ORG OPEN RIGHTS GROUP

ICO ALTERNATIVE ANNUAL REPORT

November 2024

ABOUT ORG

Open Rights Group (ORG) is a UK based digital campaigning organisation working to protect fundamental rights to privacy and free speech online. With over 40,000 supporters, we are a grassroots organisation with local groups across the UK.

Our work on data protection and privacy includes challenging the immigration exemption to UK data protection law, defending the General Data Protection Regulation (GDPR) from attempts to water down its provisions, and challenging uncontrolled and unlawful data sharing by online advertisers.

openrightsgroup.org

Authors:

Jacob Ohrvik-Stott, Data Protection Consultant

Jim Killock, Executive Director, Open Rights Group

Mariano delli Santi, Legal and Policy Officer, Open Rights Group

EXECUTIVE SUMMARY

In this report the Open Rights Group offers our perspective on the Information Commissioner's Office's (ICO) 2023-24 Annual report, and recently published data on the enforcement action it has taken (or not) over the most recent financial year. Our analysis scrutinises the ICO's controversial policy experiment to limit fining public sector organisations to only the most severe data breaches – and explores the structural and cultural factors that have shaped the office's overly cautious approach to enforcement. While the new Data Access and Use Bill has removed some poorly thought out proposals to make the ICO beholden to ministers, it does not make any changes to the relationship of the ICO to Parliament or the courts; there is therefore a danger that the ICO will continue to feel little institutional pressure to improve: the message of this report needs to be heard.

Data protection needs to be understood a critical component in delivering a fair society. It protects against abusive and discriminatory decisions being made with data. It is used to ensure transparency in disputes with employers, customer services and even the police. As technologies like Artificial Intelligence (AI) progress, data protection rights help ensure that technology is not abused, and remains accountable. However, the reality of these rights depends greatly on our Information Commissioner, and their willingness to take dissuasive action against unlawful practices. This is especially true as the people most likely to be impacted are also often less able to take enforcement action themselves.

The ICO has been entrusted with an extensive range of enforcement powers by Parliament, and by extension the UK public. Data protection law was designed to enable the regulator to use the full range of these powers, ranging from reprimands for lower-risk incidents through to substantial fines and criminal prosecutions for individuals for the most severe breaches.

But its enforcement track record shows the ICO's use of these powers is skewed, having only issued four data protection law-related fines to private sector organisations in the last financial year. This record stands in contrast with the ICO's international counterparts, where data protection authorities across Europe have issued fines against a number of social media, AI and adtech companies – all high-risk areas where the ICO has seemingly failed to act over the past year. The office's two-year "public sector approach trial" has meant fines were reserved to one extremely severe case, where a Ministry of Defence (MoD) data leak risked the lives of 245 Afghanis.[1] 90% of the office's remaining enforcement actions resulted in public reprimands, but the prevalence of repeat offenders (including the MoD) suggests these interventions have not been sufficiently dissuasive. Other cases, including Home Office schemes tracking migrants through physical GPS tags, and destruction of police records needed for prosecution and defence, indicate that the ICO is struggling to prevent real harms through its approach to the state sector.

Even regarding simple problems, like the late processing of subject access requests (SARs), the ICO has been reluctant to take action against state bodies including local councils or the police, despite issues persisting over several years. In these cases, problems with the delivery of local services and access to justice are the likely result of the ICO's reluctance to act.

Several interconnected factors explain the ICO's reticence to adequately enforce data protection law. Public statements from the Commissioner – and political pressures exemplified by the previous government's proposal to give Ministers powers to influence ICO priorities in the Data Protection and Digital Information (DPDI) Bill[2] – suggest their priorities have been swayed by resource pragmatism and political saliency.

1 https://ico.org.uk/action-weve-taken/enforcement/ministry-of-defence-1/

2 https://bills.parliament.uk/bills/3430

Internally, the fallout from various unfavourable legal rulings, an over-focus on "assurance" initiatives, and the challenge of getting to grips with emerging technologies have all created a culture of enforcement caution. Externally, the ambiguity of the regulatory Growth Duty, and demands that the office engage with data protection reforms and digital regulations beyond its direct remit, have also distracted the ICO from enforcing the law. Exacerbating this all is a lack of independent oversight and constructive challenge: the government has seemed inappropriately keen to shape the office's strategy, whilst parliamentary attention has been ad hoc and piecemeal.

To address these challenges, and ensure the ICO's enforcement approach adequately upholds the public's data rights, we make eight overarching recommendations:

Recommendation 1: The ICO's forthcoming Regulatory Action Policy should prioritise transparency and clarity and be subject to regular external review.

Options and actions for doing so include:

- **A biyearly independent audit of the Regulatory Action Policy**, evaluating both how the ICO is implementing its policy, and its impacts on regulated entities' data practices.
- **Turning the Regulatory Action Policy into a live document with a clear hierarchy of enforcement policies**. This should clearly articulate how enforcement-related policies interact with each other and be easy to navigate (and by extension scrutinise) in one document. The document must be updated before a substantial change in enforcement approach has happened (rather than being announced ad hoc by the Commissioner at semi-public events).
- **Explaining how technology's potential for systemic impacts on equalities and human rights is factored into the enforcement strategy.**
- **Including a statutory requirement within the Data Use and Access (DUA) Bill for the ICO to publish their assessment logic and evidence base for all enforcement actions**. This must also include cases they have decided not to investigate following UK GDPR complaints past a certain reasonable threshold.

Recommendation 2: Independent research and legislative reform should be made to benchmark the ICO's private sector enforcement approach against other data protection authorities.

Options and actions for implementing this recommendation include:

- Amending the DUA Bill to **mandate the ICO to publish a list of priority sectors for enforcement,** where widespread data practices set problematic norms and cause harm (for example social media platform's illegal use of children's data, and the opaque adtech market). This should include information about the potential risks to equal and fair outcomes through an equalities assessment.
- UK Research and Innovation funding ongoing **independent research benchmarking ICO performance against international comparators.** This is compatible with the research council's mission to enrich lives and drive economic growth, given the important role data protection compliance plays in both. This research could be extended to other regulators with cross-economy remits.

Recommendation 3: The ICO should use the full range of its enforcement powers in the public sector – until and unless it can prove alternative approaches result in a substantial improvement in data protection compliance.

Options and actions for implementing this recommendation include:

- **Publishing all evidence resulting from the two-year "public sector approach trial"**[3] where public sector organisations were only fined as a last resort. If the evidence paints the pilot in a positive light, they should launch an external consultation and enable an independent audit of relevant data to validate their findings.

3 Source: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/06/ico-statement-on-its-public-sector-approach-trial/

- **Parliament exploring approaches for mitigating the potential impact of public sector fines on public services and data protection breach victims.** This could, for example, include ensuring a proportion of income from fines is invested in improving public sector data protection practices, or through establishing compensation or financial support funds for people impacted by breaches.

- **The DUA Bill banning the ICO from issuing more than one reprimand to an organisation**. Any subsequent breaches should result in an escalation of action – not additional "final reprimands" that both undermine the premise of the initial reprimand and have little impact on behaviour.

- **The DUA Bill requiring the ICO to publish a league table of public sector bodies' SAR performance.** Organisations who consistently fail to meet the required SAR standards compliance could then be prioritised for enforcement

Recommendation 4: The ICO should publish "lessons learnt" and develop international agreements that reduce the risk of enforcement action challenge.

Options and actions for implementing this recommendation include:

- Securing commitments from international regulatory agencies (where formal cooperation agreements exist) to **compel organisations subject to enforcement actions in those regions to demonstrate how they comply with UK data protection law.** This should include the European Data Protection Board and international DPAs, and other UK sectoral regulators such as the CMA where relevant.

- **Conducting an internal review of decision-making underpinning enforcement actions overturned by the Information Tribunal,** to identify the root causes of failure to meet legal standards. This evidence should be periodically reported to the Science, Innovation and Technology Select Committee, or Parliament.

Recommendation 5: The data protection risks of AI should be managed through better use of ICO transparency and data restriction powers, and legislative reforms to promote risk transparency.

Options and actions for implementing this recommendation include:

- **Establishing a mandatory UK-wide public sector AI registry** through the DUA Bill. This would ensure transparency to citizens using these systems, and enable external scrutiny of the ICO's decisions not to investigate these applications. This could follow the precedent set by the Scottish government AI Register.[4]

- **Issuing temporary data processing prevention orders to high-risk emerging technologies** that have systemic privacy impacts, until these applications can prove they are compliant with data protection law. This could include frontier AI models demonstrably trained on UK citizen data or automated public sector decision-making, and follows the precedent set by other European DPAs.

- **Compelling frontier AI model developers to provide the ICO with detailed information about the provenance of model training data.** This legal requirement could be enshrined in the DUA Bill, or in the forthcoming AI Bill.

- **Publishing an Action Plan for the ICO to deliver on its international treaty commitments on AI safety.**[5] This could be incorporated in the updated ICO Strategic Approach on Regulating AI.[6]

4 Source: https://scottishairegister.com/

5 Source: https://www.gov.uk/government/news/uk-signs-first-international-treaty-addressing-risks-of-artificial-intelligence

6 Source: https://ico.org.uk/media/about-the-ico/consultation-responses/4029424/regulating-ai-the-icos-strategic-approach.pdf

Recommendation 6: The ICO should clarify how it interprets the Growth Duty in its enforcement approach.

Options and actions for implementing this recommendation include:

- Including explicit detail on how it will **prevent unfair competition and consumer harm from data protection non-compliance in the ICO's updated Regulatory Action Policy**. This is a Growth Duty obligation. In doing so the ICO should formally consult with the CMA and refer to competition law enforcement decisions where the competition implications of data assets were considered.
- Ensuring the **list of priority sectors for investigation (outlined in recommendation 2) explicitly factors in areas where data protection practices may create unfair competition**.

Recommendation 7: The government should commit to providing additional funding to the ICO for functions that solely focus on engaging with non-data protection issues (for example online safety).

This would ensure these functions do not come at the expense of delivering the ICO's core regulatory remit, and could be part of ICO reforms considered in the DUA Bill.

Recommendation 8: Oversight of the ICO is strengthened through reform of Commissioner appointment procedures, Select Committees, and legal institutions.

Options and actions for implementing this recommendation include:

- **The Science, Innovation and Technology Select Committee establishing a Sub-committee on data protection effectiveness and reforms.** This would provide independent scrutiny of the proposed DUA Bill (following the precedent of the sub-committee on the online safety regime), and the ICO.
- **Transferring to the Science, Innovation and Technology Select Committee the responsibility for budget and the appointment process of the Information Commissioner's Office.** Currently, the Information Commissioner remains a Ministerial appointment, and select committee opinions on appointments as part of pre-appointment scrutiny are non-binding. Making the Information Commissioner a parliamentary appointment would increase arms-length from the government, and is likely to foster more active Parliamentary oversight.
- Giving the **Science, Innovation and Technology Select Committee a veto on ICO appointments**, if legislators are less ambitious; this would begin the process of ensuring the ICO's independence from government and giving a parliamentary committee more political responsibility for ensuring the appointments are successful.
- **Establishing a Data Rights Ombudsman** with powers to adjudicate on data subjects' appeals on how the ICO has responded to their complaints. A new independent body is necessary to deal with the volume of potential appeals, which the Information Tribunal does not currently have the capacity to do. This body could also provide valuable insights (through caseload data) on if and how the ICO is effectively responding to public complaints.
- Proving funding and legal powers for **the Equality and Human Rights Commission (EHRC), to periodically and publicly review the state of data-protection related rights in the UK.** This would ensure comprehensive scrutiny of data protection from the perspective of fundamental rights – a precondition to promote inclusive growth and ensure that the public can reap the benefits of innovation rather than be damaged by its externalities.

1 INTRODUCTION

In July 2024, the UK's data protection regulator the Information Commissioner's Office (ICO) published its Annual Report and Financial Statements for the 2023-24 financial year.[7] In it the ICO reviews its performance over the last year, providing valuable data and reflections on how it has enforced and championed the legislation it oversees.

The ICO has also recently committed to publish details of the reprimands it issues in response to a Freedom of Information (FOI) request made by data protection specialist Jon Baines,[8] which revealed a history of non-disclosure for reprimands issued to public sector authorities. As a result, valuable data relating to the ICO's enforcement approach is now available to the public: it shows where the ICO has investigated public and private bodies, and the proportion of these investigations that have resulted in reprimands, enforcement orders (that obligate recipients to change their data practices), or fines. These publications come at a time when the new Labour government plans to reform both data protection regulation and the ICO,[9] and the regulator approaches the conclusion of ICO25 – a three-year strategy initiated by current Commissioner John Edwards in January 2022.[10]

July 2024 also marked the end of Edwards' "two-year trial" of the ICO's revised approach to working with public authorities. This experiment, described in an open letter to public authorities,[11] is most notable for its controversial stance on its use (or arguably misuse) of its enforcement powers. The ICO opted to rely on "increased use of the ICO's wider powers, including warnings, reprimands and enforcement notices, with fines only issued in the most serious cases". Central to this strategy are bold claims that fines do not act as an effective deterrent for the public sector and indirectly punish victims of data breaches. As Edwards puts it "the 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…In effect, people affected by a breach get punished twice".[12]

The urgent need to test these claims against recently-published ICO enforcement data, the changing political context, and the ICO's impending strategic refresh mean it is a critical moment to shape the ICO's enforcement approach. The Open Rights Group is committed to providing this constructive challenge, having previously recommended legislative reforms for making the ICO more effective[13] and examined its failure to act during the Covid-19 pandemic.[14] This report builds on this work to explore how the ICO can better enforce the laws that the UK's parliament, and the citizens they represent, have asked it to.

