no jurisdiction over public sector	-	-

Sources: ICO analysis.

The information presented in the table was collected through direct engagement with DPAs, and Table 9 presents the list of all DPAs that were contacted for information.

Table 9: List of DPAs contacted

Country	Authority
Albania	Information and Data Protection Commissioner (IDP)
Andorra	Andorran Data Protection Agency (APDA)
Armenia	Personal Data Protection Agency (PDPA)
Argentina	Agencia de Acceso a la Información Pública (AAIP)
Australia	Office of the Australian Information Commissioner
Australia, New South Wales	Information and Privacy Commission (IPC) New South Wales (NSW)
Australia, Northern Territory	Information Commissioner Northern Territory
Australia, Victoria	Office of the Victorian Information Commissioner (OVIC)
Brazil	National Data Protection Authority
Bermuda	Office of the Privacy Commissioner
Bosnia & Herzegovina	Personal Data Protection Agency (AZLP)
Canada	Office of the Privacy Commissioner
Dubai	Commissioner of Data Protection, Dubai International Financial Centre
Georgia	Personal Data Protection Service
Ghana	Data Protection Commission
Gibraltar	Gibraltar Regulatory Authority
Guernsey	Office of the Data Protection Authority
Hong Kong	Office of the Privacy Commissioner for Personal Data (PCPD)

Isle of Man	Isle of Man Information Commissioner
Israel	Privacy Protection Authority
Japan	Personal Information Protection Commission
Jersey	Jersey Office of the Information Commissioner
Mauritius	Data Protection Office
Mexico	National Institute for Transparency, Access to Information and Personal Data Protection (INAI)
Morocco	National commission for the control and the protection of personal data (CNDP)
New Zealand	Office of the Privacy Commissioner
South Korea	Personal Information Protection Commission (PIPC)
Switzerland	Federal Data Protection and Information Commissioner (FDPIC)
Switzerland, Cantone Ticino	Data Protection Authority
Switzerland, Kanton Basel-Landschaft	Data Protection Office
Switzerland, Kanton Berne	Data Protection Supervisory Authority
Switzerland, Kanton Luzern	Data Protection Authority
Switzerland, Stadt Basel	Data Protection Office
Switzerland, Solothurn	Data Protection Agency
Switzerland, Zurich	Data Protection Authority
United States	Federal Trade Commission
Uruguay	Personal Data Regulatory and Control Unit

Source: ICO analysis.

Annex D: Central government DPO survey

D.1 Background

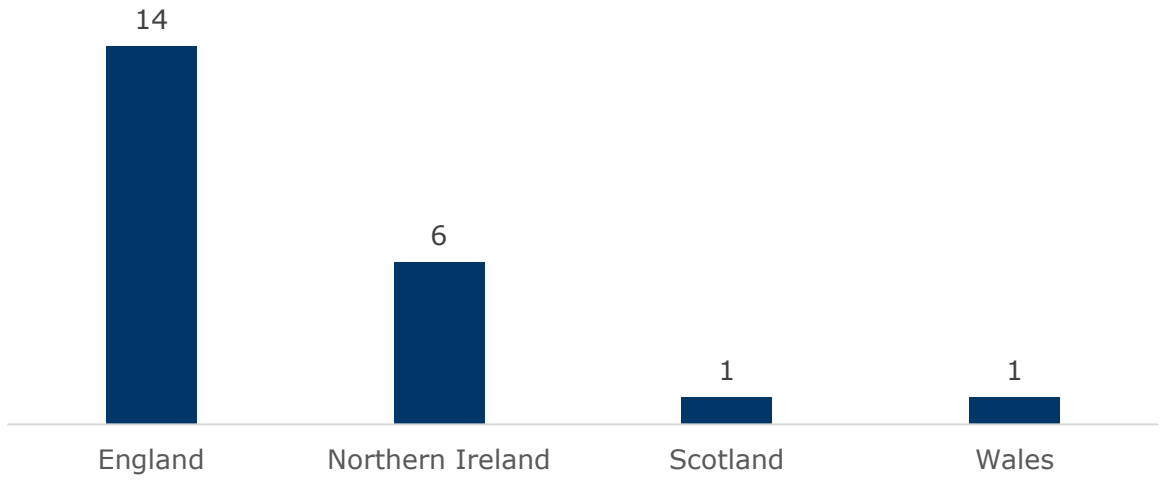
In July 2024, we conducted an end of trial survey of UK data protection officers (DPOs) working in the public sector. This repeated a baseline survey, originally carried out in November 2022.

In total, 34 public sector DPOs completed the survey. Following the data cleaning process, 22 respondents (compared to 28 respondents in November 2022) were included in the final analysis. This included:

- 14 DPOs (23 in November 2022) in central government departments[20]; and
- Eight DPOs (five in November 2022) in the devolved administrations[21].

The 12 respondents that have been excluded from the analysis were from DPOs working in the wider public sector. As the survey concerned the impacts of the PSA on central government departments, these results have been excluded from the analysis. The results from these respondents are instead covered elsewhere in the report, as relevant. The geographical breakdown of respondents included in the final analysis is set out in Figure 10 below.

Figure 10: Geographical breakdown of respondents



Source: ICO analysis (n=22).

[20] The variation in response rates between the baseline survey and the second wave is likely linked to a more coordinated response from central government in wave two. There were multiple responses from some departments for the baseline.
[21] The devolved administrations have differing structures. There is a central structure in Scotland and Wales, and a multi-department structure in Northern Ireland. The Scottish and Welsh Governments thus have one DPO covering the whole executive and the Northern Ireland executive have a DPO for each department. Thus, the variation in response rates across the devolved administrations

It is worth caveating that there are likely some comparability limitations between the baseline survey and wave two at the end of the trial period due to the changed sample sizes (discussed above). Also it is also likely that the respondents within departments have changed since the baseline survey was conducted, reflecting standard trends in personnel changes. Accordingly, caution should be exercised when making comparisons between time periods.

