The Information Commissioner's Office response to the Department for Digital, Culture, Media and Sport's consultation on the National Data Strategy

Summary

The Information Commissioner welcomes the development of the National Data Strategy (NDS) which aims to harness the opportunities and address the challenges presented by the rapid development in data driven technologies. The ICO's response to the NDS focusses on our view of the role data protection and the flexible regulatory framework will play in the successful roll-out and delivery of the strategy's ambitions, helping to secure trust from citizens and consumers.

Our response includes details about how the data protection principles can support the missions and pillars of the NDS, alongside a number of practical examples and case studies. In summary it makes the following key points:

- The Commissioner supports the missions and pillars set out in the NDS.
- The Covid-19 crisis has accelerated the growth of digital and data-enabled services, such as online shopping, increased working from home and virtual medical consultations. It has also created a renewed focus on using data to support research and tracking health outcomes. As we rebuild, high data protection standards will be vital in ensuring the benefits of these advances can be maximised for all citizens.
- The recently modernised data protection framework provides many of the tools needed to support the NDS's vision of the UK as a global digital leader, through applying a principle based approach and accountability systems, including the use of sectoral certification and codes for AI and machine learning.
- Data protection is an enabler of innovation and economic growth because it builds public trust that their data will be protected; provides organisations with the confidence to share data to improve the quality and efficiency of public services; and supports the take-up and use of new data-enabled services.
- Transparency is a crucial part of building this trust. In the public sector the Freedom of Information Act (FOIA), open data and the proactive

publication of data sets will help deliver this transparency and underpin public confidence in data-enabled public services.

- Accountability, including privacy by design and default is also key, helping ensure responsible data use is at the heart of the approach of both businesses and government. We propose that the NDS would benefit from a greater focus on accountability as both an enabler and protector.
- The uses of data in both public and private sectors are complex and varied, and pose different risks. A risk-based approach will be important to ensure the actions taken are flexible and proportionate. A risk-based and principle driven approach will enable SMEs, start-ups and innovators to build in key protections from the outset and unlock important benefits from data use.
- It is crucial to promote a data sharing culture that both enables and protects, and dispels misconceptions by providing education, guidance and advice. The ICO's forthcoming Data Sharing Code will also play an important role in this.
- Trust and accountability will also be key to ensure data continues to flow internationally post-transition.

About the ICO

1. The Information Commissioner has responsibility in the UK for promoting and enforcing the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA 2018), the Freedom of Information Act 2000 (FOIA), the Re-Use of Public Sector Information Regulations 2015 (RPSI), the Environmental Information Regulations 2004 (EIR) and the Privacy and Electronic Communications Regulations 2003 (PECR), amongst others.

2. The Commissioner is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations and taking appropriate action where the law is broken.

Introduction

3. The Commissioner recognises the importance of the proposed National Data Strategy (NDS), the drivers that sit behind it and the outcomes it is seeking to achieve. The Commissioner supports the missions and pillars set out in the strategy. This response seeks to highlight how data protection can enable innovation, and how high standards and accountability can play a crucial role in its delivery.

4. Data protection plays a central role in promoting economic growth by encouraging public trust in innovation and supporting the UK as it steps forward in the global economy. The current pandemic has brought this into sharp focus. Principles of data protection, such as transparency, fairness and proportionality, build public trust and confidence in the way personal data is used and, in turn, enable businesses to innovate and grow. Successful data processing initiatives in the public sector are also dependent on trust. Effective and responsible data sharing across the public sector can improve the quality of public services, save money, and improve decision-making. Initiatives which use data responsibly will not only contribute to a pro-growth agenda but will also secure individual rights in practice and protect society from harm.

5. As personal information increasingly becomes central to all facets of our lives from finance, through health, to education and communication, the need to protect individuals also becomes increasingly important. The ICO enables organisations and individuals to navigate how to achieve this responsibly through clear guidance, support and acting as a regulatory backstop, while encouraging the growth of technology and innovation.

6. Our guidance and support underlines the vital importance of baking data protection into new products and technologies, especially when developed at pace, following a privacy by design and default approach[1]. The ICO would welcome a more explicit recognition of this approach in the NDS.

7. The role of FOIA, open government and proactive publication of datasets in the public sector are also key enablers in the development of a positive culture. This helps underpin trust and confidence in public authorities and demonstrates that the decisions and actions they take are worthy of the trust that citizens place in them. This in turn will facilitate public accountability. The ICO proposes that the NDS can do more to highlight the role of FOIA and the RSPI as an enabler of open data.

8. Government's response to the coronavirus pandemic has underlined the vital importance of data in the provision of public services. Adapting rapidly in an emergency need not mean lower standards of data protection and, in fact, having those standards means that organisations are well-placed to respond to shifting demands with confidence. It is important to learn lessons from data innovation during the pandemic.