7 https://ico.org.uk/media/about-the-ico/documents/4030348/annual-report-2023-24.pdf

8 https://www.gmal.co.uk/what-happened-recently-with-the-ico/

9 https://www.openrightsgroup.org/blog/light-and-shadow-of-the-digital-information-and-smart-data-bill/

10 https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/ico25-plan/

11 https://www.openrightsgroup.org/blog/light-and-shadow-of-the-digital-information-and-smart-data-bill/

12 https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/06/ico-sets-out-revised-approach-to-public-sector-enforcement/

13 https://www.openrightsgroup.org/publications/briefing-the-ico-isnt-working/

14 https://www.openrightsgroup.org/press-releases/org-report-finds-that-ico-failed-to-hold-the-government-to-account-over-use-of-public-health-data-during-pandemic/

2 WHAT ENFORCEMENT POWERS DOES THE ICO HOLD?

The ICO, through the UK GDPR (formerly the GDPR pre-Brexit) and Data Protection Act 2018 (DPA), has been granted powers by parliament to help it uphold the privacy rights of UK citizens. When UK public sector bodies and organisations that process the data of UK citizens breach data protection law, the ICO can use the full range of its powers to bring these organisations into line. This includes:

- **Warnings** where a proposed data processing activity threatens non-compliance.
- **Reprimands**, where data protection laws have been breached, but the incident is not considered serious enough to justify an enforcement notice or fine. Reprimands can be published publicly by the ICO, but can't be appealed by the recipient. This lack of appeal is a subject of some controversy, given the impact on the reprimanded organisation's reputation.
- **Enforcement notices** that compel an organisation to change its data protection practices. Urgent enforcement notices must be actioned within 24 hours. They can be appealed.
- **Fines,** which by way of "penalty notices", are typically issued when the ICO believes that significant harm has taken place. These fines can be up to £17.5 million or 4% of an organisation's annual worldwide turnover, depending on whichever is greater. They can also be appealed.
- **Criminal prosecution** for a narrow range of data misuses. This includes individuals that knowingly or recklessly obtain, share, retain or buy personal data without the permission of the data controller, with a view to selling that data.

The ICO also holds powers to issue information and assessment notices, that respectively compel organisations to provide information or permit a compliance assessment of their data processing activities. These powers enable the regulatory investigations that lay the groundwork for the potential use of the enforcement powers listed above.

The ICO holds similar (although not identical) powers under the other legal regimes it is responsible for enforcing. Assessment notices, warnings, reprimands, enforcement notices and penalty notices can also be issued for breaches of the Privacy and Electronic Communications Regulations (PECR) that covers electronic marketing activities. Where public sector organisations fail to adequately respond to a request for information under the Freedom of Information (FOI) Act, the ICO can issue a legally-binding decision notice that compels them to take corrective actions. If an individual or organisation deliberately destroys, hides or alters information to prevent it being released, a criminal charge can follow, but no fines can be issued under the FOI Act.[15]

15 https://ico.org.uk/for-organisations/foi/foi-complaints-and-ico-enforcement-powers/

2.1 WHAT SHAPES THE ICO'S ENFORCEMENT DECISIONS?

The ICO's decisions around if, when, and how to exercise their powers are influenced by a range of factors. Some of these factors derive from data protection law; for example Article 35 obligates the ICO to publish a list of data processing they consider to be high-risk (which in turn should inform their enforcement approach). Elsewhere the ICO's Regulatory Action Policy, participation in regulatory networks, and wider strategies (for example ICO25 and Prosecution Policy Statement) both describe and shape their thinking around enforcement. Overall, the ICO's enforcement strategy is shaped by a wide range of considerations including:

- **The "seriousness" of the breach,** considering a range of contextual factors such as the number of people affected, the duration of the incident, and the severity of the associated risks.
- **The compliance history of the organisation involved**: Repeat offenders should – in theory at least – be treated more harshly by the ICO.
- **Impact on sector norms**: The ICO's Regulatory Action Policy states that if they consider an organisation to be representative of a sector, they are likely to take firmer action to mitigate "the possibility of similar issues arising again across that group or sector if not addressed".[16]
- **Economic impacts**, including the cost to organisations of addressing the data protection breach. Under the Deregulation Act 2015 the ICO has a legal duty to consider economic growth when exercising its functions.
- **Public interest**, for example, to test an issue under dispute.
- **"Aggravating factors"** that essentially equate to general bad behaviours such as negligent organisational practice, failure to follow a sectoral code of conduct, ignoring ICO guidance, or failure to alert the ICO in an appropriate time window.
- **"Mitigating factors"** that in the ICO's view partially excuse a breach, for example including actions taken to compensate victims, the use of protective technologies, following sectoral standards, and early notification of the ICO.
- **Other regulators' actions:** the ICO considers whether other regulatory bodies are looking at the same issue. In the context of partnerships with international DPAs (for example through the Global Cooperation Arrangement for Privacy Enforcement network), they may also be more likely to take action where a joint investigation is viable.
- **Resource pragmatism,** considering the effort-to-reward ratio for potential regulatory actions. Speaking at the IAPP Data Protection Intensive in February, 2024 John Edwards summed up their current position: "Given our limited resources, we want to get the most bang for our buck and focus our efforts where we can make the biggest difference in 2024."[17]
- **Political saliency**: Whilst the ICO is in theory an independent body, it is difficult for it to shield itself from political influences in practice. This is shown in the ICO's overly permissive approach to public health data regulation during Covid-19,[18] where they worked closely with the government to advise them on data protection. The previous Conservative government even went so far as to propose enshrining political influence in law: the DPDI Bill had proposed giving government Ministers powers to designate the ICO's strategic priorities.

16 https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf

17 https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/02/john-edwards-speaks-at-iapp-s-data-protection-intensive-uk/

18 https://www.openrightsgroup.org/press-releases/org-report-finds-that-ico-failed-to-hold-the-government-to-account-over-use-of-public-health-data-during-pandemic/

On the one hand, this broad range of considerations suggests that the ICO has tried to take a nuanced and contextual view of their enforcement action. Many, if not all, of these factors are however ambiguous and often in tension. In the absence of a clear and explicit hierarchy (for example an explicit policy that economic impacts are secondary to the harms caused by the breach), the factors risk also being used as a laundry list from which the ICO can selectively choose to justify any and all decisions they make.

This issue is aggravated by the fact that the ICO's Current Regulatory Action Policy is out of date. The current policy was published under the previous Commissioner Elizabeth Denham in 2022, but sits among a number of new regulatory documents such as the data protection fining guidance[19] or the Regulatory Approach ICO25[20] document. A "regulatory risk review" project to transform the ICO's approach to regulatory action was first made public by the Commissioner in an October 2023 speech.[21] But since then the ICO has said little more, leaving others to guess at how the ICO will – or won't – use their enforcement powers.

Less obvious within the factors we have identified is the social impact of breaches to data protection. The relevance of data protection as an instrument for ensuring that equalities and human rights are protected is usually taken for granted within data protection circles, and is mentioned within the current Regulatory Action Plan. However, it is not yet sufficiently articulated, especially given the potential for AI and other technologies to create unequal and discriminatory outcomes, as we discuss below. This should be placed more centrally into the ICO's thinking regarding enforcement.

Recommendation 1:

The ICO's forthcoming Regulatory Action Policy should prioritise transparency and clarity and be subject to regular external review.

Options and actions for doing so include:

- A biyearly independent audit of the Regulatory Action Policy, evaluating both how the ICO is implementing its policy, and its impacts on regulated entities' data practices.
- Turning the Regulatory Action Policy into a live document with a clear hierarchy of enforcement policies. This should clearly articulate how enforcement-related policies interact with each other and be easy to navigate (and by extension scrutinise) in one document. The document must be updated before a substantial change in enforcement approach has happened (rather than being announced ad hoc by the Commissioner at semi-public events).
- Explaining how technology's potential for systemic impacts on equalities and human rights is factored into the enforcement strategy
- Including a statutory requirement within the DUA Bill for the ICO to publish their assessment logic and evidence base for all enforcement actions. This must also include cases they have decided *not* to investigate following UK GDPR complaints past a certain reasonable threshold.

19 https://ico.org.uk/about-the-ico/our-information/policies-and-procedures/data-protection-fining-guidance/

20 https://ico.org.uk/media/about-the-ico/policies-and-procedures/4022320/regulatory-posture-document-post-ico25.pdf

21 https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/10/john-edwards-opening-speech-at-dppc-2023/

3 HOW DOES THE ICO (MIS)USE ITS ENFORCEMENT POWERS?

The ICO's enforcement record paints a picture of caution and permissiveness across the 2023-2024 financial year. In the public sector, a middling number of reprimands stands in contrast to a scarcity of enforcement notices and fines – one fine, two enforcement notices, and 28 reprimands were issued to state bodies.

These reprimands appear to represent about half of the ICO's use of enforcement powers. In the private sector nearly all enforcement actions concerned spam, cold calling and junk mail, with many relating to the PECR regime. 20 of 21 fines and a similar number of the enforcement orders relate to these cases. Only eight UK GDPR-related enforcement actions were taken against private sector organisations, relating to security failures, data leaks, abuse of data or profiling.

Overall the ICO investigated 5.5% of the 11,680 personal data breaches reported to them, implying 642 investigations as a result. As the ICO does not publish comprehensive data on warnings issued it is not possible to provide an accurate figure of how frequently this power was used. But some details within their annual report offer a partial view – in November 2023 for example they warned "53 of the UK's top 100 websites" that they faced enforcement action if they did not make it easy for users to reject cookies.

SECTOR	FINES	ENFORCEMENT NOTICES	REPRIMANDS	TOTAL
Public	1	2	28	31[22]
Private	22	20	7	49[23]
Third sector		1	2	3[24]
Total data protection actions	23	23	37	83[25]

Table 1: summary of ICO enforcement activities in the 2023-2024 financial year

22 The total of 32 actions recorded ICO for central and local government, health, education and childcare, includes one FoI action against Shropshire Council and one against an Academy Trust. https://ico.org.uk/action-weve-taken/enforcement/?facet_type=&facet_sector=Criminal+justice&facet_sector=Local+government&facet_sector=Health&facet_sector=Central+government&facet_sector=Education+and+childcare&facet_date=custom&date_from=01%2F04%2F2023&date_to=31%2F03%2F2024

23 A total of 42 actions against marketing, financial, general business, utilities, legal, media, online retail and transport are recorded by the ICO. We included a further seven enforcement actions that were not classified, see Appendix III https://ico.org.uk/action-weve-taken/enforcement/?facet_type=&facet_sector=Marketing&facet_sector=Finance+insurance+and+credit&facet_sector=General+business&facet_sector=Utilities&facet_sector=Legal&facet_sector=Media&facet_sector=Online+technology+and+telecoms&facet_sector=Retail+and+manufacture&facet_sector=Transport+and+leisure&facet_date=custom&date_from=01%2F04%2F2023&date_to=31%2F03%2F2024

24 Achieving for Children, reprimand, https://ico.org.uk/action-weve-taken/enforcement/achieving-for-children/ Penny Appeal, enforcement notice, https://ico.org.uk/action-weve-taken/enforcement/penny-appeal/ and Finham Park Multi Academy Trust https://ico.org.uk/action-weve-taken/enforcement/finham-park-multi-academy-trust/

25 A total of 84 enforcement actions are recorded by the ICO; (one FoI enforcement order gainst Shropshire is not counted here). See Appendix III https://ico.org.uk/action-weve-taken/enforcement/?facet_type=&facet_sector=&facet_date=custom&date_from=01%2F04%2F2023&date_to=31%2F03%2F2024

3.1 PRIVATE SECTOR ENFORCEMENT

Given the low volume of enforcement activity relating to private sector data protection practice over the last year, it is difficult to offer any practical insights beyond the fact the ICO seems reluctant to enforce these laws.

The ICO's most substantial private sector fine was issued to the social media platform TikTok. This £12.7 million fine (currently under appeal) represents a substantial proportion of the total £15.65 million of monetary penalties they issued last year. Tik Tok's data protection infringements included processing the data of users aged under 13 without parental consent or an appropriate legal basis, implementing inadequate age assurance measures to identify these children, and failing to be transparent around how user data is used.

Only two other private sector fines were issued by the ICO in the last financial year. In one, a reprimand was issued against the Bank of Ireland, which had made serious errors regarding credit records.[26] This may have had significant impacts on people applying for loans and mortgages. In another case, Serco was given an enforcement order to stop using pervasive fingerprinting and facial recognition technologies for workplace monitoring purposes.[27]

Comparisons with international Data Protection Authorities (DPAs)

The ICO's soft approach to enforcement against exploitative industry data practices stands in contrast to some of its international counterparts.

