The ICO's review into data sharing under the Digital Economy Act 2017

March 2023



Contents

Executive summary	3
Introduction	4
Our approach	5
The DEA Framework Review	7
The DEA data sharing reviews	15
Thanks	24
Appendices	25

Executive summary

- The Information Commissioner's Office (ICO) has undertaken a review of the data sharing powers under Part 5 of the Digital Economy Act 2017 (DEA).
- The work began with a pilot data sharing review beginning in March 2021. We completed the remainder of the review in summer 2022.
- We found that the framework for data sharing under the DEA provides a supportive background to help organisations share data in ways that benefit the public. The framework includes robust safeguards that ensure organisations share data responsibly and in alignment with data protection principles, while also safeguarding people's rights.
- We also found strong evidence of good practice in compliance with the DEA framework. Our data sharing review findings have shown that organisations are delivering the benefits of responsible, proportionate data sharing.
- Where we have found areas for improvement, we have found organisations responsive and open to our recommendations.
- Our recommendations will be valuable to other organisations planning to use the DEA powers in the future.

Introduction

The powers under the DEA offer important legal gateways that allow data sharing for the public benefit¹. They include for example, ensuring that the right people receive the energy bill rebates they are entitled to or providing the public sector with robust statistical information to understand our society and inform future policy interventions.

Data protection law enables the public sector to share personal data responsibly and this helps build public trust. When the former Information Commissioner, Elizabeth Denham, gave evidence to the Bill Committee for the Digital Economy Bill in 2016², she emphasised the importance of robust safeguards for data sharing, and she committed to undertaking a review of the framework for the DEA data sharing powers.

This report is a summary of the review we have undertaken to fulfil that commitment. It will give confidence to the public that the safeguards set out in the DEA provide a strong framework for responsible data sharing. Our report offers insights into the benefits to the public of data sharing under the DEA powers, particularly focusing on the safeguards and requirements set out in the DEA framework. Our data sharing reviews have also shone a light on areas of good practice and highlighted learning points which will be of value to government and other organisations considering using the DEA powers in the future.

¹ Appendix 2

² See Appendix 3

Our approach

We undertook our review in two parts, namely, by

- analysing the overall DEA framework, with a particular emphasis on the protections for personal data that the DEA framework offers; and
- undertaking a series of reviews of data sharing arrangements under each data sharing power under the DEA³.

DEA framework review

We reviewed the overall DEA framework (the DEA framework review), assessing the data protection safeguards and governance it provides through a documentary review of:

- the individual Codes of Practice for each type of DEA data sharing;
- the register of DEA data sharing agreements;
- the public registers of accredited researchers and accredited projects; and
- the public register of DEA accredited processing environments.

We also observed the operation of the DEA boards which are convened in relation to the DEA public service delivery power and the DEA debt and fraud powers.

Data sharing reviews

For the second and more extensive part of our review, we conducted a series of reviews of organisations involved in data sharing under the DEA. The ICO has the right to conduct audits under the Data Protection Act 2018 and the statutory DEA codes of practice also reference these powers.

Our reviews followed the data end-to-end for each sharing initiative. This allowed us to see the data flows, interactions and exchanges between data controllers, throughout the sharing initiative.

To support this end-to-end approach, we developed bespoke letters of engagement, toolkits, reporting and feedback mechanisms that allowed for short, focused reviews.

In spring 2021, we carried out a pilot review in relation to data sharing under the fuel poverty provisions of the DEA⁴. In this pilot, we concluded that our approach worked and specifically that the revised processes we had devised were fit for purpose.

³ Apart from data sharing under Chapter 6 of the DEA as there was no sharing under that Chapter involving personal data at that time

⁴ Sections 36 and 37 DEA

ICO review - Digital Economy Act 2017

We selected sample data sharing arrangements under each of the remaining chapters of Part 5 of the DEA for the remainder of the reviews, based on their complexity and varied approaches. We also aimed to offer a comprehensive review of the methodologies that data controllers used to manage the data sharing. We completed our work for these reviews in summer 2022.

All participants were keen to learn from our findings and make improvements.

The DEA Framework Review

The DEA statutory Codes of Practice

In the course of our review, we considered the governance arrangements under the DEA statutory codes.

The DEA Code⁵ – public service delivery, debt and fraud

The DEA Code came into effect before the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) came into force, although it looked ahead to the implementation of this legislation. The DEA code refers to the need to comply with the data protection legislation. It does not impose additional legal obligations but sets out principles and good practice in relation to data sharing under the DEA public service delivery, debt and fraud powers. These principles include:

- adopting a data protection by design approach;
- being familiar with the data protection legislation, the data protection principles set out in the DEA code and the ICO's data sharing code;
- seeking advice from legal advisers and data governance and security experts;
- conducting privacy assessments (or data protection impact assessments (DPIAs)); and
- providing information about the data sharing for inclusion in the DEA register.