The remainder of this annex chapter is set out as follows:

- awareness of the PSA;
- rationale for the PSA;
- agreement with the PSA;
- views on published reprimands;
- views on upstream engagement activities;
- standing of data protection within central government;
- impacts of PSA within central government departments; and
- views of the ICO.

D.2 Awareness of PSA

Nearly all respondents (around 90%, 20 respondents) were aware of the ICO's PSA:

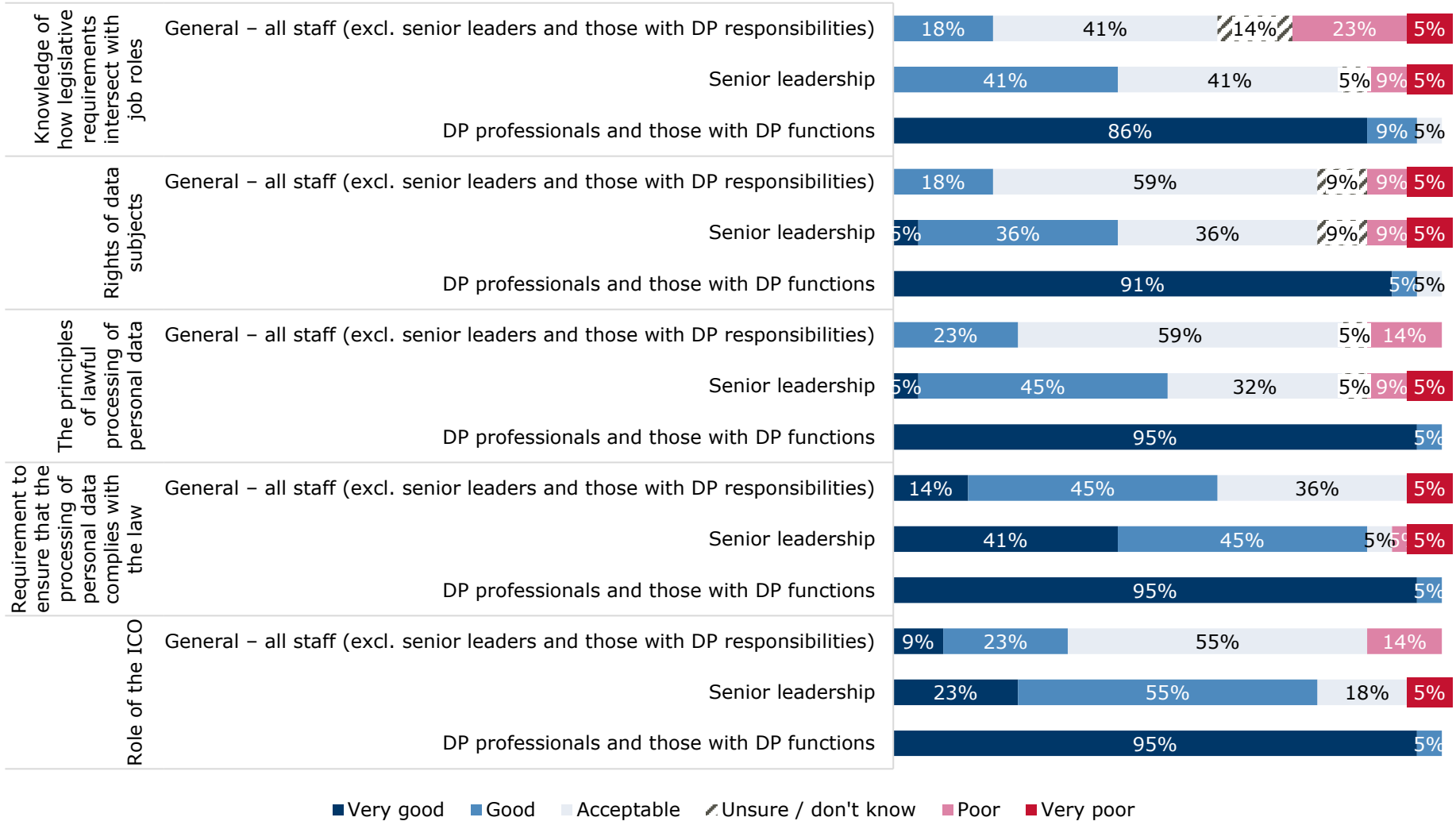
- 77% (64% in 2022) were "fully aware"; and
- 14% (36% in 2022) had "some general awareness".

The remaining 9% (0% in 2022) were "not aware of the revised public sector approach". The results indicate an increased depth of awareness amongst respondents compared to the baseline survey, despite an apparent rise in the number that were not aware of the PSA. The latter represents just two respondents and is likely linked to factors such as personnel changes or use of different terminology.

The majority of respondents (73%, 16 respondents) became aware of the PSA from the ICO website (27%, six respondents); the baseline survey (23%, five respondents); and stakeholder or representative bodies (23%, five respondents). This represents a shift from the baseline survey in 2022, where the most common source of awareness was an ICO representative (half of respondents).

Respondents were asked to rate levels of awareness related to the ICO and data protection matters by staff groups, as illustrated in Figure 11. As would likely be expected, the highest awareness levels across all three categories were amongst 'Data protection professionals and those with data protection functions', followed by 'Senior leadership' and then 'All other staff'.

Figure 11: How would you rate levels of awareness of the following data protection matters amongst the following staff groups?



Source: ICO analysis (n=22).

Compared with 2022, respondents felt awareness among 'Data protection professionals and those with data protection functions' had increased, whereas it was felt that awareness among 'senior leadership' and 'General – all staff' had decreased marginally. It should be noted that the awareness rating was linked to the specific data protection matters noted in Table 10 rather than data protection more generally. Also the comparability limitations noted at the outset should be borne in mind.