The French DPA issued a 150€ million fine against Google for deceiving users into consenting to cookie banners' requests to be profiled.[28] As a result, Google implemented a "reject all" button for online tracking cookies.[29] Similarly the Belgian DPA issued a €250,000 fine against the Interactive Advertising Bureau for the illegality of its Transparency and Consent Framework, which underpins the functioning of cookie banners, and ordered the IAB to rectify its operations.[30] As a result, the updated TCF 2.2 policy now allows online tracking on an opt-in basis only, and requires a full disclosure of the companies to which personal data is being broadcasted.[31]

Meta has also been the target of several enforcement actions in the EU, and was forced to first stop forcing users' consent to behavioural profiling via its Terms of Service, then to offer an ad-free version of its service.[32] The EDPB is looking at Facebook's attempt to force users into accepting online tracking with a consent or pay choice.[33] Facebook still forces UK users to consent to behavioural profiling by embedding their consent into its Terms of Service.[34] In contrast the ICO has consulted on the "consent or pay" model, but has not yet taken action.[35][36]

---

26 https://ico.org.uk/action-weve-taken/enforcement/bank-of-ireland/

27 https://ico.org.uk/action-weve-taken/enforcement/serco-leisure-operating-limited-and-relevant-associated-trusts/

28 https://www.cnil.fr/en/closure-injunction-issued-against-google

29 https://www.lexology.com/library/detail.aspx?g=544630a5-8a25-4e39-abf6-1e726c10ead8

30 https://www.dataprotectionauthority.be/citizen/iab-europe-case-the-cjeu-answers-the-questions-referred-for-a-preliminary-ruling

31 https://iabeurope.eu/tcf-2-2-launches-all-you-need-to-know/

32 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0252 and https://www.edpb.europa.eu/news/news/2023/edpb-urgent-binding-decision-processing-personal-data-behavioural-advertising-meta_en

33 https://www.edpb.europa.eu/news/news/2024/edpb-consent-or-pay-models-should-offer-real-choice_en

34 https://www.facebook.com/legal/terms accessed from UK IP address: "We don't charge you to use Facebook or the other products and services covered by these Terms, unless we state otherwise. Instead, businesses, organisations and other persons pay us to show you ads for their products and services. Our Products enable you to connect with your friends and communities and to receive personalised content and ads that we think may be relevant to you and your interests. You acknowledge that by using our Products, we will show you ads that we think may be relevant to you and your interests. We use your personal data to help determine which personalised ads to show you."

35 https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/call-for-views-on-consent-or-pay-business-models/

36 https://www.openrightsgroup.org/publications/org-response-to-the-ico-consent-or-pay-consultation/

In the TikTok case, the ICO rightly used its powers to address problematic use of children's data in a sector – social media – where such practices are widespread. But this case unfortunately presents just as many questions as answers. The issues within the case occurred between 2018-2020, with the ICO taking three years to reach its ultimate decision. Whilst some lag is unavoidable due to the legal processes that need to be worked through, even the Commissioner himself has acknowledged that the ICO's investigations are too slow. Speaking at the DPPC 2023 he explained:

"We've identified some of the reasons for significant delays that occur in our investigations, such as over-resourcing lower-level regulatory activity. We're working to resolve those so we can be more agile and responsive to emerging issues and stop or punish harmful practices more effectively."[37]

The nature of TikTok's failure to prevent underage users accessing their platform also opens up a critical question: Why hasn't the ICO taken action against the many other social media platforms children under 13 access in contravention of user policies? Ofcom's Children's Media Use and Attitudes research highlights the scale of this problem, finding that in 2024 half of children under 13 use at least one social media site despite minimum age requirements being above this age.[38] The ICO's Children's Code, and Commissioner's Opinions on Age Assurance, both demand that they take strong action against this issue. But they have yet to do so.

This inaction reflects a pattern seen elsewhere, where the ICO is reluctant to take action against exploitative data practices that are endemic across high-value digital industries such as adtech. Here, the ICO has yet to act despite acknowledging problems since 2018 following a complaint filed by Killock and Veale against the uncontrolled flow of personal data in the adtech bidding system. This approach seems to fly in the face of the ICO's commitment within their Regulatory Action Policy (discussed in section 2.1) to prioritise enforcing against practices that raise "the possibility of similar issues arising again across that group or sector if not addressed". When faced with the prospect of tackling systemic failings across sectors, the ICO instead seems nervous about undermining the economic growth that comes with exploitative data practices – and the pushback that would inevitably occur if they were to regulate.

As we note below, many emerging technologies have the potential to create discriminatory and unfair outcomes. The ICO should make sure there is a strong understanding of these risks for private sector enforcement work.

Recommendation 2:

Independent research and legislative reform should be made to benchmark the ICO's private sector enforcement approach against other data protection authorities.

Options and actions for implementing this recommendation include:

- Amending the DUA Bill to **mandate the ICO to publish a list of priority sectors for enforcement,** where widespread data practices set problematic norms and cause harm (for example social media platform's illegal use of children's data, and the opaque adtech market). This should include information about the potential risks to equal and fair outcomes through an equalities assessment.
- UK Research and Innovation funding ongoing **independent research benchmarking ICO performance against international comparators.** This is compatible with the research council's mission to enrich lives and drive economic growth, given the important role data protection compliance plays in both. This research could be extended to other regulators with cross-economy remits.

37 https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/10/john-edwards-opening-speech-at-dppc-2023/

38 https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/media-literacy-research/children/children-media-use-and-attitudes-2024/childrens-media-literacy-report-2024.pdf?v=368229

3.2 PUBLIC SECTOR ENFORCEMENT

As noted in the introduction, in the 2023-2024 financial year, there was a substantial change in the ICO's approach to public sector enforcement, with the office opting not to fine organisations within it. As a result the majority of the notices issued in the last year were reprimands, issued against state organisations, ministries, law enforcement, health and educational bodies.

The exception to this was a fine issued to the Ministry of Defence in relation to a data leak revealing the personal identities of 245 Afghanis.[39] The ICO fined the Ministry of Defence (MoD) just £300,000, although this figure included reductions for "mitigating factors" in the difficulties surrounding the evacuation. Due to the ICO's policy not to fine public sector organisations, this fine was "reduced" from £1 million.

Two enforcement orders were also issued in 2023-2024. One was in regard of the loss of control of child abuse case files, where an employee had removed the material on a data stick subsequently used to copy movies at home. The other was against the Home Office for their trialled GPS tagging of refugees.[40] The location of 600 migrants was monitored through their GPS data, which in the ICO's view was "potentially excessive and irrelevant".

Comparisons with international Data Protection Authorities

The ICO's soft stance on public sector enforcement contrasts with the regulatory approach of many other international DPAs. Here we outline some illustrative examples of this.

The Greek DPA issued a €175,000 fine to the Ministry of Immigration and Asylum for its failure to conduct a required Data Protection Impact Assessment regarding the Centaur surveillance system, which uses CCTV and drones to track migration, and the Hyperion system, which is used to track entry and exit of people from centres.[41] In contrast, the UK Home Office has not been fined despite their long-track record of GDPR violations. The Home Office was issued three consecutive reprimands in 2022 for a number of data protection breaches,[42] recording and publishing conversations with Windrush victims without consent,[43] and a systemic failure to answer to SARs within statutory limits, with over 22,000 requests handled late.[44]

The Italian DPA has ordered the police and a number of local authorities to stop using facial recognition technologies until a legal framework is established by the Government.[45] In the UK, the police have not been sanctioned for their failure to stop using live facial recognition technology, despite the fact that a UK Court found it was illegal in the absence of an established legal framework.[46]

The Norwegian DPA ordered the rectification of exams' results in a case similar to the A-level algorithm scandal in the UK, which the ICO reacted weakly to.[47] The Danish DPA has ordered schools to stop relying on Google Workspace due to the privacy risks it constituted for children.[48] This followed several EU DPAs enforcing against Google Analytics following the Schrems II judgement.[49]

39 https://ico.org.uk/action-weve-taken/enforcement/ministry-of-defence-1/

40 https://ico.org.uk/action-weve-taken/enforcement/home-office/

41 https://www.computerweekly.com/news/366580074/Greek-government-fined-over-AI-surveillance-in-refugee-camps

42 https://ico.org.uk/action-weve-taken/enforcement/secretary-of-state-for-the-home-department/

43 https://ico.org.uk/action-weve-taken/enforcement/secretary-of-state-for-the-home-department-home-office/

44 https://ico.org.uk/action-weve-taken/enforcement/secretary-of-state-for-the-home-department-home-office-1/

45 https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9823282

46 https://www.bbc.co.uk/news/uk-wales-53734716

47 https://www.dataguidance.com/news/norway-datatilsynet-issues-order-ibo-rectify-unfairly

48 https://www.edpb.europa.eu/news/national-news/2022/danish-dpa-imposes-ban-use-google-workspace-elsinore-municipality_en

49 https://noyb.eu/en/update-cnil-decides-eu-us-data-transfer-google-analytics-illegal

The gravity of the public sector's data mispractice is clear: Leaks of Afghanis data posed a direct risk to their lives, given the implications of the Taliban government becoming aware of these people's intentions to seek political refuge. Migrants are also particularly vulnerable to disproportionate surveillance given the political attention on immigration, and their relative lack of resources and rights to challenge data-driven systems.

3.3 REPRIMANDS IN THE PUBLIC SECTOR

The ICO issued 28 reprimands to the public sector over the last financial year. In several cases, police, prosecutors or the NHS exposed personal address details of victims of abuse, or witnesses to crime, to their abusers or those they were accusing, creating immediate personal, physical risks. In one example involving Thames Valley Police, the person affected had to move house.[50] In another, patients of the University Hospital of Derby and Burton NHS Trust (UHDB) did not receive medical treatment for up to two years.[51] Some of the cases investigated by the ICO had major impacts on both individuals' privacy and the functioning of the organisations involved. In one case, two police authorities, West Mercia Police and Warwickshire Police, lost the detailed records of investigations they had made, retaining only the "sanitised" or summary versions. This could have impacted prosecutions or caused potential miscarriages of justice.[52] Elsewhere two police authorities, Sussex Police and Surrey Police, recorded the conversations of hundreds of thousands of individuals without their consent.[53]

These cases – and many others detailed within Appendix II of this report – show the gravity of the issues at stake. However, the ICO's implied policy is to only use its strongest enforcement powers where breaches have posed a direct threat to life or involve child abuse. To justify this, we would expect there to be substantial evidence that reprimands lead to genuine changes in public sector practice. Sadly, this evidence is lacking.

Despite the enforcement actions taken against the MoD and the Home Office (described in section 3.2), and the seriousness of the issues at stake, it should be noted that both of these departments have continued to face data protection challenges. The MoD has since suffered further data breaches, including the recent loss of personnel records.[54] The scheme and practice of GPS tagging of migrants awaiting immigration decisions continues, despite concerns over the proportionality and accuracy of the GPS tagging systems. In some cases, migrants awaiting decisions on "bail" have even been forced by the Home Office to continue to wear tags that were malfunctioning or broken.

The reprimand issued to West Midlands Police (WMP) is another case of repeat offending. The force made a catalogue of errors between 2020-2022 due to mixing the personal data of a crime victim and suspect – including attending the wrong address when attempting to find a person regarding serious safeguarding concerns and incorrectly visiting the school of the wrong person's child. It appears to be clear that a reprimand was not a strong enough deterrent in this context, because WMP did not take steps to rectify the error with the urgency required in the first instance.[55]

SARs are an important vehicle for ensuring individuals' privacy and safety. People may use SARs, for example, if they are concerned about their health treatment from the NHS, attempting to resolve employment or benefit disputes, or seeking to understand why they have been investigated by police or

50 https://ico.org.uk/media/action-weve-taken/reprimands/4025394/tvp-reprimand-20230530.pdf

51 https://ico.org.uk/action-weve-taken/enforcement/university-hospital-of-derby-and-burton-nhs-trust-uhdb/

52 https://ico.org.uk/action-weve-taken/enforcement/chief-constable-west-mercia-police-and-chief-constable-warwickshire-police/

53 https://ico.org.uk/action-weve-taken/enforcement/sussex-police/

54 MoD data breach: UK armed forces' personal details accessed in hack, 6 May 2024, https://www.bbc.co.uk/news/uk-68966497

55 https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/03/ico-reprimands-west-midlands-police-for-data-protection-failure/

prosecutors.[56] Since 2018 however, the ICO has also been attempting to get three authorities to deal with their SAR backlogs without success. This year, six years after this problem first became apparent, Plymouth City Council, Devon and Cornwall Police and Dorset Police were each sent a "final reprimand".

AUTHORITY	BACKLOG SINCE	BACKLOG DETAILS
Plymouth City Council[57]	2018	Up to two years wait
Norfolk County Council[58]	April 2021	Over half of SARs handled late since April 2021
London Borough of Lewisham[59]	January 2022	35% of requests handled late
Chief Constable Devon and Cornwall Police[60]	2018	33% over seven months late, 19% over one year old
Chief Constable Dorset Police[61]	2018	33% over seven months old, 24% over one year

Table 2: Overview of Subject Access Request Backlogs

Lastly, the ICO's position on public sector reprimands is partially contradicted by the fine it issued to the Central Young Men's Christian Association, in April 2024 just outside the financial year.[62] Part of the ICO's logic in withholding fines to the public sector is that data breach victims "pay twice" through the impact fines have on the provisions of the public service that support these victims. This must surely also be true in the charity sector, where organisations face even more acute financial challenges relative to public sector bodies funded through taxation.

56 The Gangs Matrix, operated by the Metropolitan Police, is a good illustration of the potential effect of late processing of SARs. The Gangs Matrix was a watchlist of people who the police had designated as "gang nominals" based on vague criteria, such as who your family and friends were and what music videos you shared online. When Awate Suleiman submitted a SAR to the Met Police to enquire whether he was on the Gangs Matrix database, it took the Met 30 months to respond. Suleiman spent years fearing he was on the Matrix as a result of experiencing over-policing, including being arrested for offences he did not commit. It was only once he launched legal proceedings that he was told that he was not on it. As a result of the legal challenge brought by Liberty on behalf of Awate Suleiman and UNJUST, the Met were forced to concede that the operation of the Matrix was unlawful as it breached the right to a private and family life.