9. The ICO has been involved in advising the Government on the correct use of data in several pandemic responses and, along with them, has gained valuable insight.

---

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-act/

10. At the end of the transition period, the United Kingdom will be presented with a series of opportunities and challenges for the use and sharing of data internationally. There are a series of mechanisms outlined in this response to ensure that the UK is well-positioned to enable the continued flow of personal and other data internationally, based on trust and accountability.

Unlocking the value of data

11. The value of data is increasing all the time and is becoming ever more central to the operation of businesses both large and small. There is a challenge and an opportunity to support businesses, not only in identifying the type and sources of data they need, but also in maximising the efficient use of data once it's in their possession.

12. The ICO welcomes the importance placed on high data protection standards in the NDS. Data protection law must work in practical terms for both organisations and the public. After the transition period, the UK will have an independent data protection policy and the ICO will continue to provide expert regulatory advice to Government on how the data protection framework works in practice, and its role in protecting individuals' information rights and enabling data use.

13. The importance of clear and practical guidance is recognised by the ICO and work will continue in order to provide this support to organisations, particularly in the context of new technologies and uses of data and through the Sandbox programme.

14. The ICO broadly supports the aim of the first mission in unlocking the value of data across the economy, including the vital importance of ensuring good data quality. The ICO also notes the need for public trust in data collection for successful public sector data processing. Technological advances mean that there is an increasing ability to gain insights from smaller data sets. Additional protection for individuals provided by using aggregated data or anonymised information, or privacy enhancing technologies, can also reduce the risk of potential harm. Although sufficient data will be required to avoid the possibilities of bias or discrimination and to ensure individual and wider societal benefit.

15. The ICO's guidance and advice provides a clear framework to assist organisations in complying with data protection principles, including those relating to purpose, accuracy and data minimisation[2]. In particular, recent innovation in data analysis and other techniques emphasise the importance of the quality of the data, rather than just the quantity. Other technological

[2] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

advances, with appropriate safeguards, may mean that more can be done with less, as well as providing for individuals by using aggregated data or anonymised information, or privacy enhancing technologies, reducing the risk of potential harm.

16. The NDS could explain the importance of organisations having a clear approach to implementing the data protection principles and the wider benefits in doing so – highlighting the role they play in trust and confidence, and the wider connections to issues such as cyber risk and processing costs. To ensure that data protection is built into the approach taken by data intensive businesses and public services it is vital that this is undertaken sustainably over time and that there is Board level leadership to embed the data governance needed.

17. The NDS can do more to highlight the importance of transparency and how it can be realised in practice. As the amount of data in circulation increases, individuals need to be given simpler and more effective ways to understand how their personal data is being used and can have the opportunity to make real choices. Organisations will need to develop innovative solutions, drawing on usability and interactive design to ensure people can understand how their data will be used and they can exercise meaningful control. The NDS could illustrate more clearly how data protection can operate in practice and how to engage the public.

18. This will also require a clearer understanding of the relationship between data ethics and data protection, as compliance with the law will always need to be at the core of any approach to data, but data ethics can play an important role in assessing issues within data protection law such as fairness, harm and risk.

Accountability

19. Accountability under data protection law can be a key pillar in enabling and unlocking the benefits of data use highlighted in the NDS, whilst maintaining high standards, safeguards and trust and confidence. The ICO's guidance explains the importance:

> "Why is accountability important?
>
> Taking responsibility for what you do with personal data, and demonstrating the steps you have taken to protect people's rights not only results in better legal compliance, it also offers you a competitive edge. Accountability is a real opportunity for you to show, and prove, how you respect people's privacy. This can help you to develop and sustain people's trust."

20. Accountability is now a legal requirement in the data protection principles, including privacy by design and default. It is positive to see this reflected in the core pillars of the strategy which will enable organisations to use data

responsibly. The ICO's Accountability framework[3] is a practical tool to support organisations in assessing and demonstrating their data protection compliance and complements this fundamental pillar of the strategy.

21. The ICO's work on codes of conduct and certification schemes also promotes a culture of accountability and innovation, which is likely to contribute to mission 2 in securing a pro-growth and trusted data regime. Codes of conduct approved by the ICO enable a sector to own and resolve key data protection challenges and also certification. Certification is a way for organisations to demonstrate compliance with data protection law. Certification scheme criteria are approved by the ICO.

22. The projects progressed through the ICO's regulatory Sandbox also show that data protection is not a barrier to innovation and how data protection by design solutions can be implemented in practical situations. More detail about the Sandbox is provided below.

Common standards

23. The ICO welcomes a regime based on standards, which can support and enable consistent approaches to data protection compliance. It will be important that any new standards are interoperable with existing data protection standards and guidance.