Review boards

The DEA Code sets out the process for the review of data sharing proposals by review boards. There is a review board for the public service delivery powers and a separate board for the debt and fraud powers. These boards differ depending on the proposals before them, but proceed on similar lines.

The DEA boards consist of senior officials in relevant information governance or social policy areas (public service delivery) or appropriately qualified subject experts from across government (debt and fraud powers) and invited members from appropriate public representative bodies and the ICO as an observer.

Under the public service delivery powers, the board will consider proposals where the sharing needs a new DEA objective. In such cases, the board has to make recommendations to the relevant Cabinet Office minister about whether

⁵ Code of Practice for public authorities disclosing information under Chapters 1, 3 and 4 (Public Service Delivery, Debt and Fraud) of Part 5 of the Digital Economy Act 2017 - GOV.UK (www.gov.uk)

they should proceed with secondary legislation to provide a statutory basis for that new objective.

Under the debt and fraud powers, the board considers proposals for data sharing pilots. Engaging in pilots offers scope for novel data sharing initiatives, allowing organisations to use pilots iteratively, learning from initial outcomes. Pilots generally operate on limited datasets which helps reduce the risks of processing. Ultimately, if the pilot is successful, the board may recommend that it progresses to 'business-as-usual' data sharing, subject to the approval of the minister.

We observed that the meetings of the each DEA review board are generally well attended. Members regularly question the presenters on their proposals and provide valuable feedback, including on matters such as the necessity and proportionality of the proposed data sharing and on specific data protection matters, before making their recommendations.

Individual controllers will be responsible for compliance with the data protection legislation and with the DEA Code in relation to any data sharing they undertake under the DEA powers. However, scrutiny by the respective board, combined with the requirements of the DEA code (including requirements to report back to the board on outcomes and findings in the case of the debt and fraud powers), adds objectivity and rigour to the process.

There has, however, been some uncertainty on occasion in relation to both boards about the scope of the role of board members and the matters they could or should take into account when reaching a decision. In the case of the debt and fraud review board, this has included debates about the matters the board should consider when reviewing a proposal for a pilot to progress to 'business as usual'.

Our view

The DEA code is required to be consistent with the ICO's data sharing code of practice, as altered or replaced from time to time. The ICO has written a new data sharing code since the DEA code came into force. We therefore **recommend** that, to ensure that it remains of most value to those sharing data under DEA powers, the DEA code should refer explicitly to 'Data sharing: A code of practice.' ⁶

Our review highlighted that organisations were not clear about who should assume the responsibilities of a 'sponsoring authority' in paragraph 43 of the DEA code. Under the DEA code, a sponsoring authority is responsible for safeguards around data sharing with non-public authorities, including ensuring that their systems and procedures are appropriate for secure data handling. We

⁶ Data sharing: a code of practice | ICO

therefore **recommend** that the DEA Code defines the term 'sponsoring authority' more clearly so organisations know if they are sponsoring authorities and therefore are aware of their role and specific obligations under the DEA code.

We **recommend** that the DEA code includes supplementary guidance about the role of board members, and the factors they should consider when reaching their decisions. Such guidance should reflect the need to take into account both the legal requirements and the good practice recommendations contained in the DEA code. In particular, we **recommend** that such guidance explicitly emphasises the need for board members to factor into their deliberations any data protection concerns that might arise from the papers they receive. Such updated guidance will also be an opportunity to include any other areas of clarification, based on learnings from the use of the DEA powers to date. Guidance of this nature will be particularly valuable for new board members.

A practical inconsistency between the boards is that the debt and fraud board receives a data protection impact assessment (DPIA) prepared by the lead organisation in the data sharing as part of the papers for each proposal. In the case of the public service delivery powers, the board does not receive a DPIA or other risk assessment, although those presenting the proposals may provide information about such matters in other ways.

We recognise that in the case of the public service delivery board, the government department that develops the policy proposal may not be a controller of personal data when the data sharing eventually takes place. However, to ensure that all DEA data sharing proposals bake in the need for data protection by design and default, we **recommend** that the DEA code contains explicit guidance to ensure that both the public service delivery board and the debt and fraud board receive DPIAs (or other suitable alternative documentation setting out the potential risks and proposed mitigations of the processing of personal data) when considering the proposals before them.

Furthermore, we **recommend** that the DEA Code contains up to date live links to the DEA register of data sharing agreements.

ICO participation in DEA review boards

The ICO has attended both review boards as an observer, since they began. We do not provide regulatory approval to the proposals before either board but we may offer observations and regulatory advice. As part of this review, we have considered whether the ICO should continue to participate in board meetings.