Table 10: Awareness of DP matters, average response in 2024 (change from 2022)

Staff group	**Data protection matter**			
	Role of the ICO	**Requirement to ensure that the processing of personal data complies with the law**	**Rights of data subjects**	**Knowledge of how legislative requirements intersect with job roles**
Data protection professionals and those with data protection functions	5.0 (+0.2)	5.0 (+0.2)	4.9 (+0.1)	4.8 (+0.0)
Senior leadership	3.9 (-0.1)	4.1 (-0.3)	3.3 (-0.1)	3.2 (+0.0)
All other staff	3.3 (-0.3)	3.6 (-0.4)	3.0 (-0.4)	2.8 (-0.2)

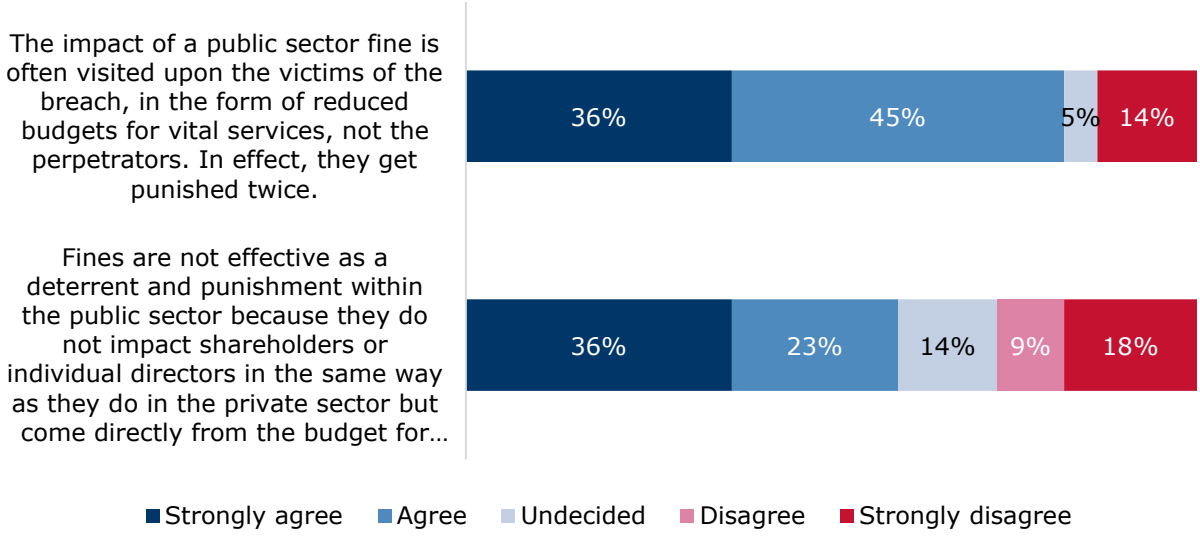
Note: To construct the average responses were given values. 'Very good' was scored 5 to 'Very poor' scored as 1. An average was then calculated and compared across the two surveys. Source: ICO analysis.

D.3 Rationale for the PSA

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, as shown in Figure 12. Compared to 2022, there was a fall in the level and strength of agreement (86% in 2022).

Around four in five (82%, 18 respondents) agreed that public sector fines impact victims of a breach in the form of reduced budgets for vital services. Although this is broadly consistent with 2022 (79% in 2022), there has been an overall marginal decline in the strength of agreement since the baseline survey.

Figure 12: Respondents' attitudes to fines

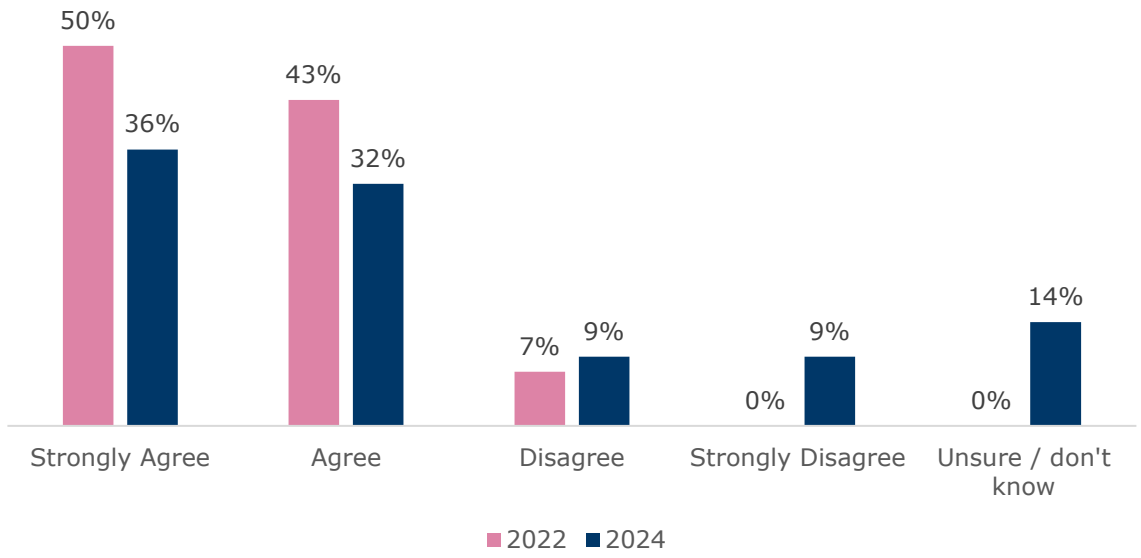


Source: ICO analysis (n=22).

D.4 Agreement with the PSA

As shown in Figure 13, there has been a decline in the level of agreement with the ICO's PSA. Although 68% (15 respondents) agreed with the PSA, this is down from 93% of respondents in 2022. It is unclear whether this reflects a shift in sentiment or is due to the volatility in sample size.

Figure 13: Respondents' level of agreement with the public sector approach



Source: ICO analysis (n=22).

Drilling down into how this has changed over the trial highlights a more balanced picture of support for the PSA:

- 36% (eight respondents) are now more supportive of the PSA than they were at the start of the trial;
- 32% (seven respondents) highlighted that their views have not changed during the trial period; and
- 23% (five respondents) were less supportive than they were at the beginning of the trial.