57 https://ico.org.uk/action-weve-taken/enforcement/plymouth-city-council/

58 https://ico.org.uk/action-weve-taken/enforcement/norfolk-county-council/

59 https://ico.org.uk/action-weve-taken/enforcement/london-borough-of-lewisham-reprimand/

60 https://ico.org.uk/action-weve-taken/enforcement/chief-constable-devon-and-cornwall-police/

61 https://ico.org.uk/action-weve-taken/enforcement/chief-constable-dorset-police/

62 https://ico.org.uk/action-weve-taken/enforcement/the-central-young-men-s-christian-association-mpn/

Recommendation 3:

The ICO should use the full range of its enforcement powers in the public sector – until and unless it can prove alternative approaches result in a substantial improvement in data protection compliance.

Options and actions for implementing this recommendation include:

- **Publishing all evidence resulting from the two-year "public sector approach trial"**[63] where public sector organisations were only fined as a last resort. If the evidence paints the pilot in a positive light, they should launch an external consultation and enable an independent audit of relevant data to validate their findings.
- **Parliament exploring approaches for mitigating the potential impact of public sector fines on public services and data protection breach victims.** This could for example include ensuring a proportion of income from fines is invested in improving public sector data protection practices, or through establishing compensation or financial support funds for people impacted by breaches.
- Amending the **DUA Bill to ban the ICO from issuing more than one reprimand to an organisation**. Any subsequent breaches should result in an escalation of action – not additional "final reprimands" that both undermine the premise of the initial reprimand and have little impact on behaviour.
- Amending the **DUA Bill to require the ICO to publish a league table of public sector bodies' subject access request (SAR) performance.** Organisations who consistently fail to meet the required SAR standards compliance could then be prioritised for enforcement.

63 Source: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/06/ico-statement-on-its-public-sector-approach-trial/

4 WHY ISN'T THE ICO ENFORCING THE LAW?

The ICO's poor enforcement record points to two overarching issues. Firstly, their approach to enforcement is beset by practical and legal challenges. And secondly that enforcement is falling down the list of their priorities, as the office is increasingly distracted by emerging technologies, internal flux, and political distractions. The following sections unpack these issues, and outline our recommendations for addressing them so that the ICO can better enforce the laws it is entrusted with.

4.1 ENFORCEMENT MISSTEPS ENGENDER CAUTION

Even on the occasions when the ICO has decided to enforce, they have frequently encountered damaging reversals through appeals. These struggles divert substantial resources to engage with associated legal processes and come with plenty of reputational risks, which in turn make the ICO less likely to enforce in the future for fear of being dragged into these situations again.

In 2020, the ICO made a humbling climbdown in relation to the fine it issued to British Airways, reducing an initial £163 million fine to only £20 million after the airline contested aspects of the ICO's decision.[64] The ICO opted not to publicly explain exactly how and why it had changed its mind – suggesting they were not keen to draw attention to the flaws inherent in the logic of their initial decision. In November 2023, the office was forced to issue a public apology to the former CEO of Natwest Group, Alison Rose, for prematurely and incorrectly issuing a public statement that she had breached the UK GDPR.[65]

A few months later in April 2024, the Upper Tribunal court dismissed the ICO's appeal against a previous related First Tier Tribunal ruling that struck down several aspects of an enforcement notice issued to Experian. The aspects of the initial February 2023 ruling for this case relating to enforcement strategy were not flattering to the Commissioner. The court noted that the ICO "fundamentally misunderstood the actual outcomes of Experian's processing",[66] which in turn led to disproportionate enforcement strategies. The ICO did not help themselves by failing to produce an economic impact assessment to accompany their enforcement decision – a basic cornerstone of any regulator's rationale for developing fines and regulatory interventions. The ICO has, to its credit, recently published an updated framework for how it decides to issue penalties and fines. But it remains to be seen if and how these changes will be effective.

It is worth noting that the ICO is not solely to blame for its legal woes, as the system it works within has sometimes failed to reach the standards required of it. The 2024 Upper Tribunal ruling for example concludes that "many of the points raised in this appeal could have been avoided if the [First Tier tribunal] had provided a timely and better reasoned decision."[67] If the ICO feels uncertain about how it will be treated within the tribunal system, this presumably will only lead to further reticence to enforce.

---

64 It should be noted that the fine issued was £30 million, but £6 million was deducted to account for various mitigating factors and £4 million was deducted to account for the impact of the COVID-19 pandemic on British Airway's finances.

65 https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/11/an-apology-from-the-ico-to-dame-alison-rose/

66 https://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i3176/Experian%20Limited%20EA-2020-0317%20FP%20(17.02.23).pdf

67 https://www.google.com/url?q=https://www.judiciary.uk/wp-content/uploads/2024/04/Information-Commissioner-v-Experian-Judgement-1.pdf&sa=D&source=docs&ust=1729594415585258&usg=AOvVaw3-SB_SJCBfkvneLblTw1-R

Finally, the ICO issued a £7.5 million fine and a facial recognition database deletion order to Clearview AI. In the case of the latter, the ICO has however been beset by familiar challenges: In November 2023 the First-tier Tribunal ruled that the UK data protection law could not have an extraterritorial effect in this case, meaning the Delaware-incorporated Clearview AI won their appeal. Notably, a central aspect of this ruling that determined the result is that the ICO did not dispute "that the acts of foreign governments would be within the material/territorial scope of the Regulations".[68] As some prominent data protection experts have noted, this interpretation of the GDPR is fundamentally flawed[69] and, indeed, none of the enforcement notices and fines against Clearview AI issued in Europe has been successfully challenged to date. It follows that the overturning of the ICO's fine against Clearview AI seems more akin to a self-inflicted defeat, whose root causes ought to be investigated.

Difficulties with enforcement create the potential for ICO policy and guidance to develop differently to what it will enforce against. We have noted this regarding adtech, where the ICO's policy work identified widespread legal non-compliance, but no enforcement took place, and regarding political parties, where ICO guidance has been stricter than practice. Indeed, it can become easier not to enforce for fear of undermining the ICO's policy position.

These issues are compounded on the international stage. The ICO's workload is now much larger relative to when the UK was inside the European market, where matters were made easier for both data controllers and DPAs by the GDPR's "one-stop shop" mechanism. The office no longer has access to the various cooperation mechanisms provided by the European Data Protection Board, nor the ability to take joint cross-border enforcement actions with European DPAs. The latter is particularly significant when considering the dynamic between the ICO and major multinational companies – the threat of losing access to the European market is no longer there.

Similarly in North America, it remains to be seen whether the 2023 UK-US Data Bridge agreement is a bellwether for a deepening alignment of data protection standards and cooperation between these regions. Significant uncertainty – stemming from the UK governments' DISD Bill reforms, increasingly divergent US state data protection laws, and debates around a US federal Act – means the ICO is unlikely to be able to count upon significant regulatory collaboration with US bodies for the foreseeable future.

Recommendation 4:

The ICO should publish "lessons learnt" and develop international agreements that reduce the risk of enforcement action challenge.

Options and actions for implementing this recommendation include:

- Securing commitments from international regulatory agencies (where formal cooperation agreements exist) to **compel organisations subject to enforcement actions in those regions to demonstrate how they comply with UK data protection law.** This should include the European Data Protection Board and international DPAs, and other UK sectoral regulators such as the CMA where relevant.
- **Conducting an internal review of decision-making underpinning enforcement actions overturned by the Information Tribunal,** to identify the root causes of failure to meet legal standards. This evidence should be periodically reported to the Science, Innovation and Technology Select Committee, or Parliament.

68 https://caselaw.nationalarchives.gov.uk/ukftt/grc/2023/819

69 https://www.ianbrown.tech/2023/10/18/uk-tribunal-fundamentally-wrong-on-clearview/

4.2 GRAPPLING WITH AI AND EMERGING TECHNOLOGIES

Of all emerging technologies, AI represents arguably the biggest challenge for the ICO, and wider society. The myriad issues they pose to privacy and data protection span the enablement of excessive surveillance, undermining security, insufficient transparency and avenues for exercising data rights, and intrusive profiling. Risk of bias and prejudice within AI systems are also well documented and substantial – both in their ability to perpetuate biases inherent in model training datasets, and through further prejudicial outcomes and outputs produced by black-box models.[70] Articulated in terms of data protection law, these risks collectively have the potential to undermine many of the fundamental principles of the UK GDPR – including those related to fairness, transparency, purpose limitation, security, accuracy and accountability.

The complexity, and sheer scale, of AI and associated risks means the ICO faces a daunting challenge. Their May 2024 Regulating AI: The ICO's Strategic Approach is their most recent articulation of how they plan to respond to it. It describes an approach that "drives forward the principles of the [previous Government's] AI regulation White Paper" through a range of policy, advice and regulatory action.[71]

The ICO's substantive activities on AI have primarily taken the form of guidance for controllers, research and interventions to shape the public debate. This focus on deep research and debate is mirrored in their wider approach to emerging technologies, for which they have established a dedicated Emerging Technologies team to look at technological developments on a "two to seven year" time horizon.[72] This function administers a grants programme, coordinates an external Technology Advisory Panel, and conducts internal and partnership horizon scanning research.

Compared to this wellspring of engagement and research, the ICO seemingly places relatively little focus on regulatory action. Of the 73 paragraph points within their AI strategy only three concern such action, whilst there is no mention at all of enforcement activities on their Our Work on Artificial Intelligence page.[73] Open Rights Group has complained to the ICO about Meta's plans to harvest user data to develop their AI models, but only recently received a reply to discuss our concerns.[74] The ICO has since decided to summarily close our and other people's complaints.

Similarly in the public sector the ICO has seemingly paid little attention to enforcing against the use of AI, beyond issuing a reprimand to Chelmer Valley high School for using facial recognition for cashless catering.[75] This is in spite of both the political push to roll out these systems across the public sector (for example in the context of the AI Opportunities Action Plan),[76] and the substantial risks inherent in them. For example, Durham Constabulary used the Harm Assessment Risk Tool (HART) to decide the probability of a person committing a crime. The prediction was based on personal characteristics including a person's age, gender and postcode, alongside crude and discriminatory data categories such as 'cramped house' and 'jobs with high turnover.'

This soft approach stands in stark contrast with that of some of the ICO's international counterparts. In March 2023 for example the Italian DPA issued an emergency order banning the use of ChatGPT until OpenAI had satisfied their regulatory concerns, having

70 In the private sector, examples have already been highlighted in cases raised by Uber workers and others, for instance, in hiring and firing situations.

71 https://www.skadden.com/-/media/files/publications/2024/05/the-uk-ico-publishes-its-strategy-on-ai-governance/regulating-ai-the-icos-strategic-approach.pdf

72 https://ico.org.uk/media/about-the-ico/disclosure-log/4029241/ic-293137-k4y5-team-descriptions.pdf

73 https://ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence/

74 https://www.openrightsgroup.org/blog/the-ico-is-leaving-an-ai-enforcement-gap-in-the-uk/

75 https://ico.org.uk/action-weve-taken/enforcement/chelmer-valley-high-school/

76 https://www.gov.uk/government/publications/artificial-intelligence-ai-opportunities-action-plan-terms-of-reference/artificial-intelligence-ai-opportunities-action-plan-terms-of-reference

previously imposed a temporary limitation of processing on TikTok in relation to their content targeting's role in the death of a young Italian child. The South Korean Personal Information Protection Commission has also fined Open AI for privacy law breaches, whilst DPAs across Japan, North America Latin America, and Europe have issued formal warnings or launched investigations into ChatGPT's data practices.[77] The UK has also recently signed an international treaty on AI safety[78], which includes commitment to uphold the rule of law and "protect human rights, including ensuring people's data is used appropriately, their privacy is respected and AI does not discriminate against them". The ICO has yet to comment or respond to this treaty.

Meanwhile the three AI-related enforcement interventions taken recently by the ICO include enforcement notices issued to Serco Leisure and Snap Inc (the latter only preliminary).

Recommendation 5:

The data protection risks of AI should be managed through better use of ICO transparency and data restriction powers, and legislative reforms to promote risk transparency.

Options and actions for implementing this recommendation include:

- **Establishing a mandatory UK-wide public sector AI registry** through the Data Use and Access Bill. This would ensure transparency to citizens using these systems, and enable external scrutiny of the ICO's decisions not to investigate these applications. This could follow the precedent set by the Scottish government AI Register.[79]
- **Issuing temporary data processing prevention orders to high-risk emerging technologies** that have systemic privacy impacts, until these applications can prove they are compliant with data protection law. This could include frontier AI models demonstrably trained on UK citizen data or automated public sector decision-making, and follows the precedent set by other European DPAs.
- **Compelling frontier AI model developers to provide the ICO with detailed information about the provenance of model training data.** This legal requirement could be enshrined in the DUA Bill, or in the forthcoming AI Bill.
- **Publishing an Action Plan for the ICO to deliver on its international treaty commitments on AI safety.**[80] This could be incorporated in the updated ICO Strategic Approach on Regulating AI.[81]

77 https://fpf.org/blog/how-data-protection-authorities-are-de-facto-regulating-generative-ai/

78 https://www.gov.uk/government/news/uk-signs-first-international-treaty-addressing-risks-of-artificial-intelligence

79 Source: https://scottishairegister.com/

80 Source: https://www.gov.uk/government/news/uk-signs-first-international-treaty-addressing-risks-of-artificial-intelligence

81 Source: https://ico.org.uk/media/about-the-ico/consultation-responses/4029424/regulating-ai-the-icos-strategic-approach.pdf

4.3 MISREADING THE "GROWTH DUTY"

The ICO's caution may sometimes be explained by its perceived need to 'balance' commercial incentives for innovation against enforcement actions. This would – in our view – however be a misreading of government guidance regarding the statutory Growth Duty placed on regulators in Section 108(1) of The Deregulation Act 2015.[82] The associated guidance[83] makes it plain that non-compliance poses a risk of encouraging damaging practices and unfair competition.