The use of the public service delivery powers to create a new objective has not been well used to date, as only one new objective has so far progressed through the whole process, although it is likely that the public sector will use these powers more extensively in the future. As a result, the boards and the public sector more generally are still developing their understanding of data sharing under this power.

The board for the debt and fraud powers has recommended a considerable number of data sharing pilots for approval and has provided constructive comments on some proposals brought to the board for an initial review. However, although a number of the pilots have returned to the board for further development, the board has so far approved only one pilot for data sharing as 'business as usual'.

Our view

Although the responsibility for the governance of both review boards and their decisions rests with the board members and the secretariat, it is likely that we will have a continuing role in providing regulatory insights at the review board meetings, when appropriate, particularly while the boards continue to consider novel areas of data sharing and while some of the DEA powers are not yet well used.

Subject to the agreement of the respective boards, the ICO intends to continue in its role as an observer on both boards at the present time.

We will however conduct a review of ICO attendance on an annual basis in consultation with the boards and the secretariat.

The DEA Civil Registration Code⁷

The DEA Civil Registration Code contains detailed guidance about data sharing for civil registration officials and its principles expressly highlight the need for disclosures to comply with the data protection legislation. Other principles provide additional safeguards around these disclosures, such as:

- ensuring that the processing is lawful and fair;
- guidance about the need for data sharing agreements and keeping them under review;
- detailed questions as part of a consistent application process for disclosure, highlighting tangible benefits, as well as addressing potential risks, for example, in relation to security when transferring information outside the UK; and
- submitting the relevant information about the sharing for inclusion in the DEA register.

Data Sharing Code of Practice: code of practice for civil registration officials disclosing information under section 19AA of the Registration Service Act 1953 - GOV.UK (www.gov.uk)

Our view

The DEA Civil Registration Code states that it is to be read alongside the ICO's data sharing code of practice, as altered or replaced from time to time. Therefore, as for the DEA code above, we **recommend** that, to ensure that it provides up to date guidance, the DEA Civil Registration Code should refer explicitly to 'Data sharing: A code of practice.'8

We also **recommend** that the DEA Civil Registration Code contains live links to the DEA register of data sharing agreements.

The DEA research code

The DEA research code includes both a Code of Practice and Accreditation Criteria. The Code of Practice relates to disclosures, processing, and the holding or use of personal information under the DEA research power. 10

The DEA research code includes safeguards around the de-identification of data and avoiding accidental or intentional disclosure of identifying data. It also contains seven principles (confidentiality, transparency, ethics and the law, public interest, proportionality, accreditation, retention and onward disclosure) that govern the disclosure of data.

The Accreditation Criteria include safeguards relating to processors, researchers/peer reviews and research projects, and in particular, the need for processors and researchers/peer reviewers to have appropriate skills and experience. Processors need to agree to comply with data policies which set out the requirements for processing under the research power.

Research projects must be in the public interest and meet appropriate ethical standards. The data must also be appropriate for the proposed research and all researchers must be named and accredited.

All processors and researchers (or peer reviewers) must agree to being included on public registers which are maintained by the UK Statistics Authority.

Our view

The Research Code of Practice contains reference to the ICO's data sharing code 2011. We **recommend** that the Research Code of Practice and Accreditation

⁸ Data sharing: a code of practice | ICO

⁹ Research Code of Practice and Accreditation Criteria - GOV.UK (www.gov.uk)

¹⁰ DEA Part 5, Chapter 5

Criteria should refer explicitly to 'Data sharing: A code of practice.' 11

The DEA Statistics Code¹²

The Statement of principles and procedures provides guidance for use of the DEA statistics power.¹³ It also includes a code of practice on changes to data systems, with guidance for public authorities when they make changes to their processes for collecting, organising, storing or retrieving information, or their processing for supplying information to the Office for National Statistics or the UK Statistics Authority.

The DEA statistics code contains six principles (confidentiality, transparency, ethics and the law, public interest, proportionality, collaboration) aimed at ensuring that high ethical and legal standards apply in the statistical life cycle. ¹⁴ In addition, the Office for National Statistics and the UK Statistics Authority are required to have regard to guidance and codes of practice, including the data protection legislation, ICO guidance and the ICO's 2011 data sharing code of practice.

Our view

We **recommend** that the DEA Statistics Code should refer explicitly to 'Data sharing: A code of practice.' 15

Summary - the DEA Codes

Although we have made recommendations for some updating and additional clarity, all the DEA Codes contain detailed guidance and safeguards around potential data sharing under the DEA. They focus on the need for strong protection standards for individuals' personal data to ensure that organisations use the DEA powers responsibly for public benefit.

Undertaking a review of each of the DEA codes will be an opportunity to update the references to guidance and other resources that they contain, and to ensure the removal of any withdrawn or obsolete guidance, where applicable.