In so far as respondents provided further comments on responses, these were mostly positive.

"Having been reprimanded and having the threat of one - I can testify that it is an effective sanction whereas a fine would just be paid as its less work than actively engaging with ICO and stakeholders to fix the problem".

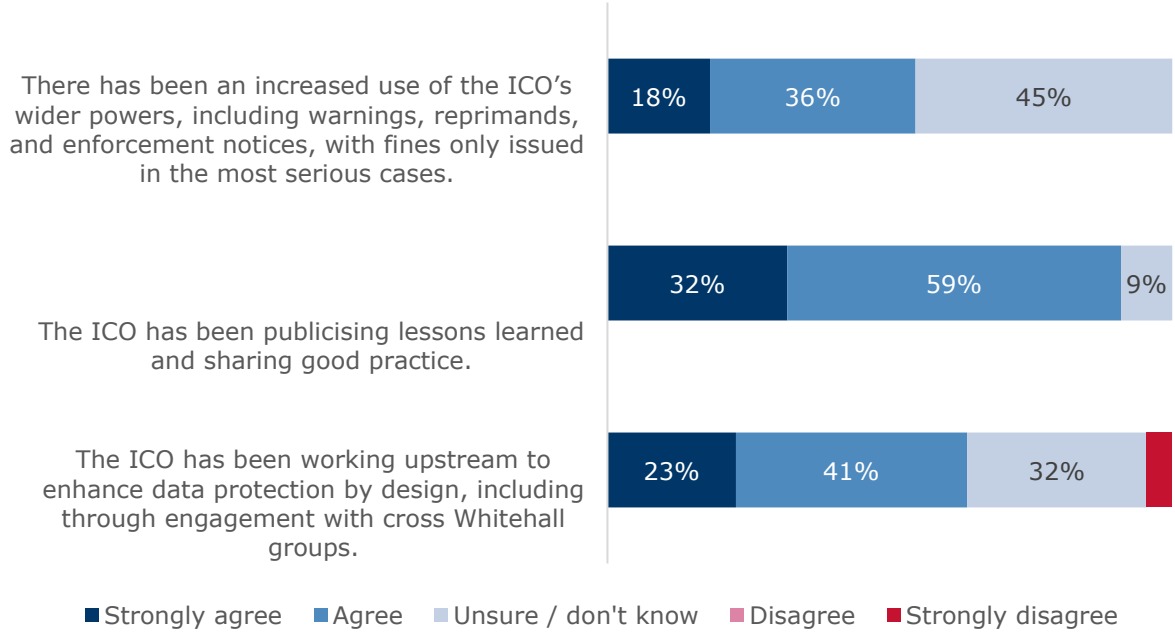
"the ICO's emphasis on reprimands, attendance at COO network meetings and issuing of surveys based on the reprimands have all helped to raise the profile of data protection".

"As the increased level of fines was a key point of interest when GDPR was introduced, I was initially concerned that removing/reducing fines for Government Departments would reduce senior engagement, but this has proven to be unfounded".

Respondents were also asked to provide an indication of their agreement that the PSA has been delivered as intended. As shown in Figure 14:

- Over half (55%, 12 respondents) agreed the PSA has seen an increased use of the ICO's wider powers such as warnings, reprimands and enforcement notices. The remaining 45% (ten respondents) were undecided.
- 91% (21 respondents) agreed that the PSA has seen the ICO publicising lessons learned and sharing best practice. The remaining 9% (one respondent) was undecided.
- Nearly two thirds (14 respondents) agreed that the ICO has been working upstream to enhance data protection by design. The remaining third (eight respondents) were either undecided (seven respondents) or disagreed (one respondent).

Figure 14: Respondents' level of agreement on activities related to the PSA



Source: ICO analysis (n=22).

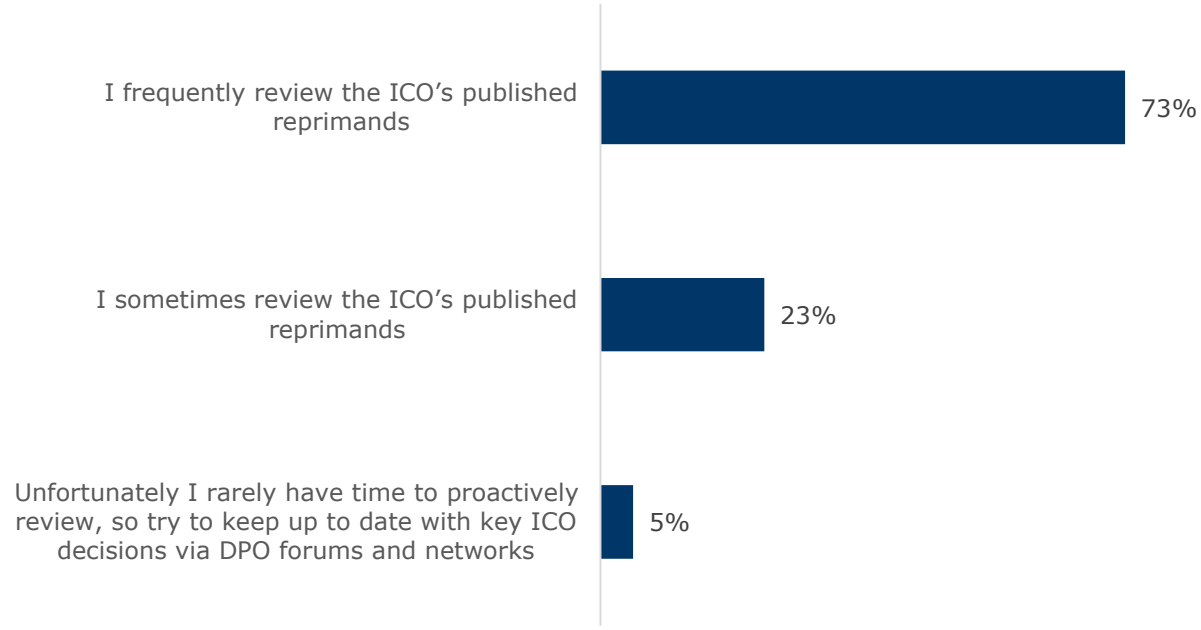
D.5 Views on published reprimands

All respondents were aware that the ICO regularly publishes reprimands that have been issued under the PSA:

- 86% (19 respondents) were "fully aware"; and
- 14% (3 respondents) had "some general awareness but did not know any detail".