24. The development of any common approach is likely to require incentives, clear, effective communication and encouragement. This could be in the form of guidance and training to tackle lack of understanding and confidence where this is found, and to reinforce the importance of responsible data usage and transparency. Positive examples and proactive sharing of good practice in the form of case studies or use cases are likely to be most helpful in helping others in meeting specific challenges. These might be in relation to privacy or security issues, which the consultation document has highlighted as potentially creating "barriers to data availability". The ICO is developing case studies illustrating good accountability practice to support its Accountability framework.

Leadership and skills

25. Strong leadership in all sectors will help in developing an organisational culture that fosters responsible data sharing, good practice and regulatory compliance. This will require staff training in appropriate skills, including on data protection and other relevant legislation, as well as effective and clear communication. Although some key decisions should be taken at board level or the equivalent, the cultural approach to the responsibilities of better data sharing need to be understood throughout the organisation, and especially by those with face-to-

[3] https://ico.org.uk/for-organisations/accountability-framework/

face contact with the public. The ICO therefore supports measures which promote this aim in the NDS.

Data sharing

26. Particularly relevant to the aims of the fourth pillar of the NDS (data availability) is the support the ICO provides to organisations in promoting good practice on data sharing. The GDPR and DPA 2018 enable fair and proportionate data sharing, but there are some misconceptions that data protection law prevents data sharing. This can mean that opportunities to share data in appropriate cases might be missed. The ICO seeks to promote a data sharing culture that both enables and protects, and to dispel these misconceptions by providing education, guidance and advice[4]. The ICO highlights the importance of communicating key messages about data sharing consistently and the importance of a coalition between regulators, public bodies and sector groups to join up in this work.

27. The ICO's revised and updated Data sharing code will clearly explain how organisations should approach the sharing of personal data. In drafting the code, the ICO consulted widely across sectors and had consistent engagement with stakeholders to ensure the code meets the needs of practitioners. The ICO will continue to engage with organisations about how to share data in line with data protection law, providing practical tools and resources and hosting stakeholder events; and work to show that data protection is an enabler to data sharing.

Data for public benefit during the coronavirus crisis

28. Data, including personal data, has been a vital tool for all sectors in responding to the current pandemic. The ICO has made it clear from the outset that data protection laws do not get in the way of effective, efficient or innovative use of data in a public health emergency, such as the Covid 19 pandemic, if the principles of transparency, fairness and proportionality are applied.

29. The ICO recognised the unprecedented challenges being faced by organisations in all sectors during the pandemic and we adjusted our regulatory approach accordingly. This was done by taking a flexible approach which recognised the pressures all organisations were under, provided effective support to businesses and public authorities, focussed our efforts on the most serious risks and greatest threats to the public, while promoting the important role that

[4] The new ICO Data Sharing Hub will go live before the end of the year.

individuals' information rights continue to have. We continue to review and revise our approach in accordance with the changing situation.[5]

30. The ICO has offered guidance and broader practical support, for example, in its advice on the Covid 19 contact tracing apps developed across the UK and in the shielding programme mentioned below. It has also stood ready to take action against those that used a public health emergency opportunistically, for example, to set up scams or contact vulnerable people using nuisance calls, unsolicited emails and spam texts.

31. In the course of the Government's development of a Covid contact tracing app, the ICO produced an 'expectations document'[6] to enable developers to better understand the data protection requirements. This has provided clarity to technical practitioners during a national crisis and will be a baseline for the ICO in case of future audits. Work in this area is continuing.

32. The example of the data sharing programme related to shielding in Annex A illustrates the importance of capturing good practice and sharing lessons learned from data sharing, and using these case studies to create more confidence in data sharing amongst practitioners and with the public.

33. The ICO welcomes the development of strong networks to better disseminate best practice in data protection and data governance. For example, in the sphere of AI, the ICO leads or participates in a number of formal and informal networks including the Regulators' AI Working Group, the AI and Data Science Regulatory Capacity Working Group, and the Digital Regulation Cooperation Forum (DRCF).

34. Insights from data are likely to be valuable for Government and other policy makers when considering the evidence base for future initiatives and in research. Some organisations have already been working towards compiling pseudonymised datasets from the financial sector to provide insights into the impact of Covid-19 on the economy.

35. This use case highlights the value and insight that can be derived from the data. As this type of data use continues to develop it will be important that the safeguards used continue to be assessed against data protection risks and how they may need to evolve. The ICO has produced guidance on anonymisation and pseudonymisation which is recognised internationally and has been the basis of standards in other jurisdictions[7]. The ICO will seek to provide further advice and guidance on use of these techniques.

