*Draft code of practice to be laid before Parliament until approved by a resolution of each House of Parliament.*

Department for
Digital, Culture,
Media & Sport

# Code of Practice for Public Authorities Sharing Information with Digital Verification Services

**October 2026**

*Draft code of practice to be laid before Parliament until approved by a resolution of each House of Parliament.*

**Department for Digital, Culture, Media & Sport**

# Code of Practice for Public Authorities Sharing Information with Digital Verification Services

Presented to Parliament pursuant to section 49 of the Data (Use and Access) Act 2025

October 2026

© Crown copyright 2026

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at:

Department for Digital, Culture, Media and Sport
100 Parliament Street
London SW1A 2BQ
Email: enquiries@dcms.gov.uk
Tel: 020 7211 6000

ISBN 978-1-5286-6495-0

E03606945 10/26

Printed on paper containing 40% recycled fibre content minimum

Printed in the UK by HH Associates Ltd. on behalf of the Controller of His Majesty's Stationery Office

# Contents

**1. Overview ..... 5**

**2. Explanation of legal powers ..... 7**

2.1 Conditions required to enable the information sharing power ..... 7

2.2 Fees ..... 8

**3. Relevant legislation ..... 9**

3.1 Overview ..... 9

3.2 Data Protection Legislation ..... 9

3.2.1 General ..... 9

3.2.2 Data Protection Principles ..... 11

3.3 Human Rights Act 1998 ..... 11

3.4 Equality Act 2010 and Gender Recognition Act 2004 ..... 11

**4. Process for using the information sharing power ..... 12**

4.1 Step 1: Preparing to share information ..... 12

4.1.1 What is the DVS Register ..... 12

4.1.2 How to check the DVS register ..... 13

4.1.3 Considerations when preparing to share information ..... 13

4.1.4 Data Protection Impact Assessment (DPIA) ..... 15

4.1.5 Data evaluation ..... 16

4.2 Step 2: Deciding what to share and why ..... 16

4.2.1 Digital verification purposes ..... 16

4.2.2 Data minimisation ..... 17

4.2.3 Data accuracy ..... 17

4.2.4 Data sharing agreements ..... 18

4.2.5 Sharing information with third parties ..... 20

4.3 Step 3: Sharing the information ..... 20

4.3.1 Technical solution ..... 20

4.3.2 Privacy information ..... 20

# 1. Overview

1. This statutory code of practice (the "**Code**") has been issued under section 49 of the Data (Use and Access) Act 2025 (the "**Data Act**"). The Code provides guidance for public authorities in disclosing information under section 45 of the Data Act.

2. Section 45 applies when a registered digital verification service ("**DVS**") provider requests information about an individual from a public authority for the purpose of providing the individual with DVS, at their request. It provides public authorities with the power to disclose that information to that provider for that purpose.

3. The Code sets out guidance for public authorities to follow when sharing information under section 45 of the Data Act. It also directs public authorities to existing legal obligations that need to be complied with in disclosing information under section 45, but it does not purport to be a statement of the law.

4. In the context of this Code, "public authority" is given the meaning set out in section 45(8) of the Data Act. "DVS" is defined in section 27 of that Act. The DVS Register is defined in section 32 of the Data Act and described in more detail in 4.1.1 of this Code. A DVS can be registered on the DVS Register whether it is based in the UK or internationally.

5. The intended audience for this Code is public authorities who may share information under section 45. Such public authorities must have regard to this Code in disclosing information under section 45 as required under section 49(3) of the Data Act. This includes public authorities in England, Wales, Scotland and Northern Ireland.

6. When section 45 is commenced, it will not be commenced in respect of the Revenue and Customs (HMRC), Welsh Revenue Authority and Revenue Scotland. The information sharing power under section 45 for these authorities will be commenced at a later date, and the Code will be revised if necessary to account for this.

7. Similarly, sections 46 to 48 of the Data Act, which refer to onward sharing of data received from HMRC, Welsh Revenue Authority and Revenue Scotland, are not in force. These will be commenced when the information sharing power for these authorities is commenced, as described above.

8. The Government has consulted Welsh Ministers, Scottish Ministers and the Department of Finance in Northern Ireland in preparing the Code, as required under section 49(5)(b)-(d) of the Data Act, and such other persons as the Secretary of State considers appropriate.

9. This Code has been developed to be consistent with the Information Commission (ICO) data sharing code of practice (the "**ICO Data Sharing Code**"), as required under section 49(2) of the Data Act. Furthermore, the Government has consulted the Information Commission in preparing the Code, as required under section 49(5)(a) of the Data Act.

10. The Code may be revised from time to time, and any new versions will be laid before Parliament. As this is the first version of the Code, the Government welcomes feedback from stakeholders that will help inform future versions. Any revisions to the Code will follow consultation with the same persons listed above as per section 49(5) of the Data Act.