As shown in Figure 15, the majority of respondents (73%, 16 respondents) review published reprimands on a regular basis.

Figure 15: Respondents' engagement with published reprimands



Source: ICO analysis (n=22).

Respondents were asked to provide their views on the effectiveness of published reprimands as a deterrent and in facilitating lessons learned. In terms of the role of reprimands as a deterrent:

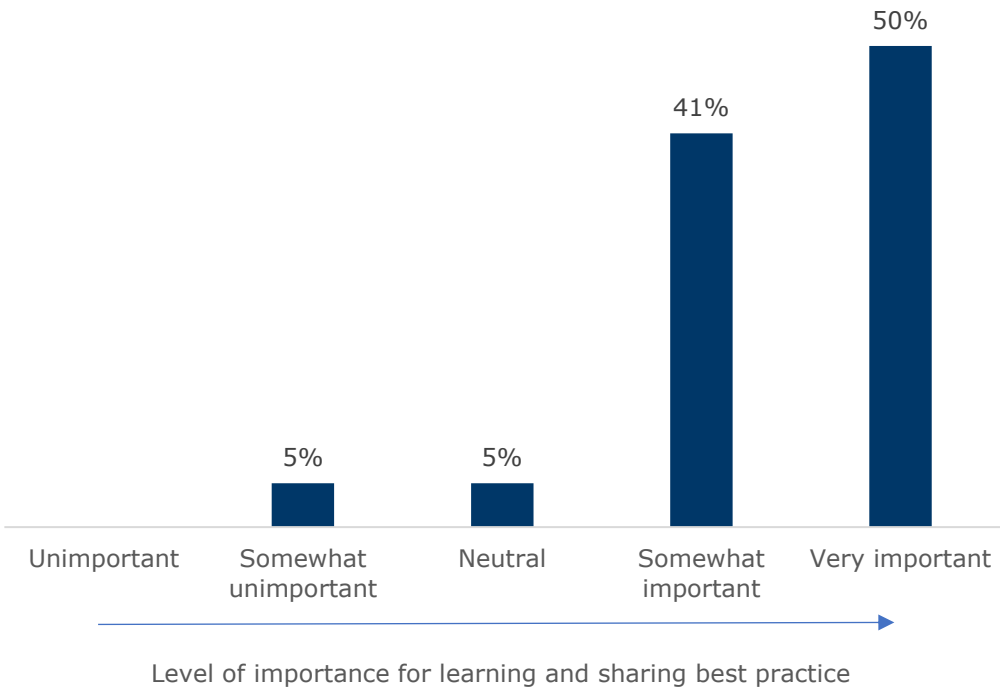
- The majority of respondents agreed that published reprimands are an effective deterrent. Responses commonly cited the negative impact of reputational damage which is effective in getting the attention of senior stakeholders.
- A number of responses agreed that reprimands were an effective deterrent, but only to a limited extent. In so far as further detail was provided, reasons included limited the coverage of reprimands in the media.
- Two respondents disagreed that published reprimands were an effective deterrent but provided no further detail or explanation.

In terms of facilitating a lessons learned approach:

- The majority of respondents agreed that published reprimands are useful in this regard. Respondents highlights 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 respondent felt that reprimands are of limited use due to difficulties in getting senior leaders to engage with them.

As shown in Figure 16, the majority of respondents (91%, 20 respondents) agreed that published reprimands were important for learning and sharing best practice within their department.

Figure 16: Views on the importance of published reprimands for sharing best practice



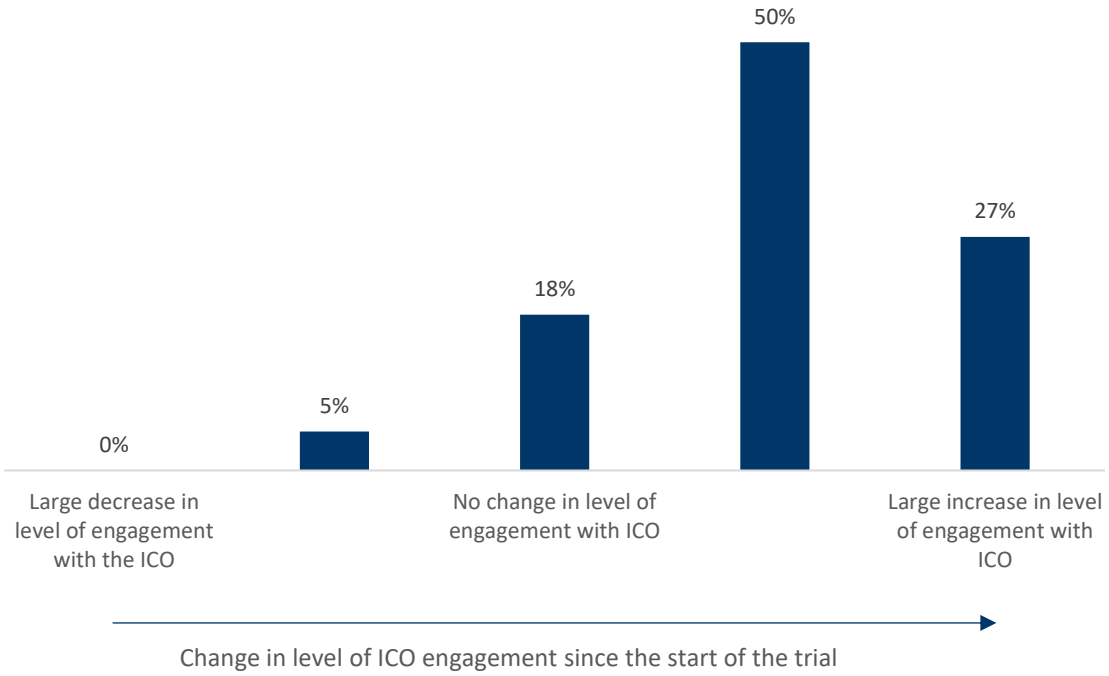
Source: ICO analysis (n=22).