Any revision of the DEA Codes requires consultation with the ICO as set out in the DEA. We welcome engagement with the relevant stakeholders in this process to ensure the DEA Codes are up to date, and provide clarity to all participants in

¹¹ Data sharing: a code of practice | ICO

¹² Statistics Statement of Principles and Code of Practice on changes to data systems - GOV.UK (www.gov.uk)

¹³ DEA, Part 5, Chapter 7

¹⁴ Paragraph 3.2 The DEA Statistics Code

¹⁵ Data sharing: a code of practice | ICO

the data sharing processes set out in them, as well as for those who scrutinise the data sharing that takes place.

The DEA framework review – the DEA registers

We did not undertake a full review of the DEA registers, but we took them into account when formulating our view of the overall DEA framework.

DEA register of data sharing agreements

The Central Digital and Data Office in Cabinet Office (CDDO) maintains a register on GOV.UK of the information sharing agreements that take place under the public service delivery, civil registration, debt and fraud powers of the DEA.¹⁶ This register was previously maintained by the Department for Digital, Culture, Media and Sport (DCMS). The register takes the form of a spreadsheet that sets out details of the DEA data sharing agreements, including names of the participants, and details of the DEA power they are exercising.

The CDDO is dependent on individual controllers supplying the required details for inclusion in the register in a timely way. This has led to delays in publishing information about some data sharing agreements.

Public registers: Accredited researchers and accredited projects and DEA Accredited processing environments

UK Statistics Authority maintains registers of accredited researchers and projects¹⁷ and a list of DEA accredited processing environments.¹⁸ UK Statistics Authority also accredits potential processors against the security controls required under the ISO27001 standard.

Our view

It is reassuring that the information about DEA sharing is publicly available. Each register is an important tool in ensuring transparency as well as being a measure of accountability for the participating organisations.

We welcome the recent positive steps to improve the presentation and quality of the information contained in the DEA register of data sharing agreements, which work is continuing.

With the passage of time, each register will include a greater amount of information relating to the activities it needs to record. We therefore **recommend** that the respective owners of each register consider how they can

¹⁶ Register of Information sharing agreements under chapters 1, 2, 3 and 4 of part 5 of the Digital Economy Act 2017 - GOV.UK (www.gov.uk)

¹⁷ Public Registers: Accredited Researchers and Accredited Projects – UK Statistics Authority

¹⁸ List of Digital Economy Act Accredited Processing Environments – UK Statistics Authority

better present this information in user-friendly ways, for example, allowing for easy sorting and filtering.

In the case of registers that record data sharing and researchers/research projects, additional information about the current status of data sharing would ensure a public record exists, even if full details are not yet available. All the registers also need to allow users to easily distinguish between activity that is ongoing, and activity that is discontinued or complete.

Such measures will ensure that the registers remain readily understandable to the public and interested organisations. They will ensure that the volume and detail on each register do not adversely impact the effectiveness of that register as a transparency measure.

The DEA data sharing reviews

We reviewed data sharing taking place under Chapters 1-5, and 7, Part 5 DEA. We did not review Chapter 6 as there was no sharing involving personal data. The reviews related to:

- Warm Homes Discount Scheme (WHDS) sharing data to verify the eligibility of low income households for rebates against electricity bills under the WHDS. This annual data share ensures that energy suppliers can apply rebates to the accounts of those who are entitled to them. (Fuel poverty)
- life event verification sharing data about validation checks to support applications for grants of probate. This ongoing data sharing aims to improve delivery of the service, by streamlining processes, improving accuracy and creating simpler customer processes, as well as reducing costs and reducing fraud and error. (Civil registration)
- pilot to establish levels of debt and vulnerability matching data to help authorities to manage and reduce debt and identify vulnerability among debtors. Participants expect that outcomes of the data sharing will ensure that they can offer support to vulnerable people as well as improve debt recovery. The data sharing will also provide efficiencies and coordination opportunities for debt enforcement action. (Debt)
- pilot to identify fraud in the public sector sharing data to identify suspected fraud in claims for Covid support measures. This ongoing data sharing aims to establish where claimants have applied for support to which they were not entitled. (Fraud)
- undergraduate data sharing data to research into education choice and its effects on several domains such as labour markets, marriage and health. Participants expect that studies into the effects of changes to admission policies will inform policy makers and universities. Further linkage with other education datasets, and potentially employment data, will provide insights into the role of education choice in outcomes. (Research)
- prisoner data sharing data about prisoner population data to develop more accurate and cost effective means of monitoring population change, and meet user needs for population and migration statistics. (Statistics)

Review methodology

We identified and reviewed 17 stakeholders using an audit style to develop our review approach. We reviewed a small number of stakeholders twice due to their

involvement in more than one of the sharing agreements that we selected for review.