"The Growth Duty does not legitimise non-compliance with other duties or objectives, and its purpose is not to achieve or pursue economic growth at the expense of necessary protections. Non-compliant activity or behaviour [...] also harms the interests of legitimate businesses that are working to comply with regulatory requirements, disrupting competition and acting as a disincentive to invest in compliance" [84]

The Guidance identifies "competition" as one of seven "Drivers of Economic Growth", and within this, has indicators for regulators to ensure they are delivering competition benefits including "Consistency – application of rules and policies are adopted and/or maintained with the minimum distortion to competition" and "Changing rules or other regulatory levers to help to level a playing field where justified competition should be occurring".[85]

The guidance is clear and accurate in the risks it identifies, but regulatory caution from the ICO appears to be causing exactly these problems, for example regarding adtech and AI. A lack of enforcement allows non-compliant actors to unfairly compete in these fields, yet the ICO does not take action, apparently for fear of restricting economic growth. Notably, the need to ensure a level playing field for legitimate businesses is absent from the commentary on economic growth duties in the ICO's draft regulatory guidance.[86]

Recommendation 6:

The ICO should clarify how it interprets the Growth Duty in its enforcement approach.

Options and actions for implementing this recommendation include:

- Including explicit detail on how it will **prevent unfair competition and consumer harm from data protection non-compliance in the ICO's updated Regulatory Action Policy**. This is a Growth Duty obligation. In doing so the ICO should formally consult with the CMA and refer to competition law enforcement decisions where the competition implications of data assets were considered.
- Ensuring the **list of priority sectors for investigation (outlined in recommendation 2) explicitly factors in areas where data protection practices may create unfair competition**.

82 https://www.legislation.gov.uk/ukpga/2015/20/section/108

83 https://www.legislation.gov.uk/ukpga/2015/20/section/110 Guidance made under s. 110(1)

84 https://www.gov.uk/government/publications/growth-duty PDF p.7

85 Ibid, p.16

86 Regulatory action policy draft (2021), ICO, p. 12 https://cy.ico.org.uk/media/about-the-ico/consultations/4019400/regulatory-action-policy-2021_for-consultation.pdf

4.4 ASSURANCE AND INTERNAL FLUX DISTRACT FROM ENFORCEMENT

The ICO's bruising encounters with enforcement decision appeals – alongside their rush to try and catch-up with emerging technology development – have led the ICO to reframe their regulatory approach. The ICO25 Strategic Plan (which sets out current Commissioner John Edwards' vision for the ICO) describes a shift towards light-touch engagement and assurance, at the expense of enforcement.[87]

Central to this strategy is the ambition to provide "regulatory certainty" to regulated organisations, to in turn, "[empower] responsible innovation and sustainable economic growth". Under this new strategic worldview, compliance with data protection law happens by giving companies better information about its requirements and benefits at an early stage, and praising compliant organisations to create reputational incentives for good behaviour. Resources are diverted towards functions that help with this deepened engagement – beefing up communications, innovation, assurance, and sandbox teams.[88] The approach can be summed up in the words of John Edwards, who in a speech at the May 2024 New Statesman Emerging Technologies summit affirmed his intention to "move away from being "the regulator of no". We want to say, how to, not don't do".[89]

The ICO's vision of regulatory certainty and assurance is a hopeful one, but seemingly naive in places. Supply (and by extension demand) for third-party data protection certification schemes – a core assurance vehicle that the ICO has previously had a dedicated team devoted to – seems chronically low. Since the introduction of the GDPR and Data Protection Act in 2018, the ICO has approved only five certification schemes.[90] Across Europe, all regulators have collectively also approved five in total.[91] The number of regulatory assurance audits completed by the ICO dropped from 94 in the 2022-23 financial year to 64 in 2023-24. Calls to the ICO helpline and live chat requests are also down, dropping from a combined 457,520 engagements in 2021-22 to 339, 654 in the most recent financial year.[92] There are caveats to this data – the advice engagement figures include requests from the public, and an argument could be made that the decline is because growing data protection knowledge means less advice is required. But regardless, it seems difficult to argue that organisations collectively want the deepened engagement and assurance promised by ICO25.

The fourth strategic objective within this strategy is to "Continuously develop the ICO's culture, capacity and capability".[93] In practice, the ICO have committed themselves to build better processes for prioritising issues, being more "empathetic" (through greater stakeholder consultation), increasing transparency of their work, and building the technical capability of their workforce. Alongside this, the ICO is implementing an Enterprise Data Strategy and a "High-performance strategy" with a view to modernising their internal infrastructure and practice.

A closer examination of the data strategy reveals some interesting self-reflections. Using the Central Digital and Data Office's

87 It should be noted that the ICO's Regulatory Action Policy would typically be the publication that provides the most detail on their regulatory posture and approach. The Regulatory Action Policy listed on their website however pre-dates the appointment of John Edwards – so ICO25 seems likely to be more reflective of their current approach.

88 The ICO's Regulatory Sandbox seeks to "support organisations who are creating products and services which utilise personal data in innovative and safe ways." Participating organisations developing these innovations do so under the regular supervision of the ICO, who advise them on potential data protection issues associated with their products. Source: https://ico.org.uk/for-organisations/advice-and-services/regulatory-sandbox/

89 https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/05/no-regulatory-wild-west-how-the-ico-applies-the-law-to-emerging-tech/

90 https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/02/ico-approves-legal-services-certification-scheme/

91 https://www.edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_en

92 https://ico.org.uk/media/about-the-ico/documents/4030348/annual-report-2023-24.pdf

93 https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/ico25-strategic-plan/how-we-will-know-if-we-have-achieved-our-objectives/4-continuously-develop-the-ico-s-culture-capacity-and-capability/

Data Maturity Assessment framework to assess their data-related skills the ICO sees strength in its investment into, and leadership support for, data capabilities. But it faces challenges around creating a culture of data use and, perhaps ironically, developing 'more granular' data governance.[94] These reflections (and the evidence-related challenges it has previously faced building enforcement cases) collectively paint a picture of an office that has sincere and commendable intention to become a modern data-enabled regulator, but has yet to realise these ambitions.

These substantial internal reforms are taking place against a backdrop of a parliamentary system that demands the ICO engages with government regulatory reforms in places, whilst in others seems uninterested in providing constructive challenge. Substantial organisational resources (presumably including a number of policy and legal specialists) have been diverted to engaging with the UK's data protection reforms, as evidenced by the establishment of a Legislative Reform directorate. Elsewhere the ICO has even established dedicated functions to engage with digital regulations beyond data protection, including Competition and Regulatory Cooperation and Online Safety teams.[95]

Recommendation 7:

The government should commit to providing additional funding to the ICO for functions that solely focus on engaging with non-data protection issues (for example online safety).

This would ensure these functions do not come at the expense of delivering the ICO's core regulatory remit, and could be part of ICO reforms considered in the DUA Bill.

4.5 A LACK OF LEGAL ACCOUNTABILITY

The UK GDPR and Data Protection Act make the ICO accountable for its decisions, in particular through enabling them to be challenged at the Information Tribunal appeals court. The UK GDPR retains Articles 78 and 79 which require the legal accountability of the ICO's decisions, so that data subjects can ensure that they can seek redress if they believe the ICO has not dealt with their complaint in a way that ensures their data protection rights are respected. In Europe, the Court of Justice has been very clear that the data subjects must be able to enforce their rights, and that DPAs have the "responsibility for ensuring that the GDPR is fully enforced with all due diligence" rather than permitting wide discretion over what is enforced against.[96] Bringing these strands together, there is clear potential for the Information Tribunal to act as a mechanism for data subjects to seek redress where they feel the ICO has not adequately upheld their rights. Professor David Erdos in 2020 proposed that the Information tribunal could use its powers to ask the ICO to progress complaints, for example.[97]

However, the Information Tribunal has taken a narrower view of its remit, leaving a judicial review as the primary route for a data subject to challenge the Commissioner if they feel they have been treated unfairly. The costs and complexities of such a review mean that it is prohibitively difficult to challenge the ICO through legal routes if it fails to uphold data protection rights after a complaint. Furthermore, the recent Delo decision at the Court of Appeal[98] has reinforced the ICO's view that it has "broad discretion" over what complaints it handles and how.[99]

94 https://dataingovernment.blog.gov.uk/2024/07/24/information-commissioners-office-unveils-data-strategy-how-we-are-shaping-the-future-of-data-in-regulating-information-rights/

95 https://ico.org.uk/media/about-the-ico/disclosure-log/4029241/ic-293137-k4y5-team-descriptions.pdf

96 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0311

97 Erdos, David, Accountability and the UK Data Protection Authority: From Cause for Data Subject Complaint to a Model for Europe? (January 17, 2020). University of Cambridge Faculty of Law Research Paper No. 14/2020, Available at SSRN: https://ssrn.com/abstract=3521372 or http://dx.doi.org/10.2139/ssrn.3521372

98 Ben Peter Delo, R (on the application of) v The Information Commissioner [2023] EWCA Civ 1141

99 https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/10/court-of-appeal-rules-ico-acted-lawfully-in-subject-access-request-complaint-litigation/

The Information Tribunal has itself twice complained about the situation, observing in Scranage that:

"There is a wider jurisdictional issue in play here. Plainly the GDPR requires that data subjects have an 'effective judicial remedy' against both a 'supervisory authority' (here, the Commissioner) and a data controller or processor (see GDPR Articles 78 and 79 respectively).

Domestic legislation provides that procedural redress against the Commissioner under Article 78(2) is sought from the Tribunal whereas substantive redress under Article 79 must be pursued in the courts (being the county court or the High Court). The policy reason for this jurisdictional disconnect, which is hardly helpful for litigants in person, or for developing a coherent system of precedent, is not immediately apparent. A comprehensive strategic review of the various appellate mechanisms for rights exercisable under the DPA is arguably long overdue."

The Information Tribunal in Killock & Veale stated in its judgement that it "would endorse those observations".[100]

The result of the current situation, in our view, is that the ICO does not in practice have to worry about data subjects challenging a lack of enforcement following a complaint. As the ICO has had considerable difficulties in taking enforcement action against companies as noted above, this creates considerable risks that the public's data rights are not adequately being defended.

5 A LACK OF INDEPENDENT OVERSIGHT

Addressing the myriad challenges facing the ICO cannot be left to the regulator alone. The reputational costs of owning internal cultural shortcomings (such as the misreading of the growth duty, or assurance displacing enforcement) mean the ICO is not likely to acknowledge them. Looking externally, it is not the ICO's place to comment on laws set by parliament that define its remit, and organisational accountability. Against this backdrop, it is clear that the ICO requires deeper external oversight of its work.

Oversight, in this context, is ultimately an umbrella term for a range of different areas where the ICO requires support or constructive challenge. This includes:

- Scrutiny of enforcement approach, considering whether the ICO's discretionary decisions collectively meet the commitments outlined in their Regulatory Action Policy.
- Validation of enforcement approach, evidencing the degree to which the Regulatory Action Policy upholds data protection law in the real world.
- Scrutiny of the appointment of the Commissioner and other senior leaders, to ensure the process is free from undue political interference and the appointee is sufficiently independent.
- Ensuring effective routes of appeal and redress where individuals and organisations disagree with outcomes of their complaints.
- Wider scrutiny of its general conduct, including transparency around enforcement rationale, spending, and adherence to professional and regulatory standards.

100 https://www.gov.uk/administrative-appeals-tribunal-decisions/james-killock-and-michael-veale-v-ico-ew-v-ico-eveleen-coghlan-on-behalf-of-c-v-ico-2021-ukut-299-aac

The ICO does not, of course, operate free from any external oversight currently. They are held generally accountable by Parliamentary Select Committees (before which the office appears occasionally), and the Treasury signs off spending bids submitted to them by the office. The Information Tribunal scrutinises some of the Commissioner's regulatory decision-making, whilst the Parliamentary and Health Service Ombudsman has oversight of the office's progression and handling of complaints.[101] Collectively however these relationships seem insufficient: oversight is too often ad hoc, external bodies (in particular the Information Tribunal) lack capacity or remit, and significant accountability gaps remain.