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.

D.6 Views on upstream engagement activities

As shown in Figure 17, over three quarters of respondents (77%, 17 respondents) noted that there had been a rise in the level of ICO engagement over the trial period.

Figure 17: 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 the levels of ICO engagement was applicable to the PSA:

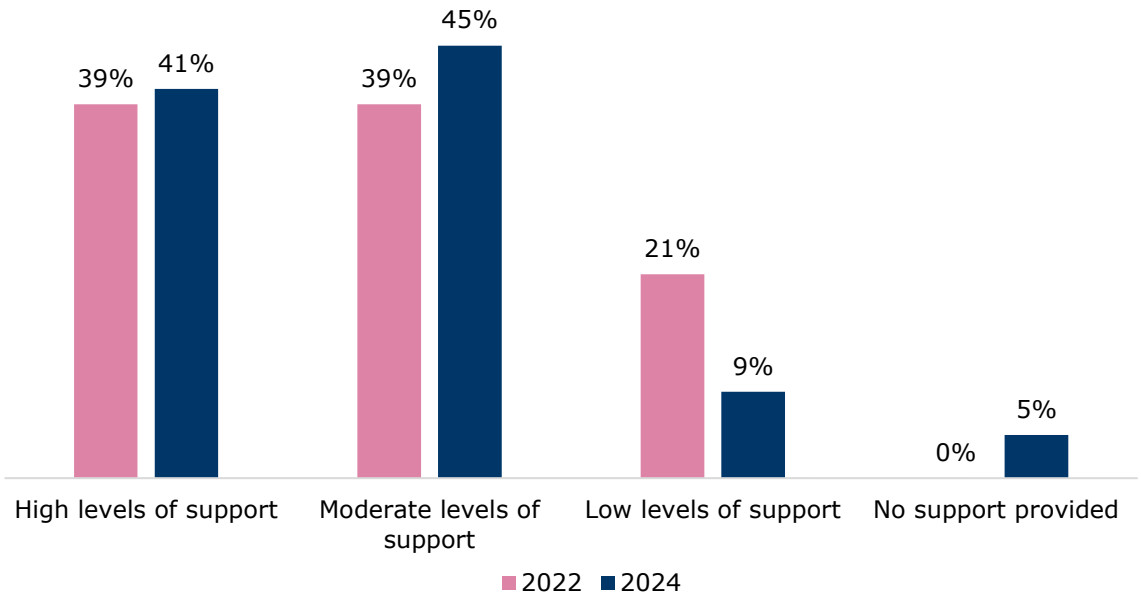
- 5% (one respondent) thought this entirely attributable to the PSA;
- 36% (eight respondents) thought this was partially attributable to the PSA;
- 27% (six respondents) thought changes in levels of engagement were entirely attributable to factors other than the PSA; and
- 23% (5 respondents) indicated that this was not applicable and 10% (2 respondents) explained other factors that had influenced changes in level of ICO engagement, including moving form a part-time to full-time DPO and the department now having more experienced practitioners and complex information access requests.

There were mixed views on how this engagement had impacted on data protection compliance within departments. Around a third (36%, eight respondents) thought this 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.

D.7 Standing of data protection within central government

Since the baseline survey 2022, there has been a slight rise in reported levels of support from senior leadership to drive compliance and high standards of information use (as shown in Figure 18). Around 86% (19 respondents) reported high or moderate levels of support, relative to 78% in 2022.

Figure 18: Levels of support from senior leadership in driving compliance



Source: ICO analysis (n=22).

The following quotes illustrate the variety of experiences reported by respondents:

"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".

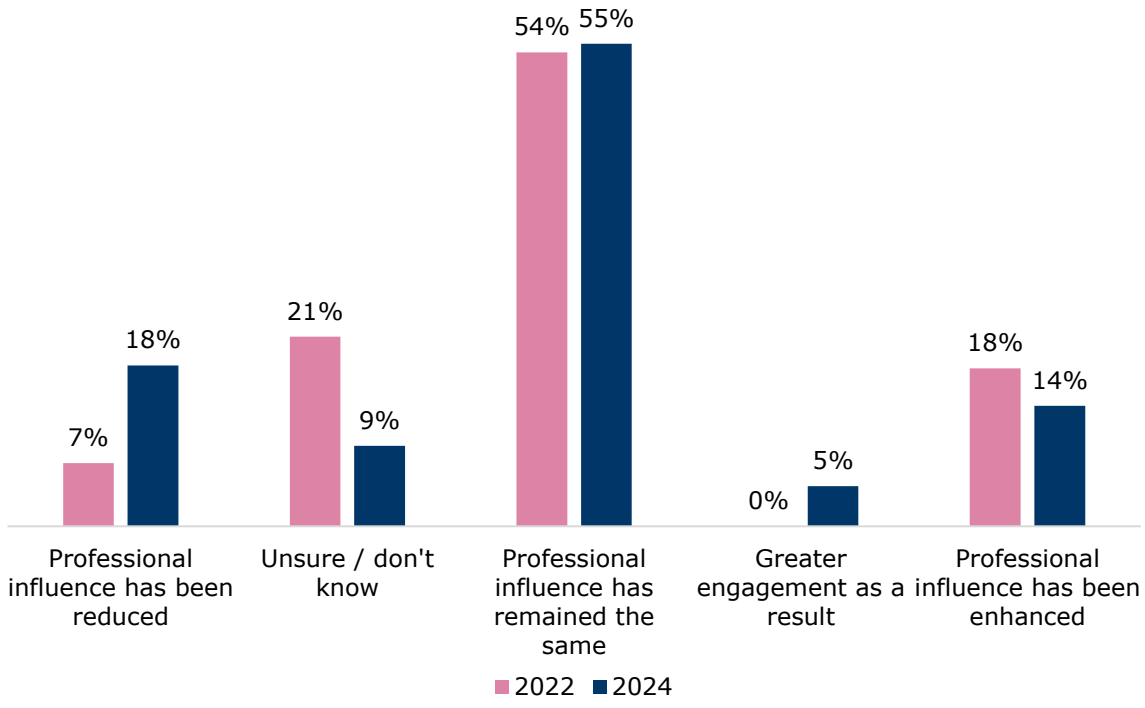
"As part of the SLT, I have good influence but it is still seen as a nuisance by some".