---

[5] https://ico.org.uk/media/about-the-ico/policies-and-procedures/2617613/ico-regulatory-approach-during-coronavirus.pdf

[6] https://ico.org.uk/media/for-organisations/documents/2617676/ico-contact-tracing-recommendations.pdf

[7] https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

Fairness and the individual

36. Data has the potential to create better outcomes for individuals, including the vulnerable, when their personal data is used responsibly and fairly in evidence-based interventions. This is a vital component in preventing harm and securing and retaining the public's trust and confidence. It ensures that citizens and groups have control over how their personal data is used and how decisions that affect them are made. It also means that the notion of responsible use of data is factored into the infrastructure, thereby adhering to the legal requirement for privacy by design and default. This means that, in the drive for growth, new and existing inequalities or harms that could be connected to data use do not go unaddressed. The ICO's revised priorities during the pandemic reflect the risks to individuals that could arise, for example, the risks involved in needing to share more data and to share it more quickly. We advised Government and supermarkets as to how they could quickly, safely and fairly share data around vulnerable people as part of the shielding programme in response to the pandemic.

37. The ICO already provides a broad range of guidance and other resources, including 'Your data matters'[8], which is particularly relevant to individuals. It empowers them to take ownership of their own personal data and to know their data protection rights. However, the ICO supports the inclusion in the NDS of a broader skills programme of education about how personal data is used in different contexts and its impact on society, as well as on specific individuals and groups. The ICO has also produced resources on matters of particular concern to students and schools[9].

38. A broader skills programme should include educational resources for business leaders, not just those who presently work with personal data. The programme could also include how data risks should be considered at Board level. These skills are particularly important in a digital context when individuals may find it more difficult to understand how personal data is being used, for example in technologies such as AI. Educational initiatives of this nature are also likely to help in addressing issues of citizen awareness and potential disengagement.

39. It is also important to recognise that some uses of personal data can also create potential for harm, discrimination or any other adverse impact, including, but not limited to those with protected characteristics as defined under the Equality Act. The use of data protection impact assessments (DPIAs) under GDPR can enable the risk of these harms to be considered, alongside wider risks, for example related to different socio-economic groups.

---

[8] https://ico.org.uk/your-data-matters/

[9] https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/exam-script-exemption-students/

40. Children are given specific protection under the GDPR. The NDS should take account of the ICO's Age appropriate design code (AADC), recently approved by Parliament[10]. It sets out 15 standards which organisations need to conform to, if they provide information society services likely to be accessed by children.

41. The NDS can reflect the reality that citizens may have a flexible approach to the use of their data – their approach to data may differ according to the nature of the organisation, the services or products involved, or the use to which it is put. This underlines the benefits of a principles-based regime which offers a common approach but with flexibility to allow for context-specific judgements.

42. For the public at large, as the commercial value of personal data grows, innovative products and services are already appearing where giving up significant amounts of personal data subsidises the price consumers pay. For example, many so-called 'free' apps offer individuals an option to pay a premium to avoid advertisements.

43. In due course, this may mean that there is the risk that individuals will be unable to afford to control their data – a kind of privacy poverty. The ICO recognises the importance of the NDS linking to other initiatives such as the work of the Digital Markets Taskforce, to find ways to manage transparency and fairness in the face of the monetisation of individuals' personal data. In particular, in situations where individuals may feel they have no practical choice but to agree for it to be collected. This will unlock more trust and confidence in how organisations can share and use data.

44. For example, caution is needed to avoid situations where individuals are put at risk or feel forced to share their personal data when accessing a service, for example using an intermediary because of a disability. This underlines the importance of fairness when using personal data, and organisations might need to take particular care when relying on consent, to ensure that it is freely given.

45. The NDS however still needs to emphasise the importance of transparency, even in circumstances where an organisation is working for the benefit of the individual. Benefit to the individual must not override the need for transparency, as demonstrated in action taken by the ICO against the Royal Free Hospital when it provided patient details to Google DeepMind without giving patients enough information.[11]

---

[10] https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/

[11] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/

46. Given the importance of transparency in this context, the ICO would also highlight the need for engagement with representative groups and civil society in certain projects involving data.

Digital Economy Act 2017

47. Powers contained in the Digital Economy Act 2017 (DEA) already provide legal gateways for data sharing. Some of these powers remain unused, although there are examples of data sharing such as those assisting people in energy poverty under the Warm Homes Discount, and the DEA review board for the debt and fraud powers has considered a range of data sharing pilots. Research undertaken on behalf of the DEA board for the public service delivery powers[12] suggests that there are misconceptions and a lack of understanding about the powers and the benefits that they can offer. In particular, further consideration may be required into how this legislation could support health data sharing in the future. The ICO welcomes further efforts to utilise these powers to allow for responsible, compliant data sharing and stands ready to assist in work to explore this.

48. The ICO also supports the continued proportionate use of the DEA's data sharing powers in both statistics and research for the Office of National Statistics and the UK Statistics Authority through its Research Accreditation Panel.