5.1 WHO SHOULD PROVIDE OVERSIGHT AND WHEN?

The ICO's remit to regulate all government departments, the office's reliance on the Treasury to provide funding, and ongoing dialogue with DSIT around data protection reforms mean oversight of the ICO creates a serious conflict of interest for Ministers. It is the Open Rights Group's strong view that these potential conflicts of interest must be avoided, and that effective accountability must be provided primarily by those outside of government.[102]

A more suitable alternative is Parliament, which is both relatively free from the aforementioned conflicts of interests and representative of a broader range of the political spectrum. In 2006, the Commons Select Committees on Constitutional Affairs recommended to make the Information Commissioner "directly responsible to, and funded by, Parliament",[103] noting that "the level of funding for the ICO can have a direct impact on its capability to enforce compliance"[104] and that "in other comparable jurisdictions such as Canada, New Zealand and Scotland, the ICO is funded directly by Parliament".[105] In 2014, the Commons Select Committee on Public Administration reiterated that "The Information Commissioner [...] should be more fully independent of Government and should report to Parliament".[106] The Committee noted the Chief Inspector of Prisons' opinion that being appointed by the Ministry would be "by its nature incompatible with full independence".[107] Gordon Brown's Commission on the UK's future report recommended that "Parliament which, unlike Whitehall, is accountable to the people, should take over responsibility for the Information Commissioner's Office to place central government under more effective scrutiny".[108]

The Institute for Government (IfG) report on Reforming Public Appointments recommended that "Appointments to roles that scrutinise the actions of politicians and the government [...] should be made public appointments and should be subject to a veto from the relevant House of Commons select committee".[109] The depth and scale of the ICO institutional issues warrants a bolder, more radical reform. Nonetheless, the IfG recommendations represent solid advice for public appointments at large, and could constitute a first, compromise step toward a greater parliamentary involvement in the oversight of the ICO.

Elsewhere, observers have called for other legal and regulatory institutions to hold the ICO to account. Professor David Erdos has for example recommended that the Equality and Human Rights Commission (EHRC) provide holistic

---

101 Source: https://ico.org.uk/about-the-ico/who-we-are/decision-making-structure/#:~:text=The%20Information%20Commissioner%20is%20held,DSIT)%20to%20Treasury%20spending%20reviews

102 See: https://www.openrightsgroup.org/publications/briefing-the-ico-isnt-working/

103 https://publications.parliament.uk/pa/cm200506/cmselect/cmconst/991/99109.htm#a22%2044

104 Ibid

105 Ibid

106 https://publications.parliament.uk/pa/cm201415/cmselect/cmpubadm/110/11009.htm

107 Ibid

108 https://labour.org.uk/wp-content/uploads/2022/12/Commission-on-the-UKs-Future.pdf

109 https://www.instituteforgovernment.org.uk/sites/default/files/publications/reforming-public-appointments.pdf https://www.instituteforgovernment.org.uk/sites/default/files/publications/reforming-public-appointments.pdf

scrutiny of the ICO's enforcement track-record from a human rights perspective.[110] The ICO's Children's Code – which is grounded in the United Nations Convention on the Rights of the Child – is emblematic of the close relationship between data protection and human rights, which gives the EHRC an appropriate lens through which to assess the ICO's impacts. As discussed in section 4.5 the remit of the Information Tribunal, who currently only scrutinise the procedural aspects of ICO decisions, could be broadened to permit wider challenge of ICO enforcement inaction.[111]

Lastly, novel or emerging institutions have the potential to strengthen ICO oversight. To reduce the caseload on the Information Tribunal, a Data Rights Ombudsman could for example be established as a backstop for the public to turn to where they feel the ICO has inadequately responded to their complaints. A precedent for this can be seen in the financial sector, where the Financial Regulators Complaints Commission provides an independent assessment of complaints against the Financial Conduct Authority, the Payment Systems Regulator, and the Prudential Regulation Authority.[112] The recently-established Regulatory Innovation Office could also have offered a potential means of setting and overseeing enforcement targets from the ICO. However, given recent announcements that the body will sit within DSIT and focus solely on space, engineering biology, healthcare technology, and autonomous systems,[113] that opportunity appears to have been missed.

None of these ideas or institutions discussed above are a silver bullet; all face their own barriers to providing adequate oversight to the ICO. The House of Lords Industry and Regulators Committee's February 2024 Who watches the watchdogs? Improving the performance, independence and accountability of UK regulators report found that parliamentary oversight of regulators is typically "reactive and piecemeal, rather than systematic and routine".[114] The House of Lords Communication Committee's 2021 Digital Regulation inquiry led to similar conclusions – ultimately recommending the establishment of a new "Joint Committee on Regulation" to better hold digital regulators such as the ICO to account. In short, if the Parliament is to provide this accountability function then their role should be limited to one they have the capacity to provide, or wider reforms are needed. Elsewhere the EHRC may hold a potential conflict of interest given it is both regulated by, and regularly collaborates with, the ICO.[115]

It seems therefore clear that a one-size-fits-all approach to ICO accountability is unlikely to work, as no one organisation is perfectly placed to provide oversight of the office's diverse activities and strategic decisions. Instead, an ecosystem of complementary institutions (and in places reforms within them) with the skills and remit needed to scrutinise specific aspects of the ICO's work is vital.

110 Source: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4284602

111 Source: https://www.openrightsgroup.org/publications/briefing-the-ico-isnt-working/#sdfootnote34sym

112 Source: https://frccommissioner.org.uk/

113 Source: https://www.gov.uk/government/news/game-changing-tech-to-reach-the-public-faster-as-dedicated-new-unit-launched-to-curb-red-tape

114 https://lordslibrary.parliament.uk/accountability-independence-and-performance-of-uk-regulators-house-of-lords-committee-report/

115 A February 2023 memorandum of understanding between the ICO and EHRC for example recognises that "over the next few years the nature of bilateral, and multilateral cooperation (involving other regulatory agencies), could evolve with the increasing range of digital policy issues where their regulatory remits intersect." Source: https://cy.ico.org.uk/media/about-the-ico/mou/4026606/20230127-mou-ico-ehrc_redacted.pdf

Recommendation 8:

Oversight of the ICO is strengthened through reform of Commissioner appointment procedures, Select Committees, and legal institutions.

Options and actions for implementing this recommendation include:

- **The Science, Innovation and Technology Select Committee establishing a Sub-committee on data protection effectiveness and reforms.** This would provide independent scrutiny of the proposed DUA Bill (following the precedent of the sub-committee on the online safety regime), and the ICO.

- **Transferring to the Science, Innovation and Technology Select Committee the responsibility for budget and the appointment process of the ICO.** Currently, the Information Commissioner remains a Ministerial appointment, and select committee opinions on appointments as part of pre-appointment scrutiny are non-binding. Making the Information Commissioner a Parliamentary appointment would increase arms length from the government, and is likely to foster more active Parliamentary oversight.

- Giving the **Science, Innovation and Technology Select Committee a veto on ICO appointments**, if legislators are less ambitious; this would begin the process of ensuring the ICO's independence from government and giving a Parliamentary committee more political responsibility for ensuring the appointments are successful.

- **Establishing a Data Rights Ombudsman** with powers to adjudicate on data subjects' appeals on how the ICO has responded to their complaints. A new independent body is necessary to deal with the volume of potential appeals, which the Information Tribunal does not currently have the capacity to do. This body could also provide valuable insights (through caseload data) on if and how the ICO is effectively responding to public complaints.

- Proving funding and legal powers for **the Equality and Human Rights Commission (EHRC), to periodically and publicly review the state of data-protection related rights in the UK.** This would ensure comprehensive scrutiny of data protection from the perspective of fundamental rights – a precondition to promote inclusive growth and ensure that the public can reap the benefits of innovation rather than be damaged by its externalities.

6 CONCLUSION

Of the many organisations discussed in this report, most – including the UK government, Parliament, the Information Tribunal, the ICO, and Open Rights Group – are united in their sincere belief that the data rights of the public must be upheld. When considering how this should be done however, opinions diverge.

The ICO's current position can be summed up by Commissioner John Edwards, whose vision for the ICO is to "move away from being "the regulator of no"... We want to say, "how to, not don't do". The analysis within this report puts this worldview under the microscope, making the case that sometimes upholding the public's data rights demands "the regulator of no". Repeat data protection offenders in the public sector, and unfavourable comparisons with other DPA's private sector enforcement records, make it clear that enforcement notices and fines are a vital but unjustifiably under utilised part of the ICO's enforcement toolkit.

With the ICO soon to publish its updated Regulatory Action Policy and the results of its public sector reprimand experiment, it is an opportune moment to reflect on both the challenges that have shaped its enforcement approach and opportunities to address them. As the new UK Parliament settles in and debates around the country's data protection laws rumble on, legislative and democratic reforms are also needed to strengthen external oversight of the ICO and ensure it has the remit and resources needed to enforce the laws entrusted to it. The recommendations within this report span many of these opportunities and reforms.

7 APPENDIX I: DETAILS OF PRIVATE SECTOR ENFORCEMENT IN 2023–2024

ORGANISATION	CASE OUTLINE	DETAILS
COLD CALLING, SPAM AND JUNK MAIL		
Pinnacle Life Limited[116]	£80,00 fine and enforcement notice for 47,998 unsolicited calls	
Penny Appeal[117]	Enforcement notice, for sending 461,650 spam text messages over a ten day period. These messages were sent to a database of individuals who had never agreed to receive marketing communication from Penny Appeal.	
L.A.D.H Limited[118]	£50,000 fine and enforcement notice for 31,329 unsolicited marketing text messages	
Poxell Ltd[119]	£150,000 fine and enforcement notice for 2,647,805 unsolicited direct marketing calls	
Skean Homes Ltd[120]	£100,000 fine and enforcement notice for 614,342 unsolicited direct marketing calls	
Grocery Delivery E-Services UK Ltd t/a HelloFresh[121]	£140,000 fine for 79 million spam emails and 1 million spam texts	
Daniel George Bentley and Taipan Trading Ltd[122]	Sole trader, enforcement notice for 2.5 million unsolicited direct marketing text messages	

116 https://ico.org.uk/action-weve-taken/enforcement/pinnacle-life-limited-en/

117 https://ico.org.uk/action-weve-taken/enforcement/penny-appeal/

118 https://ico.org.uk/action-weve-taken/enforcement/ladh-limited-mpn/

119 https://ico.org.uk/action-weve-taken/enforcement/poxell-ltd-mpn/

120 https://ico.org.uk/action-weve-taken/enforcement/skean-homes-ltd-mpn/

121 https://ico.org.uk/action-weve-taken/enforcement/grocery-delivery-e-services-uk-ltd-ta-hellofresh/

122 https://ico.org.uk/action-weve-taken/enforcement/daniel-george-bentley-and-taipan-trading-ltd/

Digivo Media Limited[123]	£170,000 Fine and enforcement notice for 415,041 unsolicited marketing text messages	
MCP Online Ltd[124]	£170,000 Fine and enforcement notice for 20,939 calls made to CTPS or TPS registered numbers	
Argentum Data Solutions Ltd[125]	£170,000 Fine and enforcement notice for 2,330,423 SMS messages sent without consent.	
RHAP Ltd[126]	£65,000 Fine and enforcement notice for 15,288 marketing calls	
House Hold Appliances 247 Ltd[127]	£55,000 Fine and enforcement notice for 19,069 marketing calls	
F12 Management Ltd[128]	£200,000 Fine and enforcement notice for 1,346,019 marketing calls	
Cover Appliance Ltd[129]	£200,000 Fine and enforcement notice for 511,499 usolicited marketing calls	
SGS Home Protect Ltd[130]	£70,000 Fine and enforcement notice for 24,214 usolicited marketing calls	
Rachel Anderton[131]	Invasion of personal privacy; conviction and fine of £142	
Simply Connecting Ltd[132]	£40,000 Fine and enforcement notice for 441,830 unsolicited direct marketing text messages	
This Is The Big Deal Limited[133]	£30,000 Fine and enforcement notice for 41,417,889 unsolicited direct marketing messages (39,906,342 emails and 1,511,547 text messages)	

123 https://ico.org.uk/action-weve-taken/enforcement/digivo-media-limited-mpn/

124 https://ico.org.uk/action-weve-taken/enforcement/mcp-online-ltd-mpn/

125 https://ico.org.uk/action-weve-taken/enforcement/argentum-data-solutions-ltd-en/

126 https://ico.org.uk/action-weve-taken/enforcement/rhap-ltd-mpn/

127 https://ico.org.uk/action-weve-taken/enforcement/house-hold-appliances-247-ltd-en/

128 https://ico.org.uk/action-weve-taken/enforcement/f12-management-ltd-en/

129 https://ico.org.uk/action-weve-taken/enforcement/cover-appliance-ltd-mpn/

130 https://ico.org.uk/action-weve-taken/enforcement/sgs-home-protect-ltd-en/

131 https://ico.org.uk/action-weve-taken/enforcement/rachel-anderton/

132 https://ico.org.uk/action-weve-taken/enforcement/simply-connecting-ltd-mpn/

133 https://ico.org.uk/action-weve-taken/enforcement/this-is-the-big-deal-limited/

Fortis Insolvency Limited[134]	£30,000 Fine and enforcement notice for 558,354 direct marketing SMS messages without valid consent	
Michael Isaacs[135]	$50k fine and court sentence; Stole data from RBS and used it	
Maxen Power Supply Limited[136]	£120,000 Fine and enforcement notice for unsolicited calls	
Crown Glazing Ltd[137]	£130,000 Fine and enforcement notice for 503,445 unsolicited calls to TPS registered numbers	
Ice Telecommunications Ltd[138]	£80,000 Fine and enforcement notice for 72,682 unsolicited marketing calls to businesses registered with the CTPS or TPS	
UK Direct Business Solutions Limited[139]	£100,000 Fine and enforcement notice for 410,369 unsolicited marketing calls to businesses registered with the CTPS or TPS	
Join the Triboo Limited[140]	£130,000 Fine and enforcement notice for 107 million direct marketing messages	

134 https://ico.org.uk/action-weve-taken/enforcement/fortis-insolvency-limited-mpn/

135 https://ico.org.uk/action-weve-taken/enforcement/michael-isaacs/

136 https://ico.org.uk/action-weve-taken/enforcement/maxen-power-supply-limited-en/