Traditionally, an audit will undertake a broad review of the data protection compliance of a single data controller. For these reviews we followed the path of the personal data in a sharing agreement from end to end between all participating controllers. Our approach in following the data journey was intended to provide a sense of how effectively and securely organisations complied with the obligations of the data protection legislation and the good practice recommendations contained in the DEA codes, including ensuring transparency and protection for the rights of individuals.

We assessed organisations against key controls, including ICO guidance. We also developed a suite of new toolkits, controls and templates for recording evidence. We developed bespoke letters of engagement and reporting templates to meet the needs of this review, including addressing the expectations of the overall review. Our emphasis on reporting was to highlight where organisations were sharing compliantly, and, where possible, to add value. Detailed reports also provided scope to explain and educate organisations, especially where this was our first time reviewing this aspect of data sharing and particularly where private and public organisations are involved end to end.

We used the ICO's standard audit methodology to complete a review of requested documentation and evidence, followed by a series of interviews with key staff involved in the data sharing process and wider data protection governance of the organisations. The controls covered, and evidence requested were bespoke to the requirements of each review and dependent on participants' role within each selected data share. The reporting did not follow a standard approach but was developed to include detailed findings against each control, along with any observations or recommendations as necessary to support the formative nature of the engagement.

We accounted for the organisational structure of the participating controllers/processors and the nature and extent of their processing of personal data, when developing the review scopes and tailored the common controls that we were testing as required. So, while each review report took into consideration the different roles of each data controller in the data sharing, we could make comparisons in their performance due to the use of common controls. Although the reviews looked at multiple data controllers and their participation in the data sharing agreements from beginning to end, the scope was relatively narrow, focusing on key aspects of:

- governance oversight (as well as end-to-end oversight)
- data sharing
- transparency and accountability
- privacy notices
- DPIAs

- any automated decisions and the implications
- information security
- records management
- data minimisation/augmentation
- training
- outside or competing regulatory requirements

In preparing participants for the review, we explained that we would advise them of any information security or legislative breaches we found.

It is standard practice to give a controller the opportunity to remedy high priority and urgent findings within an agreed period of time. The team then completes a follow-up to identify what findings the organisation has remedied and considers what further action we may need to take at that stage, according to the ICO's Regulatory Action Policy. 19 We reserve the right to consider regulatory action depending on the severity and nature of the finding.

While the reviews of DEA data sharing agreements were consensual, they did not preclude regulatory action, where necessary. All the data controllers who participated were comfortable to work with us on this basis.

Follow up and feedback

Each organisation has received a detailed report of our findings, including recommendations to amend non-compliance or improve practice, where relevant.

In the course of our reviews, we were struck by the enthusiasm of the participating organisations. All organisations were keen to know what they had done well, and how they could improve. The feedback we received has reflected the positive nature of their experiences. In particular they reported that:

- the reviews helped them understand their key risk areas with regards to their data sharing activities; and
- the recommendations we made were constructive and appropriate.

We supported the compliance teams in each organisation at an operational level as part of their continuous improvement cycle. We therefore took account of their registers of risk, action plans and associated management information. This information, together with our review findings and action plans, helped us understand how they had improved their practices when we followed up on our reviews.

In our follow up engagements, we reviewed how participants implemented our recommendations and identified if they needed any further advice. In most

¹⁹ Regulatory Action Policy (ico.org.uk)

cases, the organisation had already implemented the majority of our recommendations, before we followed up with them.

We have not found it necessary to take any regulatory action in relation to any of the participants reviewed.

Our data sharing review findings – summary

We analysed the reports of each of the 17 participating stakeholders to identify any recurring themes of good practice or areas for improvement.

The evidence suggests that, in general, the organisations we reviewed were largely aligned with the statutory code: Data Sharing: A Code of Practice²⁰ when sharing under the DEA powers and also with key supporting controls for data protection. Generally, these organisations performed well.

Notably, the majority of our recommendations across the review were of 'medium priority' ²¹ indicating that our recommendations were to enhance mitigating controls already in place, rather than to implement controls to address outstanding uncontrolled risks or non-compliance.

We encountered one organisation that performed less well where our review highlighted a number of significant areas for improvement. These findings were wide ranging and did not specifically relate to the use of the DEA powers. The organisation has accepted our findings and we are working with them to ensure they successfully implement improvements and maintain future compliance with data protection legislation.

Compliance with the data protection legislation

Generally, we found that organisations had good policies and procedures for managing the principal data protection rights under the data protection legislation. The use of common controls across the reviews meant that we could identify recurring good practice points as well as recurring areas for improvement across all the sharing agreements we reviewed. Most areas for improvement related to the need to extend policies and procedures within their data sharing agreements to ensure a collective responsibility to uphold those rights.