Business, including small and medium-sized enterprises (SMEs)

49. The existing data protection regime is universal, applying to organisations irrespective of their size. However, the ICO acknowledges that there can be challenges to compliance in some smaller organisations due to their lack of awareness of data protection matters and the absence of the necessary skills. The UK's principles based data protection framework can enable SMEs to take a risk based approach, which can scale and allow flexibility. The ICO recognises the importance of supporting SMEs to achieve practical steps to compliance, that recognises the context of their business models and resources, particularly start-ups.

50. The ICO's accountability framework[13] supports all organisations in complying with the accountability principle, including SMEs. There are also additional ICO resources targeted at smaller businesses to help organisations meet these

---

[12] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/895505/_Kantar_research_publication.pdf

[13] https://ico.org.uk/for-organisations/accountability-framework/

challenges. The ICO has created a hub on its website[14] which provides advice and support that is particularly relevant for small businesses, sole traders and community groups. In addition, staff on the ICO helpline can direct enquirers to helpful resources. A suite of resources to support organisations of all sizes, including specialist guidance for SMEs, will also accompany the ICO's forthcoming Data sharing code. It is important to note that the current data protection regime allows the regulator to take a risk-based approach and the ICO are building a range of tools to better assist SMEs, including considering how to tailor the accountability framework to specific SME needs.

51. The ICO continues to encourage business to place sufficient investment in skills around data protection and data governance. In particular, for project managers and leaders, ensuring that their own assessment of risk takes place at board level or its equivalent, as part of an accountability approach. The ICO would welcome inclusion of this approach in the NDS.

52. It is important that the NDS recognises the steps that regulators can take to enable safe and fair innovation. The ICO also supports innovation through its Sandbox (Annex B), allowing organisations to develop their projects safely and compliantly with advice from the ICO, using a privacy by design and default approach. Recent projects have included data sharing for the monitoring of the flow of funds in the financial system with the potential to combat financial crime[15] and mitigating bias in customer identity verification.[16] Use of the Sandbox helps organisations ensure a 'right first time' approach.

53. There is a risk in organisations (and SMEs in particular) having the ability to effectively risk-assess novel uses of personal data, which require a DPIA, from the data subject's perspective. In particular, if these organisations do not understand technological products for processing that they buy and use. This affects fairness, transparency and trust and potentially impacts on individuals because it is hard for organisations to explain to others how their system works, if they do not understand it themselves. The NDS could do more to recognise the importance of supporting SMEs in this area.

54. While there is discussion about the challenges that can be posed by the application of data protection to AI it is important to recognise the steps that are being taken to address this challenge. And that data protection can enable safe and fair AI innovation.

55. The ICO has focussed considerable effort on its products for the development and use of AI. This is to ensure that the ICO continues to support industry and its own audit teams in providing clarity around the audit and assessment of algorithms and AI. The ICO has proactively engaged with data scientists and

---

[14] https://ico.org.uk/for-organisations/data-protection-advice-for-small-organisations/
[15] https://ico.org.uk/media/for-organisations/documents/2618552/futureflow-sandbox-report.pdf
[16] https://ico.org.uk/media/for-organisations/documents/2618551/onfido-sandbox-report.pdf

collaborated with industry and other regulators. This has included proactive engagement with those leading on the development of responsible AI, particularly the Alan Turing Institute, to ensure that future developments are built on a privacy by design and default basis. The ICO considers that this approach, especially in the development of AI, is one that should be adopted in the NDS. The ICO is willing and able to collaborate with Government and other partners about this.

56. Working with the Alan Turing Institute, the ICO has produced guidance entitled, 'Explaining decisions made by AI'[17], and the ICO has published 'Guidance on AI and data protection'.[18] Both are likely to assist all organisations, from start-ups and SMEs, to major technological platforms and wider supply chains that develop or use AI. The ICO continues to support innovation in how to design and build AI systems to ensure that a data-driven economy is achieved in a responsible manner.

57. In its efforts to support organisations of all sizes, the ICO continues to publish and promote other guidance to create greater clarity about important issues of data protection. This has included the Commissioner's Opinions on Live Facial Recognition[19] and on the Apple/Google Covid-19 Exposure Notification API.[20] A formal Opinion on commercial use of FRT will be published in due course.

58. Better insights, leading to more efficiency, could be gained by higher quality data that is shared and made available to others appropriately. Technologies that facilitate greater control and protect individuals have the potential to create new opportunities without detriment. The ICO is continuing its work focused on data sharing that uses privacy-enhancing methods, including guidance on anonymisation and pseudonymisation. Using these methods and other data minimisation techniques will reduce privacy intrusion for individuals during processing, while allowing organisations to process personal data required to achieve business outcomes.