"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".

Respondents were asked how the level of professional influence of the DPO had changed as a result of the PSA. There were mixed views, as shown in Figure 19. Over half of respondents 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 been enhanced and 18% felt their influence had been reduced.

Figure 19: Impact of PSA on levels of professional influence



Source: ICO analysis (n=22).

D.8 Impacts of PSA within central government departments

Knowledge and awareness of data protection issues

Respondents were asked whether the PSA has had any impact on levels of knowledge and awareness of data protection in their departments. In response:

- Nearly half (45%, ten 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.

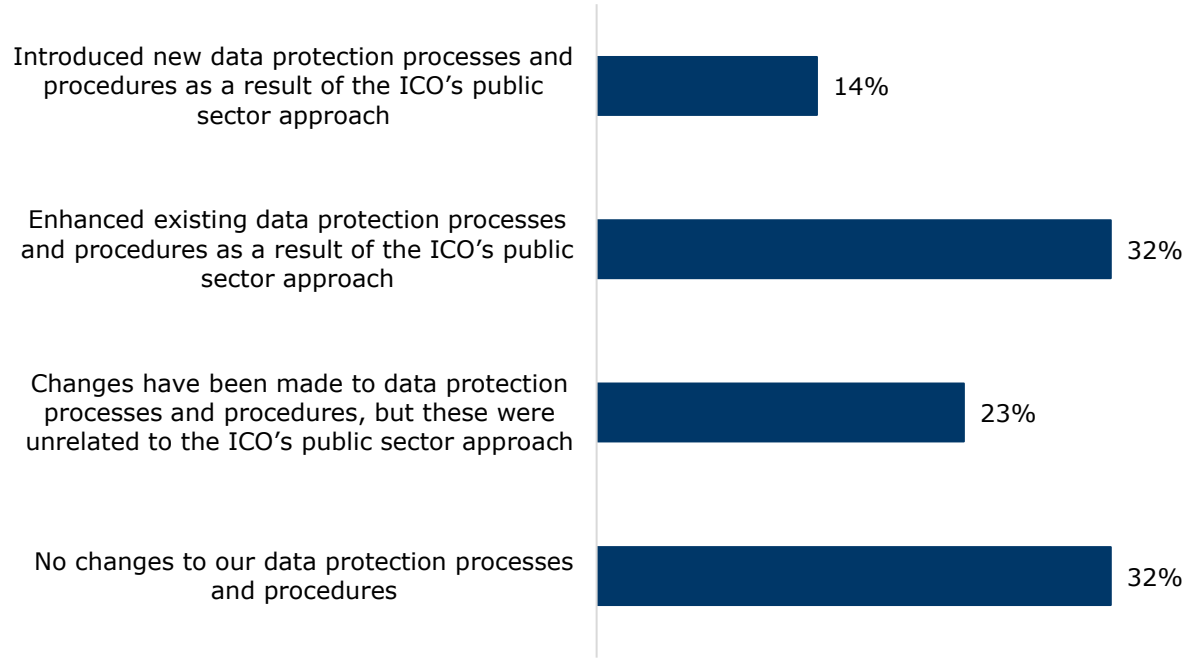
Changes to data protection processes and procedures

Respondents were also asked whether they had made any changes to their departments data protection processes and procedures as a result of the PSA. In response:

- 14% (three respondents) had introduced new data protection processes and procedures;
- around a third (32%, seven respondents) had enhanced existing data protection processes and procedures; and
- a third (32%, seven respondents) had not made changes to data protection processes and procedures.

A further 23% (five respondents) had made changes to data protection processes and procedures but highlighted that these were not made as a result of the PSA.

Figure 20: 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 respondents provided further detail, these changes included: updates to data protection guidance products in response to published reprimands; updates to training activities and regular briefings to the Chief Operating Officer (COO) in relation to data protection activities.

D.9 Views of the ICO

In terms of how the PSA has affected how departments view the ICO:

- 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 PSA "demonstrates that the ICO is responsive to the financial pressures faced by the public sector".

Those that reported having a more negative view of the ICO made the following comments:

"I have grown to view the regulator as more lenient and less robust in their enforcement activity*".*

"It is unhelpful for the main regulator to make clear as a matter of principle that they will not regulate our sector*".*

Annex E: Case studies

E.1 MoD – central government case study

Ministry of Defence (MoD) in-depth interview

Public sector approach context: During the trial period, MoD came into scope of the PSA twice: (i) early in the trial period, MoD received a reprimand[22] following an identified SAR backlog; (ii) MoD was issued with a monetary penalty[23] in February 2024 for inadvertently using the "To" field rather than the "BCC" field, disclosing 265 unique email addresses.

Response to BCC breach and earlier reprimand

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).

When probed about the impact of the ICO's regulatory intervention and how this might have differed in the absence of the public sector approach, 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".

While the journey started with the BCC breach, MoD noted that some changes had been challenging to implement and were ongoing. Key challenges experienced included clarifying accountability, getting discipline in their infrastructure set-up, and working towards a shift in culture (in terms of getting staff to understand that this is a core part of their job).