Compliance with the DEA obligations

We selected the control areas with the aim of reviewing a broad range of data protection compliance matters within the narrow scope of each data sharing activity, including the crossover between the data protection legislation and DEA

²⁰ Data sharing: a code of practice | ICO

²¹ See Appendix 4

compliance. As part of our assessment, we assessed where those obligations crossed over with the relevant DEA Code of Practice for the data share, and any further requirements unique to these codes.

In this context, it is important to note that any failure to comply with the data protection legislation also means there is a failure to comply with the relevant DEA Code of Practice.

We made two recommendations that specifically related to the DEA Code:

Our view

In our review of the fuel poverty data sharing²², we made a recommendation for clarity in relation to paragraph 43 of the DEA Code. This states that non-public authorities can only participate in an information sharing arrangement once their sponsoring public authority has assessed their systems and procedures as appropriate for secure data handling. In this instance, the DEA Code does not make it clear which organisation would be the 'sponsoring public authority'. We **recommend** a review of paragraph 43 to define this term more clearly.

Data usage agreement documentation that we reviewed as part of the Chapter 4 (fraud) review did not include a number of the contractual clauses detailed in Section 4 of the DEA Code. We therefore recommended strengthening the obligations set out in the relevant contracts and adding clauses to meet the requirements of the DEA Code.

Our data sharing review findings – Control areas

Governance

Having robust governance and accountability processes in place is essential to ensure that an organisation can demonstrate sufficient oversight, accountability, and consistency in its data sharing processes.

Areas of good practice:

- formal data sharing agreements in place between all parties involved in the data sharing processes;
- good overarching governance structures in place;
- organisations had data protection officers with supporting teams in place to carry out their functions, and information steering groups or equivalent to monitor data sharing activities;

²² DEA, Part 5, Chapter 1

 all staff we interviewed that were involved in the operational side of the data sharing arrangements demonstrated an excellent level of awareness around their role in the process.

Areas for improvement: we made recommendations about how organisations could enhance their existing governance controls, in particular by backing up processes with supporting documentation. Our recommendations included:

- ensuring appropriate internal data sharing policies are in place and accurately reflect governance arrangements about how the organisations review and approve the sharing agreements;
- documented agreements in place for the process of notifying data sharing partners in the event of a data breach;
- ensuring that the Record of Processing Activities (ROPA) documentation is in place, and data sharing arrangements included on the ROPAs include the information required under Article 30 of UK GDPR;
- ensuring that logs of sharing arrangements are in place and regularly updated to ensure they present an accurate reflection of all the data sharing activities an organisation is party to;
- documenting the roles and responsibilities involved in the DEA data sharing process;
- ensuring adequate specialist training, and undertaking a training needs analysis to ensure staff involved in the data sharing process receive sufficient training for their roles.

Transparency

Organisations must have appropriate controls in place to ensure that individuals are informed about how their personal data is processed, as required by UK GDPR Article 5(1)(a).

Areas of good practice:

- most participating organisations were able to demonstrate that they had considered transparency of processing sufficiently within the data sharing process;
- organisations provided individuals with privacy information at the time they collected their personal data;
- where organisations obtained data through a data sharing agreement, they actively published privacy information or communicated it to individuals to keep them informed on how they collect, process and/or share the personal data.

Areas for improvement: we made recommendations about how participants should improve their documentation, to ensure that privacy information they provide remains transparent and accessible. Our recommendations included:

- ensuring there is a defined process in sharing agreements for how to handle individual rights requests, such as subject access requests, with data sharing partners;
- ensuring individuals can withdraw consent (where applicable), ensuring clear guidance on how to do this (and its consequences) is readily available to data subjects on privacy notices or application forms relating to data sharing;
- ensuring that privacy notices contain full and accurate information about the retention period for data collected and shared under DEA sharing agreements.

Data quality and retention

Organisations must have appropriate Records Management processes in place to ensure compliance with UK GDPR Articles 5(1)(d)(accuracy) and (e)(storage limitation).

Areas of good practice:

- all the data sharing agreements we reviewed shared only the personal data actually needed;
- organisations showed us that they were using pseudonymisation and data minimisation techniques where possible to prevent sharing excessive or unnecessary personal data;
- in most of the data sharing arrangements we reviewed, organisations had thorough and detailed data quality and accuracy review processes.

Areas for improvement: we made recommendations about how participants should improve their documentation. Our recommendations included:

- ensuring that retention periods for shared data sets are set and recorded consistently across documentation;
- ensuring that formalised internal processes are in place to manage adherence to retention schedules;
- making sure checks are carried out with data sharing partners to confirm shared data has been deleted in line with agreed schedules;
- making sure there are processes in place to inform data sharing partners when data is found to be inaccurate.

Privacy impact assessments

Completing a Data Protection Impact Assessment (DPIA) in line with the requirements of UK GDPR Article 35 is necessary for organisations to ensure that no high risk processing takes place without considering and implementing

mitigating controls.