137 https://ico.org.uk/action-weve-taken/enforcement/crown-glazing-ltd-en/

138 https://ico.org.uk/action-weve-taken/enforcement/ice-telecommunications-ltd-en/

139 https://ico.org.uk/action-weve-taken/enforcement/uk-direct-business-solutions-limited/

140 https://ico.org.uk/action-weve-taken/enforcement/join-the-triboo-limited-en/

COMPLEX PROCESSING ISSUES		
Serco Leisure Operating Limited and relevant associated Trusts[141]	Enforcement notices against use of facial recognition and fingerprint scanning for workplace monitoring.	Serco Leisure, Serco Jersey and seven associated community leisure trusts have been issued enforcement notices ordering them to stop using facial recognition technology and fingerprint scanning to monitor employee attendance. The ICO's investigation found that Serco and the trusts have been unlawfully processing the biometric data of more than 2,000 employees at 38 leisure facilities for the purpose of monitoring attendance.
Bank of Ireland[142]	Reprimand for Incorrect credit records impacting people's ability to get loans	
TikTok Information Technologies UK Limited and TikTok Inc (TikTok)[143]	Fine of £12.7m for unlawful profiling and abuse of children's data	

141 https://ico.org.uk/action-weve-taken/enforcement/serco-leisure-operating-limited-and-relevant-associated-trusts/

142 https://ico.org.uk/action-weve-taken/enforcement/bank-of-ireland/

143 https://ico.org.uk/action-weve-taken/enforcement/tiktok/

REPRIMANDS FOR SECURITY BREACHES		
GRS (Roadstone) Limited[144]	Security failures, data exfiltration	
Gap Personnel Holdings Limited[145]	Reprimand for exposure of personal details	The Information Commissioner issued a reprimand to Gap Personnel Holdings Limited in respect of infringements of Article 32 (1), Article 32 (1) (b) and Article 32 (1) (d) of the UK GDPR. The organisation did not have appropriate security measures in place, which resulted in an unauthorised threat actor being able to access individuals personal data twice within a 12-month period.
Optionis Group Limited[146]		A reprimand was issued in respect of specific infringements of the UK GDPR, which include lack of multi-factor authentication, an inadequate account lockout policy, and no clear Bring Your Own Device policy.
Swinburne, Snowball and Jackson[147]	Reprimand after Probate paid to fraudulent actor Security measures not in place	
A recruitment company[148]	Reprimand after 12,000 people's personal data exposed or exfiltrated	
My Media World Limited t/a Brand New Tube[149]	Reprimand after 345000 people's records exfiltrated	
Achieving for Children[150]	Reprimand, after inappropriately disclosed personal data, special category data and criminal conviction data in a report.	

144 https://ico.org.uk/action-weve-taken/enforcement/grs-roadstone-limited/

145 https://ico.org.uk/action-weve-taken/enforcement/gap-personnel-holdings-limited/

146 https://ico.org.uk/action-weve-taken/enforcement/optionis-group-limited/

147 https://ico.org.uk/action-weve-taken/enforcement/swinburne-snowball-and-jackson/

148 https://ico.org.uk/action-weve-taken/enforcement/recruitment-company-reprimand/

149 https://ico.org.uk/action-weve-taken/enforcement/my-media-world-limited-ta-brand-new-tube/

150 https://ico.org.uk/action-weve-taken/enforcement/achieving-for-children/

8 APPENDIX II: DETAILS PUBLIC SECTOR REPRIMANDS 2023–2024

Cases of confirmed actual physical risk to individuals

AUTHORITY	CASE OUTLINE	DETAILS
Thames Valley Police[151]	Witness data disclosed to criminals.	"As a result of this incident, the data subject has moved address and the impact and risk to the data subject remains high"[152]
Nottinghamshire County Council[153]	Placed mother and child at danger. Lack of training and guidance on redaction.	"A social worker sent copies of the assessment report to the mother and her two ex-partners: each the father of one of the two children." "The breach … put the mother and the two children at risk of actual physical harm. The material that was disclosed to the third-party was in relation to previous domestic violence that the third party had enacted on the mother and the two children. This disclosure created a volatile and dangerous situation between the parties."[154]
University Hospital of Derby and Burton NHS Trust (UHDB)[155]	Medical care delayed for up to two years due to poor data management	UHDB failed to have adequate processes in place, especially when processing special category data, which resulted in referrals for out-patients' appointments not being processed in a timely manner. In some cases, this led to delays of up to two years before medical treatment was arranged.

151 https://ico.org.uk/action-weve-taken/enforcement/thames-valley-police/

152 https://ico.org.uk/media/action-weve-taken/reprimands/4025394/tvp-reprimand-20230530.pdf

153 https://ico.org.uk/action-weve-taken/enforcement/nottinghamshire-county-council-reprimand/

154 https://ico.org.uk/media/action-weve-taken/reprimands/4026605/nottinghamshire-county-council.pdf page 2 and 3

155 https://ico.org.uk/action-weve-taken/enforcement/university-hospital-of-derby-and-burton-nhs-trust-uhdb/

Charnwood Borough Council[156]	Disclosure of the new address of the data subject to an ex-partner who was the alleged perpetrator of domestic abuse against the data subject. The process to make address changes was not properly communicated to the data subject, and that there was an absence of a written and well communicated process for dealing with correspondence in these sensitive circumstances for staff to use. In addition, the Council had not ensured that all members of staff involved in this incident had received data protection training in the twelve months prior to the incident.	"the Council sent a letter to her previous address that she shared with her ex-partner, advising of the need to update her address. This letter contained her new address and was subsequently confirmed to have been opened and read by her ex-partner. Due to the previous allegations of domestic abuse, the disclosure of her new address has caused significant distress to the data subject and has the potential to result in harm to the data subject."[157]
University Hospitals Dorset NHS Foundation Trust[158]	An address was disclosed to an ex-partner of the data subject, something they particularly wished to be withheld following previous allegations of abuse.	"The Trust had a procedure in place that when issuing correspondence by letter would include the full postal address of other recipients of that letter without obtaining their consent to do so. This was done by way of cc at the bottom of the letter. Appropriate consideration had not been paid to the risk of this standard practice in relation to data protection and the potential impact that a disclosure could have on a data subject."[159]

156 https://ico.org.uk/action-weve-taken/enforcement/charnwood-borough-council/

157 https://ico.org.uk/media/action-weve-taken/reprimands/4027559/charnwood-bc-reprimand.pdf page 2

158 https://ico.org.uk/action-weve-taken/enforcement/university-hospitals-dorset-nhs-foundation-trust/

159 https://ico.org.uk/media/action-weve-taken/reprimands/4025003/uh-dorset-nhs-reprimand-202304.pdf page 1

Cases of significant impacts on individuals, widespread privacy breaches and catastrophic data loss

AUTHORITY	CASE DETAILS	
Mayor's Office for Policing and Crime (MOPAC)[160]	394 people's inquiries made public via a webform	Data potentially accessed related to police complaints.
Chief Constable West Midlands Police[161]	West Midlands Police failed to ensure the accuracy of the personal data of these two individuals, resulting in multiple incidents where officers attended a wrong address, including on one occasion when there were serious safeguarding concerns relating to one of the individuals.	"WMP officers attended the wrong individual's address when attempting to locate the other individual for which they had serious safeguarding concerns relating to domestic violence; and attending the wrong individual's child's school when attempting to locate the other individual."[162]
South Tees Hospitals NHS Trust[163]	Appointment letter regarding a medical appointment sent to the wrong address, causing anxiety for family members as the recipients were not familiar with the situation	A Trust administrator sent a standard letter to inform the father of a child patient of an appointment made for the child to attend hospital for a medical examination. The appointment letter was sent to the wrong address. The letter was sent to the address of family of the child's mother, Though only basic details were included in the letter, a leaflet with advice was included in the envelope with the letter. This caused significant distress to the father, child and to the family.
Nottinghamshire Police[164]	Witness data exposed	Training on redaction not properly implemented, updates to policies communicated by email. No danger to the individual was noted in this case.[165]
The Patient and Client Council[166]	Gender dysphoria information exposed in cc email	

160 https://ico.org.uk/action-weve-taken/enforcement/mayor-s-office-for-policing-and-crime-mopac/

161 https://ico.org.uk/action-weve-taken/enforcement/chief-constable-west-midlands-police/

162 https://ico.org.uk/media/action-weve-taken/reprimands/4028638/20240226-wmp-final-reprimand.pdf

163 https://ico.org.uk/action-weve-taken/enforcement/south-tees-hospitals-nhs-trust/

164 https://ico.org.uk/action-weve-taken/enforcement/nottinghamshire-police/

165 https://ico.org.uk/media/action-weve-taken/reprimands/4027166/nottinghamshire-police-reprimand.pdf

166 https://ico.org.uk/action-weve-taken/enforcement/the-patient-and-client-council/

Executive Office[167]	Historical Institutional Abuse (HIA) Inquiry exposed 250 emails in a cc list	"Of … 209 email addresses, 110 email addresses contained the individuals' full name"[168]
Ministry of Justice[169]	Disclosure of adoption details against court instruction	
Crown Prosecution Service[170]	Child abuse case files left CPS office on a USB stick, subsequently used to copy movies at home	
Ministry of Justice[171]	Four bags of confidential waste were found in an unsecured holding area in the prison, which both prisoners and staff had access to	"In addition to being in an unsecured location, some of the bags had not been sealed or shredded correctly and contained information relating to both prison staff and prisoners. This included medical data, security vetting details and a Report [blank] During this period we are aware that 44 individuals potentially viewed the information contained in the confidential waste bags. prisoners were identified as having removed information."[172]
NHS Lanarkshire[173]	WhatsApp used to share 500 patients' details	

167 https://ico.org.uk/action-weve-taken/enforcement/executive-office/

168 https://ico.org.uk/media/action-weve-taken/reprimands/4026064/executive-office-reprimand-20230721.pdf

169 https://ico.org.uk/action-weve-taken/enforcement/ministry-of-justice-reprimand/

170 https://ico.org.uk/action-weve-taken/enforcement/crown-prosecution-service-1/

171 https://ico.org.uk/action-weve-taken/enforcement/ministry-of-justice-1/

172 https://ico.org.uk/media/action-weve-taken/reprimands/4025227/20230524-reprimand-moj_redacted.pdf

173 https://ico.org.uk/action-weve-taken/enforcement/nhs-lanarkshire/

Chief Constable West Mercia Police and Chief Constable Warwickshire Police[174]	Catastrophic data loss	"It is noted that at the time of entering the Alliance, Warwickshire Police 'back record converted' its logs from into its new system. This was a total of 160,203 sanitised logs and the information related to 55,195 nominals. Therefore, the sanitised logs from can still be viewed by Warwickshire Police, however was the only system which contained the unsanitised logs and the following information: – source/provenance including names and addresses/location of source. – Submitting Officer including name, rank, role and shift. – Unsanitised text including names, addresses/ locations, allegations of criminal conduct, previous convictions or cautions, details of relationships and associations. – Risk assessments regarding the including information such as previous convictions of the subject of the and/or their associates, details of any further allegations of criminal conduct. The information which has been lost on provided important context and is needed for the assessment of reliability of the and the risks associated with it."
Sussex Police[175] **and Surrey Police**[176]	200,000 recordings of phone conversations, likely with victims, witnesses, and perpetrators of suspected crimes, were automatically saved.[177]	

174 https://ico.org.uk/action-weve-taken/enforcement/chief-constable-west-mercia-police-and-chief-constable-warwickshire-police/

175 https://ico.org.uk/action-weve-taken/enforcement/sussex-police/

176 https://ico.org.uk/action-weve-taken/enforcement/surrey-police/

177 https://ico.org.uk/media/action-weve-taken/reprimands/4024930/sussex-police.pdf

Police Service of Northern Ireland (PSNI)[178]	Disclosure of criminal data to US DoHS	This had an impact on 174 data subjects. This unlawful sharing of personal data including basic personal identifiers (such as name and contact details), information recorded within an Electronic System for Travel Authorisation (ESTA) or VISA applications, information relevant to locating missing persons, criminal conviction data, and biometric data, had been taking place since 2016 and continued following the introduction of DPA 2018 until 15 October 2020. Members of staff within the EU had legitimate but insufficiently regulated access to various PSNI systems and were able to extract personal data which was then unlawfully shared with DHS.[179]

FOI handling

Shropshire Council[180]	At least 2021	"At the time of writing [April 2023] the Council still has a backlog of 143 overdue requests. The oldest unanswered request dates back to April 2021, with remaining requests dating from January 2022 and every subsequent month to the present day."[181]

178 https://ico.org.uk/action-weve-taken/enforcement/police-service-of-northern-ireland-psni/

179 https://ico.org.uk/media/action-weve-taken/reprimands/4027163/reprimand-psni.pdf

180 https://ico.org.uk/action-weve-taken/enforcement/shropshire-council/

181 https://ico.org.uk/media/action-weve-taken/enforcement-notices/4025076/shropshire-en-202305.pdf page 5

9 APPENDIX III: ENFORCEMENT ACTION CALCULATIONS

These were included as private sector enforcement actions:

- Fortis Insolvency Limited (Fine and enforcement notice)[182]
- Poxell Ltd (Fine and enforcement notice)[183]
- Skean Homes Ltd (Fine and enforcement notice)[184]
- F12 Management Ltd (Enforcement notice)[185]

This was not included in total figures

- Shropshire Council (FOI handling, reprimand)[186]

FULL LIST OF ENFORCEMENT NOTICES

This is the list of 83 data protection notices issued by the ICO.[187] Shropshire Council's FoI notice is therefore excluded from this list. The table shows whether the notice was for a public, private or third sector organisation, and whether was a fine, enforcement notice or a reprimand.