59. The ICO also recommends the use of DPIAs to demonstrate the necessity and proportionality of the processing of personal data, the impact on individuals, and the risks of bias and trade-offs, including broader risks in AI. These assessments can be used by businesses to develop a stronger risk management culture.

---

[17] https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/explaining-decisions-made-with-ai/
[18] https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-artificial-intelligence-and-data-protection/
[19] https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf
[20] https://ico.org.uk/media/about-the-ico/documents/2617653/apple-google-api-opinion-final-april-2020.pdf

60. The ICO continues to work with both Government and other regulators to provide additional support and advice to all organisations, including SMEs.

61. The NDS could provide additional support for SMEs, allowing them to develop additional skills in order to participate more fully in the digital economy. These might include resources around the ability to collect good quality data; interpret data and gain valuable insights; and manage their data responsibly. Low cost tools that support SMEs to automate data analytics and reduce time could help, as could an awareness campaign to promote the benefits of increased use of personal and non-personal data use.

62. Development of tools to help SMEs (and other organisations) procure and build compliant and ethical AI systems would also be of assistance. For example, these might include checklists for procurement, so that SMEs might be able to critically and constructively assess products and not find themselves having to accept whatever is being offered. A standard set of criteria might help with this, like the AI procurement guidelines[21] produced for the public sector.

63. The NDS could also include the possibility of certification and kite marking of AI systems that are on the market. Certifications under GDPR might also be appropriate for deployment of these systems. The ICO has developed a range of tools that can help organisations realise their desired outcomes. The current legislative regime is still relatively new and there is significant scope for creating and developing these tools further within this framework, such as in data sharing, AI, or innovation.

Infrastructure

64. The NDS should include specific reference to the need to consider data protection by design and default when selecting services and products to use in data processing activities. In other words, when third parties supply products or services to process personal data, the data service provider should choose suppliers that design their products or services with data protection in mind.

65. The use of a small number of infrastructure service providers by an increasing number of organisations potentially increases risk. This risk increases, not only in relation to cyberattack, breaches, and targeting by malicious actors, but also because of the potential scale of the damage if something goes wrong. It is therefore incumbent on organisations that provide these services and those who use them to create environments where there are appropriate levels of assurance and accountability. For example, one of the expectations set out in the ICO's accountability framework is that organisations processing personal data carry out due diligence checks to guarantee that processors will implement

[21] https://www.gov.uk/government/publications/guidelines-for-ai-procurement/guidelines-for-ai-procurement

appropriate technical and organisational measures to meet GDPR requirements. Expectations will increase in proportion to the risks.

66. The NDS might also need to consider whether there should be a shift in the relationship between dominant service providers and smaller organisations - both from the point of view of their respective responsibilities, and because of the potential for such dominance to stifle real choice and control. In this respect, government has a role in setting standards, which might be through a combination of voluntary compliance and regulation. Specific legislation in this area might also be considered given the increasing dependence of society on personal and non-personal data.

67. The NDS will need to consider the needs and requirements of the procurement process. This should build in due diligence checks proportionate to the risk of the processing before a contract is agreed with a processor. This should include data security checks and other assurance measures such as site visits, system testing and audit requests.

68. Additionally, the NDS might consider support to enable standardisation of common contract clauses. This would allow organisations to conduct audits or checks to confirm that the processor is complying with all contractual terms and conditions. Routine compliance checks should be carried out, proportionate to the risks, to test that processors are complying with contractual agreements. This would include ensuring compliance with agreed retention periods.

International flow of data

69. The ICO is pleased to note the Government's recognition in mission 5 of the vital role that trust plays in allowing the flows of data between countries that underpin international trade. Robust, effective data protection law, based on common global principles, is a key aspect of building this trust and therefore enabling these international data flows.

70. The data protection rules in force in the UK today are built on these principles. They were developed not only to protect privacy and other individual rights, but to allow the free flow of data between countries offering an equivalent level of protection. The NDS should therefore ensure that the future development of the UK's data protection policy upholds and builds on the core rights, principles and protections for personal data that have been enjoyed by UK citizens for more than 35 years, and that these protections continue to apply to UK citizens' data when it is transferred to other countries. The need for the UK's data protection standards to keep pace with new technology and innovative data use is also recognised.

71. The Government's commitment to work with the ICO to develop cooperation with other national data protection authorities is also welcome. However, the

ICO would emphasise the need for those standards to be recognised globally in order for them to be meaningful in the context of international data flows.

72. To this end, the ICO sees significant benefit in the UK ratifying the modernised version of Convention 108 (a Council of Europe treaty open to accession by non-CoE States), also known as Convention 108+. As it is the only global data protection treaty for data protection, with a potential to grow globally, ratification would reaffirm the UK's commitment to common global data protection standards. This would support mission 5 of the NDS, as well as supporting pillar 4 (responsible use of data).