11. Public authorities operating in Wales must comply with any statutory duties they have to provide services in Welsh and ensure that information requests in Welsh are treated no less favourably than those in English, and similarly that information stored in Welsh is treated no less favourably. The Bilingual Technology Toolkit provides practical guidance to help organisations design, procure and deliver digital services that offer an equally high-quality user experience in both Welsh and English, with bilingual provision built in from the outset.

12. Welsh public authorities should also consider the Wales Accord on the Sharing of Personal Information. This will include using the relevant templates as appropriate and following the principles of the Accord. Scottish public authorities should consider the Scottish Information Toolkit.

# 2. Explanation of legal powers

## 2.1 Conditions required to enable the information sharing power

13. Section 45 of the Data Act applies when a registered DVS provider requests information about an individual from a public authority, for the purpose of providing the individual with DVS at that individual's request. The request must be made in in relation to delivery of a DVS in respect of which the DVS provider is registered. This is important to note as a registered DVS provider could provide some services which are registered and some which are not.

14. Section 45(2) provides public authorities with the power to lawfully disclose the requested information to the registered DVS. Section 45 also provides that certain conditions must be met for the public authorities to exercise this power. The following section outlines these conditions as set out in section 45 of the Data Act.

15. Firstly, the public authority must have received a request for information about an individual from a registered DVS provider for the purpose of providing DVS for that individual. Public authorities must ensure the DVS is certified by an accredited conformity assessment body and is currently registered on the DVS register. There is further guidance on this in 4.1.1 and 4.1.2 of this Code.

16. Secondly, section 45(1)(b) of the Data Act makes it clear that information can only be shared with such a registered DVS provider where the individual to whom the information relates has requested their service(s), and the disclosure of information is for the purpose of providing the DVS for the individual. There is further guidance on this in 4.2.4 of this Code.

17. Finally, public authorities are not permitted to share information under section 45 which:

    1. is prohibited by any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016; or

    2. would contravene the data protection legislation (as set out in 3.2 of this Code); or

    3. was obtained by the authority otherwise than in connection with the exercise of its functions of a public nature.

18. As section 45(6) of the Data Act makes clear, the information sharing power under section 45(2) does not override existing powers to disclose information.

## 2.2 Fees

19. Section 45(7) of the Data Act allows a public authority to charge fees to registered DVS providers who are requesting information under section 45.

20. Public authorities can decide the level of fees and fee charging structure in respect of the disclosure of information under section 45, but this should be proportionate and fair and in line with public law principles. Fees must be cost neutral and not be used to make a profit. For example, public authorities may choose to implement a cost per check model, an upfront payment model, or a combination of these models.

21. When setting a fee charging scheme, it is important for public authorities to do so in a transparent, evidenced manner and without unequal treatment. Public authorities are strongly advised to seek specialist advice, such as from their financial or commercial teams, when designing this scheme.

22. When considering the structure and level of fees, public authorities can take into account the costs accrued for setting up, maintaining and improving systems, including the administration and governance for data sharing as well as the technical architecture.

23. Public authorities should comply with HM Treasury Managing Public Money Guidance or its equivalents produced by devolved governments. The Scottish equivalent is the Scottish Public Finance Manual. The Welsh equivalent is the Managing Welsh Public Money guidance. The Northern Irish equivalent is Manging Public Money NI guidance. Each set of guidance highlights the need for public authorities to act transparently in the application of fees and charges.

24. It is recommended that contractual agreements are put in place between the public authority and the registered DVS provider before information sharing takes place. This agreement should set out the structure and level of fees.

# 3. Relevant legislation

## 3.1 Overview

25. In order to disclose information lawfully to registered DVS under section 45 of the Data Act, public authorities must comply with relevant legislation. This includes the data protection legislation, the Human Rights Act 1998 and the Investigatory Powers Act 2016.

26. The following section signposts to some of the key legislative provisions which public authorities need to comply with in disclosing information to DVS under section 45. However, public authorities must be mindful of all legislative obligations which may be relevant to them or the specific dataset when sharing information under section 45.

## 3.2 Data Protection Legislation

### 3.2.1 General

27. The Data Protection Act 2018 ("**DPA**") and the UK General Data Protection Regulation ("**UK GDPR**") and any regulations made under that legislation, form the UK's data protection legislation (see the definition in section 3(9) of the DPA).

28. Public authorities sharing information under the power in section 45 of the Data Act are required to comply with the data protection legislation. As per section 45(4) of the Data Act, this information sharing power does not authorise the disclosure of information which would contravene existing data protection legislation. However, the section 45 power in the Data Act will be taken into account when determining whether a disclosure contravenes that data protection legislation.

29. This Code is consistent with the ICO's Data Sharing Code, as required by section 49(2) of the Data Act. When implementing guidance set out by this Code public authorities must ensure the steps they take are compliant with any relevant legislation and guidance. If a public authority is unsure or has concerns as to whether a proposed instance of information sharing is permitted, they should seek advice from their data protection officer and/or another suitably qualified responsible person.