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

[22] ibid
[23] ICO (2024) *Ministry of Defence monetary penalty notice.* Available at: https://ico.org.uk/action-weve-taken/enforcement/ministry-of-defence-1/ (Accessed: 12 September 2024).

were able to invest in a single workflow assessment across the organisation and improve both front and back-end systems as a result, which had also started to drive savings that could be reinvested elsewhere.

Views on the PSA

MoD shared thoughts on different aspects of the ICO's public sector approach trial, including:

- **the increased use of reprimands**: MoD noted that reprimands are helpful in creating the conversation and increasing focus on avoiding the issue occurring again, but thought that if overused, they may lose impact over time.
- **use of the Commissioner's discretion to reduce the impact of fines on the public sector**: MoD highlighted that within their data protection networks, there had been no drop-off in interest in response to reduced use of fines. "We watch and follow any data protection issues in the news closely and what action the ICO is taking. There was no response in the slightest about cooling focus on data protection due to less fines".
- **better engagement including publicising lessons learned and sharing good practice:** MoD indicated that increased informal engagement with the ICO had been useful and that they appreciated having the opportunity to be able to reach out for advice and guidance.

More broadly, MoD emphasised the significance of reputational impacts within central government departments and at Civil Service board level, which were felt to be more meaningful than a monetary penalty. MoD noted that this approach to calling out those that do not '*hit the mark*' is the important aspect of the public sector approach to reinforce:

"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".

E.2 DWP – central government case study

Department for Work and Pensions (DWP) in-depth interview
Public sector approach context: During the trial period, DWP was issued with a reprimand[24] for inappropriate disclosure of individuals personal data by

[24] ICO (2022) *Department for Work and Pensions reprimand.* Available at: https://ico.org.uk/action-weve-taken/enforcement/department-for-work-and-pensions/ (Accessed: 12 September 2024).

Child Maintenance Appeals (CM Appeals) within DWP related to redaction functionality.

Response to breach and reprimand

DWP made a number of internal process improvements in response to the breach including:

- **strengthening internal data protection practices** around the introduction new software packages;
- updating **internal guidance** on redaction;
- **staff awareness raising** to reinforce best practice; and
- **training for staff** involved in redaction around what constitutes personal data.

When probed about the impact of the ICO's regulatory intervention and how this might have differed in the absence of the public sector approach, for example a fine issued rather than a reprimand, the response from DWP demonstrated the importance of the operational context in terms of how fines impact the delivery of services. DWP noted that its budget comes from the Treasury and that receiving a fine would not have directly impacted on frontline services, as not serving customers would not be an option.

This will differ markedly across the public sector given the varying scale and scope of organisations. This reflects the wide ranging nature of the public sector, where organisations often serve a diverse range of objectives and customers.

Views on the public sector approach

One aspect of the ICO's public sector approach trial included the increased use of reprimands. DWP agreed that reprimands are useful as a deterrent, since their publication can have a detrimental effect on departments' trust or reputation. As a tool for improving knowledge and awareness, DWP noted that "they always try to learn lessons" from published reprimands and that 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".

For example, DWP made specific improvements to data protection processes (strengthening guidance on redaction and processes around giving out information in response to FOIs) in response to a data breach at a different public authority 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.

DWP believed that the increased focus on alternative regulatory tools, such as published reprimands as part of the trial was "the right approach" and "makes sense". Overall, the ICO's PSA has driven impact by increased use of reprimands to facilitate lesson learning. However, DWP highlighted that its response to the breach would have remained the same, with or without the trial approach.

E.3 Anonymised case study

In-depth interview with a public organisation in a devolved area

Public sector approach context: A reprimand was issued during the trial period linked to an incident disclosing special category data due to an email sent using carbon copy (CC) rather than blind carbon copy (BCC).

Awareness of the PSA

The public organisation had not been explicitly aware of the ICO's trial change in stance to regulating the public sector. Furthermore, the trial approach was not referenced in the reprimand that was issued. However, the organisation highlighted that the nature of engagement with the ICO had improved from their perspective, and that this may have been a result of the change in approach.

The organisation highlighted that there had been a significant level of scrutiny and repetition in questions asked during the investigation period, which was extended, and that this had been challenging. However, they described current engagement with the local ICO office as 'very positive and supportive', noting that 'we feel we can pick up phone to get advice on changes we are trying to implement, such as new processes, templates and procedures' and that a workshop facilitated by the ICO had been useful. This demonstrates the enhanced upstream approach, introduced as part of the public sector approach trial.

Changes to data protection practices – impact

The organisation made a number of changes to their data protection processes and procedures as a result of the incident. These were described as more a direct response to the realisation that they'd had a UK GDPR infringement, rather than being implemented due to the ICO's reprimand (which was issued two years after the infringement occurred).

"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".

Changes that the organisation made following the infringement include:

- **The introduction of an information governance group** comprising of senior management and an external DPO. These meetings include a regular review of processes and cover information governance, information assets, and disposal of information, amongst other issues.
- An update of **policies around email communications.**
- The enhanced provision of **training to staff**. This includes annual training delivered by the DPO as well as a workshop facilitated by the ICO.
- **Regular staff communication**.
- **Exploring ways to limit the scope for human error,** such as email systems which remove the auto insert of email, as well as physical prompts with mitigating actions to consider.

Here we see how the prospect of supervisory and enforcement action drives changes to enhance data protection compliance and culture.

Views on reprimands as a regulatory tool and the wider approach

The organisation believed that 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 for the public seeking support.

When probed about the impact of the ICO's regulatory intervention and how this might have differed if a monetary penalty had been issued rather than a reprimand, the organisation thought that this would have had direct implications for the delivery of frontline public services, and disproportionately so in small organisations with a small budget. This has the potential to doubly impact the public who seek the organisation's services.

"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".

Reflecting on the potential lessons the ICO could learn from the trial, the organisation suggested that when determining the regulatory intervention, the ICO should give consideration to the impact of regulatory activities on smaller organisations, the nature of their role and how regulatory enforcement actions can impact on public trust and service capacity.