73. Similarly, the ICO recommends continued adherence to the Privacy Guidelines of the Organisation for Economic Cooperation and Development (OECD) which lay out the principles on which most modern data protection laws are based. They remain an important point of reference in policy discussions and have had a substantial impact, including as the basis for many national laws. Nearly every OECD country now has one or more laws protecting privacy, and even countries outside the OECD often look to these guidelines when developing their own national data protection laws. The Privacy Guidelines are currently being reviewed to ensure they remain relevant and fit for purpose in today's increasingly globalised and digital world. This review is being overseen by the OECD Working Party on Data Governance and Privacy (DGP), which is chaired by ICO's Deputy Commissioner for Regulatory Strategy, Steve Wood.

74. The Information Commissioner, Elizabeth Denham, also chairs the Global Privacy Assembly (GPA), the global forum for data protection and privacy authorities. The Assembly seeks to provide leadership at international level in data protection and privacy. It does this by connecting the efforts of more than 130 data protection and privacy authorities from across the globe. As Chair of the GPA, the Commissioner is leading work on building interoperability between different data protection regimes.

75. In these positions of influence, the ICO looks forward to continuing this work to help ensure that the UK remains at the forefront of modern data protection regulation and that UK citizens can continue to enjoy the benefits of the global digital economy whilst retaining the level of protection that they currently enjoy.

Personal data transfer tools and accountability mechanisms

76. The Government must ensure any new UK adequacy regulations, international agreements or other tools for transferring personal data abroad give businesses and other organisations the trust and confidence to participate in the global digital economy. This confidence has been dented in recent years following the successful legal challenges to the Safe Harbor and Privacy Shield adequacy decisions which provided a mechanism for personal data to be transferred from the EU to the USA. This highlights the need for the Government to create

robust transfer tools, with safeguards for individuals which stand up to scrutiny, whilst also recognising the need for practical, scalable and risk-based mechanisms that can work for organisations' uses of data in the modern digital economy.

77. The use of the accountability mechanisms provided by the adequate safeguards of 'binding corporate rules' and 'codes of conduct' could be encouraged as part of the NDS to facilitate international transfers between corporate groups or those engaged in joint economic activities and sectors. There may be similar accountability mechanisms that it would be possible to develop for transfers beyond corporate or sectoral groups, for example, covering common transfers or transfers for a particular purpose. A key point will be maintaining high data protection standards in terms of transfers whilst ensuring that mechanisms are understood and not overly complex for the full range of UK controllers and different risks posed by transfers.

Transparency

78. The ICO recognises that opportunities are not limited to the processing of personal data, and the NDS can encourage the more extensive use of other forms of data. In this respect, FOIA, the EIR and RPSI have the potential to open up more public sector data to the public, including businesses and civil society.

79. The ICO would highlight the role that FOIA can play in opening up public data. Public authorities, as defined under FOIA, are required to make information available to the public as part of their publication scheme obligations[22] and this should be part of normal business activity. Public authorities should regard the publication of information as by default and not exception, thereby contributing to transparency and underpinning the accountability of public bodies towards citizens. There is an added efficiency in that where information is proactively published, individuals have no need to make freedom of information requests for it. It should also be mentioned that the EIR require public authorities who are subject to the regulations to proactively publish environmental information.

80. There are many examples of where FOIA has driven open data – the regular publication of MOT test data and restaurant hygiene ratings have come about following FOI requests and ICO decisions.

81. RPSI regulations allow individuals or organisations to re-use information from the public sector, commonly with the aim of producing a new product or resource on a commercial basis. The ICO receives few complaints in this area, which may indicate that information is already properly made available by public sector bodies. However, there may be benefits in reviewing the extent to

[22] https://ico.org.uk/for-organisations/guide-to-freedom-of-information/publication-scheme/

which this could be further actively encouraged and promoted to ensure that individuals and the private sector are fully aware of the regulations and the potential benefits can be maximised. Government may also want to consider opening out information to the wider public which is currently only supplied to commercial entities.

82. The public sector should publish DPIAs for large change programmes and new policies focused on delivering the NDS.

83. The NDS should also encourage and support more extensive proactive publication of information related to the delivery of public services, building upon existing freedom of information requirements. This will further citizens understanding of decisions that affect their daily lives, enabling them to call organisations to account for their decision-making in matters such as procurement and the use of public funds. These factors are essential to encourage citizen participation, and ensure accountability, trust and improved services. The ICO's report, 'Outsourcing Oversight?'[23] has made several recommendations in this area.

Conclusion

84. The ICO welcomes the opportunity to continue to provide independent advice and evidence to Government from its experience as regulator. Areas for cooperation include, but are not limited to, data sharing, use of artificial intelligence, protecting children online, embedding the accountability framework, and support for SMEs.