This was the area that showed the broadest variation in compliance between the organisations we reviewed – some showed us good practice in relation to DPIAs, while others needed further support in this area.

Areas of good practice:

- some organisations showed us an exemplary approach to DPIAs they completed them before processing took place and their documentation contained thorough, detailed assessments including mitigating actions for any identified risks;
- all organisations appointed suitably senior members of staff with responsibility for information risk management;
- all organisations assigned staff as information asset owners to ensure there were accountable risk owners in place;
- all organisations demonstrated an awareness that high risk processing should be referred to the ICO for review.

Areas for improvement: the following are examples of the recommendations we made for organisations that needed additional support in this area:

- the need to carry out DPIAs before sharing data;
- providing sufficient detail on DPIA documents about data shares for example, the volume of data being shared;
- detailing the lawful basis relied on with sufficient detail. For example, if public task is relied on as the lawful basis, the DPIA needs to show how it is documented in law;
- ensuring staff appointed with responsibility for the management of information risk have appropriate visibility and have final sign-off of DPIAs:
- undertaking reviews of DPIAs on a routine basis;
- providing sufficient DPIA training for staff involved in the process.

Security

Having appropriate security measures in place is essential to prevent data breaches such as unlawful access to information, and the damage and/or distress for individuals who are the subject of the impacted data.

Areas of good practice:

 all participants showed us that they had technical security measures in place that were proportionate to the data being processed to protect the data received and transmitted; all staff interviewed that were involved in the operational side of the data sharing arrangements demonstrated excellent information security awareness and data sharing best practice knowledge.

Areas for improvement: we made recommendations about how participants should improve security for personal data, including providing documentation to ensure accountability and consistency in their procedures. Examples of our recommendations are:

- ensuring that documented operational procedures for data sharing are in place;
- ensuring that data breach protocol documentation includes details on the procedures for informing individuals in the event of a breach;
- ensuring that access permissions are reviewed routinely and documented.

Thanks

We would like to note that all the organisations who participated in these reviews did so consensually and allowed the ICO Assurance team to complete a detailed scrutiny of data sharing practices, despite no prior perceived risk or concern for their data processing.

The ICO would like to thank all participants for their support of this review of the DEA powers.

Appendices

Appendix 1: Summary of DEA framework recommendations

Area	Recommendation
The Code of Practice for public authorities disclosing information under Chapters 1, 3 and 4 (Public Service Delivery, Debt and Fraud) of Part 5 of the Digital Economy Act 2017	 Explicit reference to 'Data sharing: A code of practice.' ²³ Clarification of the term 'sponsoring authority' in paragraph 43 Inclusion of guidance for board members, including the need to factor data protection concerns into their deliberations Guidance that both review boards receive DPIAs or similar documents Inclusion of live links to the DEA register of data sharing agreements
The Data Sharing Code of Practice: code of practice for civil registration officials disclosing information under section 19AA of the Registration Service Act 1953 of Part 5 of the DEA 2017	 Explicit reference to 'Data sharing: A code of practice.' Inclusion of live links to the DEA register of data sharing agreements
Research Code of Practice and accreditation criteria	 Explicit reference to `Data sharing: A code of practice.'
Statistics Statement of Principles and Code of Practice on changes to data systems	 Explicit reference to 'Data sharing: A code of practice.'
DEA registers	 Improvement in the presentation of information in the registers

²³ Data sharing: a code of practice | ICO

Appendix 2: The DEA powers – sharing for better public services

The DEA is divided into seven Chapters, each providing a different purpose for sharing:

- Chapter 1: the disclosure of information to improve public service delivery;
- Chapter 2: the disclosure of civil registration information to allow public authorities to deliver their functions more effectively;
- Chapter 3: the disclosure of information for recovering debt owed to the public sector;
- Chapter 4: the disclosure of information for the purposes of combating fraud against the public sector;
- Chapter 5: permitting public authorities to share de-identified information with accredited researchers for the purposes of research in the public interest;
- Chapter 6:24 enabling HMRC, the Welsh Revenue Authority and Revenue Scotland to share general and aggregate data, which is non-identifying information, to allow them to play a wider role in policy development;
- Chapter 7: supporting the reuse of administrative data and access to real time data to produce up to date national and official statistics.

Appendix 3: The commitment to review

On 13 October 2016 the former Information Commissioner, Elizabeth Denham, appeared at the Public Bill Committee for the Digital Economy Bill (Third Sitting). The Commissioner gave a commitment to carry out a review of the data sharing arrangements contained in the Bill, specifically with regards to compliance with data protection legislation.

In the former Information Commissioner's letter²⁵ dated 7 December 2016 to the Minister of State for the Department of Digital, Culture, Media and Sport (DCMS), she reiterated her intention to review all the powers in Part 5 of the DEA.