ORGANISATION	STATE	PRIVATE	THIRD SECTOR	FINE	ENFORCEMENT NOTICE	REPRI-MAND
Home Office[188]	1				1	
Dover Harbour Board[189]	1					1
Chief Constable of Kent Police[190]	1					1
Mayor's Office for Policing and Crime (MOPAC)[191]	1					1
Pinnacle Life Ltd[192]		1			1	

182 https://ico.org.uk/action-weve-taken/enforcement/fortis-insolvency-limited-mpn/ and https://ico.org.uk/action-weve-taken/enforcement/fortis-insolvency-limited-en/

183 https://ico.org.uk/action-weve-taken/enforcement/poxell-ltd-en/ and https://ico.org.uk/action-weve-taken/enforcement/poxell-ltd-mpn/

184 https://ico.org.uk/action-weve-taken/enforcement/skean-homes-ltd-mpn/ and https://ico.org.uk/action-weve-taken/enforcement/skean-homes-ltd-en/

185 https://ico.org.uk/action-weve-taken/enforcement/fortis-insolvency-limited-en/

186 https://ico.org.uk/action-weve-taken/enforcement/shropshire-council/

187 https://ico.org.uk/action-weve-taken/enforcement/?facet_type=&facet_sector=&facet_date=custom&date_from=01%2F04%2F2023&date_to=31%2F03%2F2024

188 https://ico.org.uk/action-weve-taken/enforcement/home-office/

189 https://ico.org.uk/action-weve-taken/enforcement/dover-harbour-board/

190 https://ico.org.uk/action-weve-taken/enforcement/chief-constable-of-kent-police-1/

191 https://ico.org.uk/action-weve-taken/enforcement/mayor-s-office-for-policing-and-crime-mopac/

192 https://ico.org.uk/action-weve-taken/enforcement/pinnacle-life-limited-en/

Pinnacle Life Ltd[193]		1		1		
Penny Appeal[194]			1		1	
Chief Constable West Midlands Police[195]	1					1
Ministry of Defence[196]	1			1		
Serco Leisure Operating Limited and relevant associated Trusts[197]		1			1	
Chief Constable Devon and Cornwall Police[198]	1					1
Chief Constable Dorset Police[199]	1					1
L.A.D.H Limited[200]		1			1	
L.A.D.H Limited[201]		1		1		
Crown Prosecution Service[202]	1				1	
Poxell Ltd[203]		1			1	
Poxell Ltd[204]		1		1		
Skean Homes Ltd[205]		1		1		
Skean Homes Ltd[206]		1			1	
Grocery Delivery E-Services UK Ltd t/a HelloFresh[207]		1		1		
South Tees Hospitals NHS Trust[208]	1					1
Finham Park Academy Trust[209]			1			1

193 https://ico.org.uk/action-weve-taken/enforcement/pinnacle-life-limited-mpn/

194 https://ico.org.uk/action-weve-taken/enforcement/penny-appeal/

195 https://ico.org.uk/action-weve-taken/enforcement/chief-constable-west-midlands-police/

196 https://ico.org.uk/action-weve-taken/enforcement/ministry-of-defence-1/

197 https://ico.org.uk/action-weve-taken/enforcement/serco-leisure-operating-limited-and-relevant-associated-trusts/

198 https://ico.org.uk/action-weve-taken/enforcement/chief-constable-devon-and-cornwall-police/

199 https://ico.org.uk/action-weve-taken/enforcement/chief-constable-dorset-police/

200 https://ico.org.uk/action-weve-taken/enforcement/ladh-limited-en/

201 https://ico.org.uk/action-weve-taken/enforcement/ladh-limited-mpn/

202 https://ico.org.uk/action-weve-taken/enforcement/crown-prosecution-service-1/

203 https://ico.org.uk/action-weve-taken/enforcement/poxell-ltd-en/

204 https://ico.org.uk/action-weve-taken/enforcement/poxell-ltd-mpn/

205 https://ico.org.uk/action-weve-taken/enforcement/skean-homes-ltd-mpn/

206 https://ico.org.uk/action-weve-taken/enforcement/skean-homes-ltd-en/

207 https://ico.org.uk/action-weve-taken/enforcement/grocery-delivery-e-services-uk-ltd-ta-hellofresh/

208 https://ico.org.uk/action-weve-taken/enforcement/south-tees-hospitals-nhs-trust/

209 https://ico.org.uk/action-weve-taken/enforcement/finham-park-multi-academy-trust/

Daniel George Bentley and Taipan Trading Ltd[210]		1			1	
Bank of Ireland[211]		1				1
Charnwood Borough Council[212]	1					1
NHS Fife[213]	1					1
GRS (Roadstone) Limited[214]		1				1
University Hospital of Derby and Burton NHS Trust (UHDB)[215]	1					1
Police Service of Northern Ireland (PSNI)[216]	1					1
Argentum Data Solutions Ltd[217]		1			1	
Argentum Data Solutions Ltd[218]		1		1		
Gap Personnel Holdings Limited[219]		1				1
Optionis Group Limited[220]		1				1
Chief Constable West Mercia Police and Chief Constable Warwickshire Police[221]	1					1
Digivo Media Limited[222]		1			1	
Digivo Media Limited[223]		1		1		
MCP Online Ltd[224]		1			1	
MCP Online Ltd[225]		1		1		

210 https://ico.org.uk/action-weve-taken/enforcement/daniel-george-bentley-and-taipan-trading-ltd/

211 https://ico.org.uk/action-weve-taken/enforcement/bank-of-ireland/

212 https://ico.org.uk/action-weve-taken/enforcement/charnwood-borough-council/

213 https://ico.org.uk/action-weve-taken/enforcement/nhs-fife/

214 https://ico.org.uk/action-weve-taken/enforcement/grs-roadstone-limited/

215 https://ico.org.uk/action-weve-taken/enforcement/university-hospital-of-derby-and-burton-nhs-trust-uhdb/

216 https://ico.org.uk/action-weve-taken/enforcement/police-service-of-northern-ireland-psni/

217 https://ico.org.uk/action-weve-taken/enforcement/argentum-data-solutions-ltd-en/

218 https://ico.org.uk/action-weve-taken/enforcement/argentum-data-solutions-ltd-mpn/

219 https://ico.org.uk/action-weve-taken/enforcement/gap-personnel-holdings-limited/

220 https://ico.org.uk/action-weve-taken/enforcement/optionis-group-limited/

221 https://ico.org.uk/action-weve-taken/enforcement/chief-constable-west-mercia-police-and-chief-constable-warwickshire-police/

222 https://ico.org.uk/action-weve-taken/enforcement/digivo-media-limited-en/

223 https://ico.org.uk/action-weve-taken/enforcement/digivo-media-limited-mpn/

224 https://ico.org.uk/action-weve-taken/enforcement/mcp-online-ltd-en/

225 https://ico.org.uk/action-weve-taken/enforcement/mcp-online-ltd-mpn/

Nottinghamshire County Council[226]	1					1
RHAP Ltd[227]		1			1	
RHAP Ltd[228]		1		1		
House Hold Appliances 247 Ltd[229]		1			1	
House Hold Appliances 247 Ltd[230]		1		1		
F12 Management Ltd[231]		1			1	
F12 Management Ltd[232]		1		1		
Cover Appliance Ltd[233]		1		1		
Cover Appliance Ltd[234]		1			1	
SGS Home Protect Ltd[235]		1			1	
SGS Home Protect Ltd[236]		1		1		
Ministry of Justice[237]	1					1
Simply Connecting Ltd[238]		1		1		
Simply Connecting Ltd[239]		1			1	
Gloucester City Council[240]	1					1
This Is The Big Deal Limited[241]		1		1		
London Borough of Lewisham[242]	1					1
Swinburne, Snowball and Jackson[243]		1				1

226 https://ico.org.uk/action-weve-taken/enforcement/nottinghamshire-county-council-reprimand/

227 https://ico.org.uk/action-weve-taken/enforcement/rhap-ltd-en/

228 https://ico.org.uk/action-weve-taken/enforcement/rhap-ltd-mpn/

229 https://ico.org.uk/action-weve-taken/enforcement/house-hold-appliances-247-ltd-en/

230 https://ico.org.uk/action-weve-taken/enforcement/house-hold-appliances-247-ltd-mpn/

231 https://ico.org.uk/action-weve-taken/enforcement/f12-management-ltd-en/

232 https://ico.org.uk/action-weve-taken/enforcement/f12-management-ltd-mpn/

233 https://ico.org.uk/action-weve-taken/enforcement/cover-appliance-ltd-mpn/

234 https://ico.org.uk/action-weve-taken/enforcement/cover-appliance-limited-en/

235 https://ico.org.uk/action-weve-taken/enforcement/sgs-home-protect-ltd-en/

236 https://ico.org.uk/action-weve-taken/enforcement/sgs-home-protect-ltd-mpn/

237 https://ico.org.uk/action-weve-taken/enforcement/ministry-of-justice-reprimand/

238 https://ico.org.uk/action-weve-taken/enforcement/simply-connecting-ltd-mpn/

239 https://ico.org.uk/action-weve-taken/enforcement/simply-connecting-ltd-en/

240 https://ico.org.uk/action-weve-taken/enforcement/gloucester-city-council/

241 https://ico.org.uk/action-weve-taken/enforcement/this-is-the-big-deal-limited/

242 https://ico.org.uk/action-weve-taken/enforcement/london-borough-of-lewisham-reprimand/

243 https://ico.org.uk/action-weve-taken/enforcement/swinburne-snowball-and-jackson/

A recruitment company[244]		1				1
NHS Lanarkshire[245]	1					1
My Media World Limited t/a Brand New Tube[246]		1				1
Executive Office[247]	1					1
The Patient and Client Council[248]	1					1
Fortis Insolvency Limited[249]		1		1		
Fortis Insolvency Limited[250]		1			1	
Nottinghamshire Police[251]	1					1
Maxen Power Supply Limited[252]		1			1	
Crown Glazing Ltd[253]		1			1	
Crown Glazing Ltd[254]		1		1		
Maxen Power Supply Limited[255]		1		1		
Thames Valley Police[256]	1					1
Parkside Community Primary School[257]	1					1
Ice Telecommunications Ltd[258]		1			1	
Ice Telecommunications Ltd[259]		1		1		
UK Direct Business Solutions Limited[260]		1		1		

244 https://ico.org.uk/action-weve-taken/enforcement/recruitment-company-reprimand/

245 https://ico.org.uk/action-weve-taken/enforcement/nhs-lanarkshire/

246 https://ico.org.uk/action-weve-taken/enforcement/my-media-world-limited-ta-brand-new-tube/

247 https://ico.org.uk/action-weve-taken/enforcement/executive-office/

248 https://ico.org.uk/action-weve-taken/enforcement/the-patient-and-client-council/

249 https://ico.org.uk/action-weve-taken/enforcement/fortis-insolvency-limited-mpn/

250 https://ico.org.uk/action-weve-taken/enforcement/fortis-insolvency-limited-en/

251 https://ico.org.uk/action-weve-taken/enforcement/nottinghamshire-police/

252 https://ico.org.uk/action-weve-taken/enforcement/maxen-power-supply-limited-en/

253 https://ico.org.uk/action-weve-taken/enforcement/crown-glazing-ltd-en/

254 https://ico.org.uk/action-weve-taken/enforcement/crown-glazing-ltd-mpn/

255 https://ico.org.uk/action-weve-taken/enforcement/maxen-power-supply-limited-en/

256 https://ico.org.uk/action-weve-taken/enforcement/thames-valley-police/

257 https://ico.org.uk/action-weve-taken/enforcement/parkside-community-primary-school/

258 https://ico.org.uk/action-weve-taken/enforcement/ice-telecommunications-ltd-en/

259 https://ico.org.uk/action-weve-taken/enforcement/ice-telecommunications-ltd-mpn/

260 https://ico.org.uk/action-weve-taken/enforcement/uk-direct-business-solutions-limited/

TikTok Information Technologies UK Limited and TikTok Inc (TikTok)[261]		1		1		
Norfolk County Council[262]	1					1
Plymouth City Council[263]	1					1
Ministry of Justice[264]	1					1
University Hospitals Dorset NHS Foundation Trust[265]	1					1
Join the Triboo Limited[266]		1			1	
Join the Triboo Limited[267]		1		1		
Sussex Police[268]	1					1
Surrey Police[269]	1					1
Achieving for Children[270]			1			1
Totals	**31**	**49**	**3**	**23**	**23**	**37**

261 https://ico.org.uk/action-weve-taken/enforcement/tiktok/

262 https://ico.org.uk/action-weve-taken/enforcement/norfolk-county-council/

263 https://ico.org.uk/action-weve-taken/enforcement/plymouth-city-council/

264 https://ico.org.uk/action-weve-taken/enforcement/ministry-of-justice-1/

265 https://ico.org.uk/action-weve-taken/enforcement/university-hospitals-dorset-nhs-foundation-trust/

266 https://ico.org.uk/action-weve-taken/enforcement/join-the-triboo-limited-en/

267 https://ico.org.uk/action-weve-taken/enforcement/join-the-triboo-limited-mpn/

268 https://ico.org.uk/action-weve-taken/enforcement/sussex-police/

269 https://ico.org.uk/action-weve-taken/enforcement/surrey-police/

270 https://ico.org.uk/action-weve-taken/enforcement/achieving-for-children/

openrightsgroup.org