85. Data, and particularly personal data, is already the driver of growth in the economy and the delivery of public services. A strong national strategy to maximise the benefits of data use is essential. The ICO is pro-innovation, supports growth and sees data protection as an enabler of both. A strategy underpinned by the principles of fairness, transparency and security will create public trust and lay the foundations for the success of the NDS.

86. The ICO looks forward to providing regulatory advice and guidance in support of the NDS.

[23] https://ico.org.uk/media/about-the-ico/documents/2614204/outsourcing-oversight-ico-report-to-parliament.pdf

Annex A : The Shielding Programme

1. The sharing of the shielded patient data is an example where personal data was shown to be shared effectively and at speed, while still protecting personal data during the pandemic. By identifying appropriate lawful bases for the processing, the organisations underlined the enabling features of data protection.

2. The shielding programme involved the rapid coordination of four Whitehall government departments, the NHS, a network of local authority hubs, and supermarkets providing grocery delivery services to the extremely clinically vulnerable who were shielding. There was a willingness on the part of all involved to collaborate. While the ICO has not undertaken a detailed analysis of all parties' data processing practices, from what we understand today, there are positive lessons to be highlighted.

3. A significant advantage was the maturity of the data protection compliance functions in each of the organisations. All had clear processes and procedures in place which allowed the organisations to respond rapidly to the need to share data for the public good, while protecting individuals' privacy and complying with the key obligations of data protection law. For example, safeguards were part of the conversation from the outset.

4. Also important in its success was the consideration given to the transparency information made available to individuals and the sequencing of such information. The messaging was provided by different stakeholders in the correct order, meaning the original message gave the context in which the data was being shared.

5. The shielding programme made efforts to put the individual in control of what happened to their data – there was an opt-in element to the service before certain aspects of the sharing took place (for example, sharing with food suppliers). This helped meet the requirement for proportionality, as well as building trust and confidence in the project.

6. The guidance produced by the Ministry for Housing, Communities and Local Government (MHCLG) which was provided to local authorities represented a good practice approach which could be replicated elsewhere. In particular, by helping to define the purposes for which the data could be used and shared, showing that personal data standards can be maintained in an emergency.

7. The ICO was able to provide guidance about the gateways for sharing. For example, allowing supermarkets to process personal data for the reasons defined within the shielding programme, therefore supporting sharing with organisations in the private sector where there was a clear public interest. While organisations in health and social care may be more familiar with their ability to share in a public health emergency, in this case, all parties were confident that there was a lawful basis for this public-private sharing.

Government shared personal data with supermarkets, and the supermarkets were able to identify a lawful basis for receipt and processing of that personal data, in the circumstances of the shielding programme.

8. The ICO is now conducting a survey to assess what worked well in the rapid establishment of this programme and what lessons can be drawn for the future.

Annex B: The ICO's Regulatory Sandbox

1. The ICO's Regulatory Sandbox allows organisations to ensure they take a privacy by design approach when creating innovative products and services utilising personal data. The Sandbox process allows organisations, including SMEs, to work transparently with the ICO to take advantage of our data protection expertise and ensure that their product or service proactively complies with data protection legislation at the design stage.

2. For example, the ICO has worked with Onfido, an organisation which provides identity verification services on behalf of its business clients, to improve its service by ensuring that their Facial Recognition Technology (FRT) functioned fairly and inclusively for all data subjects by measuring and mitigating any perceived bias present in its FRT models.

3. In order to ensure that Onfido undertook its research to measure and mitigate bias in a manner that respects and protects the rights and freedoms of individuals (as far as their privacy is concerned), Onfido applied to enter the ICO's Regulatory Sandbox. Between July 2019 and August 2020 the ICO and Onfido worked together when considering the key data protection issues associated with this project which included considering:

    - complex data controllership issues relating to the data used by Onfido to train its FRT models;
    - whether Onfido were processing special categories of personal data when training their FRT models;
    - which GDPR lawful basis and conditions for processing were likely to be the most appropriate for Onfido to rely on to process personal data;
    - how Onfido should look to provide adequate privacy information about its processing activities to data subjects; and
    - how Onfido should facilitate data subjects' rights requests.

4. Through our work with Onfido in the Sandbox, the ICO has gained a valuable insight into the practical issues for a supply chain involved with the provision of AI services, particularly where the application of data protection legislation and guidance to such an environment is not always clear. It is hoped that the ICO's engagement with Onfido will allow the ICO to further develop its thinking on data protection based issues surrounding complex AI supply chains. This is an important step towards better clarifying how controllers and processors involved in such AI supply chains can ensure their compliance with UK data protection legislation. Ultimately, such clarity should result in privacy benefits to the data subject.

5. The ICO's Sandbox has now reopened and is accepting expressions of interest in participation from organisations with products and services which focus on

data sharing and the application of the ICO’s recently published Age appropriate design code (AADC).