 $^{^{24}}$ We did not review data sharing under Chapter 6 of the DEA as there was no sharing under that Chapter involving personal data at the time

²⁵ See Appendix 2





Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF T. 0303 123 1113 F. 01625 524510 www.ico.org.uk

Rt Hon Matthew Hancock MP Minister of State for Digital and Culture Department for Culture Media and Sport 4th Floor, 100 Parliament Street London SWIA 2BO

7 December 2016

Digital Economy Bill

Dean Mr. Hancock:

Thank you for giving me an opportunity to discuss my remaining concerns about the privacy implications of the Digital Economy Bill at my recent meeting with you. You are aware of my views that additional safeguards on the face of the Bill are needed to ensure effective protection for individuals and would help build greater trust and transparency in data sharing for the public. As the Bill starts its journey through the House of Lords, I thought it would be helpful if I reiterated the main points I raised about Part 5 of the Bill.

I am also aware that the clauses on age verification for access to online pornography have become a focal point of debate during the passage of the Bill through the Commons; therefore, I would like to highlight my concern that there is a significant privacy risk if the implemented age verification systems do not have the right safeguards.

Data sharing safeguards

As you are aware, my main concern is that there are sufficient safeguards in Part 5 of the Digital Economy Bill. We discussed a number of possible safeguards including data sharing registers and references on the face of the Bill to Privacy Impact Assessments (PIAs) and our Privacy Notices Code, and why further transparency is important. It is vital that there are two strong layers of transparency for data sharing – to enable effective delivery of key information to the public and more detailed information to enable more active groups to scrutinise and hold public bodies to account for the data sharing. I welcome the references to the importance of privacy impact assessments and privacy notices in the four draft codes of practice but I am strongly in favour of reference to them in the Bill itself.

The evidence I gave to the Bill Committee highlighted the importance of the transparency requirements in the GDPR and including PIAS on the face of the Bill will support the requirements of the GDPR. I am supportive of data registers as a transparency measure although I don't believe it would be necessary for the ICO to maintain an overarching register.

I believe it is important for Parliament to review all aspects of data sharing, not just the clauses relating to fraud and debt, after an appropriate time. This will allow for objective consideration of whether the data sharing is transparent, necessary and proportionate in practice. When I appeared before the Public Bill Committee I said it was my intention, using the powers in the Data Protection Act 1998, to review and to report back to Parliament two to three years into this regime, with particular regard to bulk data sharing.

I also remain committed to making the case for an additional offence for re-identifying anonymised personal information, as recently added to Australian law. I would be keen for it to be covered in work on sanctions and penalties for GDPR implementation if not in Digital Economy Bill.

I also recommended that the government undertake further work to develop consistency between the codes that accompany Part 5 of the Bill and align them more closely with my statutory data sharing code of practice. I am pleased that your officials continue to work closely with mine on the development of these codes.

Age verification for access to online pornography

The provisions on age verification for access to online pornography have been widely debated during the passage of the Bill through the Commons. I have been clear in my evidence to the Public Bill Committee and my more detailed response to the DCMS consultation, about the importance of a privacy by design approach in implementing any age verification system. I consider there is a significant privacy risk if the implemented systems do not have the right safeguards.

I consider that it is not privacy intrusive for an individual to be able to prove who they are in a secure and reliable way – or to prove that they have a particular attribute (for example, that they are of a particular age). Any solution used needs to find a balance between verifying the age of individuals and minimising the collection and retention of personal data. It also needs to address in a proportionate way the issue of confirming that it is an adult using a device, or sitting at terminal equipment. It is important that any implemented system must be compliant with the requirements of the Data Protection Act and the Privacy and Electronic Communications Regulation.

I therefore propose that a provision is added to the Bill that would create an obligation to take privacy by design approach, which could be set out in a new code of practice.

I continue to be asked for my views on various parts of the Bill and it is likely that this will continue during the passage of the Bill through the Lords. I will of course provide my perspective as necessary but in the interests of transparency I hope this letter is helpful in articulating my remaining concerns and would be happy to have further discussions on any of these points.

Elizabeth Denham

Information Commissioner

Jams sincerely

This letter has also been addressed to Chris Skidmore MP

Appendix 4: Priority ratings for review findings

Urgent Priority Recommendations -

These recommendations are intended to address risks which represent clear and immediate risks to the data controller's ability to comply with the requirements of data protection legislation.

High Priority Recommendations -

These recommendations address risks which should be tackled at the earliest opportunity to mitigate the chances of a breach of data protection legislation.

Medium Priority Recommendations -

These recommendations address medium level risks which can be tackled over a longer timeframe or where some mitigating controls are already in place, but could be enhanced.

Low Priority Recommendations -

These recommendations represent enhancements to existing controls to ensure low level risks are fully mitigated or where we are recommending that the data controller sees existing plans through to completion.