30. A public authority will be processing personal data when sharing information under section 45 (and when preparing to share such data) and so the data protection legislation applies. "Personal data" is defined in the data protection legislation.

31. For the purposes of this Code, the term “information sharing” will include the sharing of personal data but also may extend to information more widely as it relates to providing DVS, and therefore has a broader meaning than the term “data sharing”. Data protection legislation does not apply to non-personal data.

32. Public authorities making the decision to exercise this power will be “controllers” in relation to subsequent processing of personal data under the power in section 45 of the Data Act and will need to comply with the relevant requirements under the data protection legislation (guidance for controllers has been issued by the ICO).[1] This includes complying with the data protection principles in Article 5 of the UK GDPR (see 3.2.2 of this Code).

33. Prior to sharing any personal data under section 45 of the Data Act with a DVS, public authorities must identify a lawful basis for processing personal data in Article 6(1) UK GDPR. The lawful basis relied upon must be documented. The ICO has issued guidance on lawful bases.[2]

34. If public authorities share special category data (see Article 9 of the UK GDPR) with registered DVS, they must have both a lawful basis under Article 6(1) of the UK GDPR and must meet one of the conditions under Article 9 of the UK GDPR and (where relevant) Schedule 1 to the DPA. The ICO has issued guidance on special category data.[3]

35. In addition, personal data relating to criminal convictions and offences or related security measures is given additional protection under Article 10 of the UK GDPR, section 11 of, and Schedule 1 to, the DPA. Public authorities must adhere to additional conditions if processing this data. The ICO has issued guidance on criminal offence data.[4]

36. As per section 164A of the DPA, a data controller must have a process for complaints. This involves the data controller acknowledging the complaint within 30 days, beginning on the date the complaint is received. The data controller must also take appropriate steps to respond to the complaint and inform the complainant of the outcome of the complaint without undue delay.

---

[1] ICO Guidance: a guide to controllers and processors

[2] ICO Guidance: a guide to lawful basis

[3] ICO Guidance: special category data

[4] ICO Guidance: criminal offence data

### 3.2.2 Data Protection Principles

37. Article 5 of the UK GDPR sets out 7 mandatory principles relating to processing of personal data:

    1. Lawfulness, fairness and transparency
    2. Purpose limitation
    3. Data minimisation
    4. Accuracy
    5. Storage limitation
    6. Integrity and confidentiality (security)
    7. Accountability

38. Public authorities can find information on these principles on the ICO's website,[5] and may seek advice from their data protection officer.

39. Data controllers have overall responsibility for compliance with these principles and are required to have appropriate measures and records in place to demonstrate compliance. This includes contracts between controllers and processors, appropriate documentation and, where appropriate, codes of conduct. If the information sharing is likely to pose high risks to individuals, then a data protection impact assessment is required (see 4.1.4 of this Code).

## 3.3 Human Rights Act 1998

40. Public authorities must ensure that information sharing is compliant with the Human Rights Act 1998. Article 8 of the European Convention on Human Rights, which gives everyone the right to respect for their private life, family life, home and correspondence, is especially relevant when sharing personal information. Any interference with this right must be lawful, necessary and proportionate to certain specified aims.

## 3.4 Equality Act 2010 and Gender Recognition Act 2004

41. Information sharing under section 45 must be compliant with the Equality Act 2010 and the Gender Recognition Act 2004.

---

[5] ICO Guidance: a guide to data protection principles

# 4. Process for using the information sharing power

42. The following section of the Code highlights key considerations and best practices public authorities should consider at key stages of implementing and using the information sharing power under section 45 of the Data Act.

## 4.1 Step 1: Preparing to share information

### 4.1.1 What is the DVS Register

43. The DVS register is established and maintained by the Secretary of State under section 32 of the Data Act. It is a publicly available list of persons who hold a valid certificate from an accredited conformity assessment body certifying that the DVS they provide are provided in accordance with a relevant version of the DVS trust framework (published pursuant to section 28 of the Data Act) ("**trust framework**"), and who have been registered by the Secretary of State.

44. The trust framework is a set of rules which aims to ensure that digital identity products are safe, secure and reliable. It is technology-agnostic, meaning that it does not mandate the use of specific technical architecture for a DVS. The trust framework covers areas such as privacy, data protection, fraud management, cyber security, and inclusion. Under section 28 of the Data Act, the Secretary of State has a duty to prepare and publish the trust framework and is given a power to revise and republish it. Section 31 imposes a duty on the Secretary of State to review it at least every 12 months.

45. Supplementary codes are additional rules prepared and published by the Secretary of State under section 29 of the Data Act that supplement the trust framework. These may provide further specific rules tailored to particular use cases, for example, the supplementary code for digital right to work checks. The DVS register also records 'supplementary notes' in register entries to indicate whether a DVS is registered as providing specific services in accordance with a supplementary code (see section 36 of the Data Act).

46. Section 45(1)(a) of the Data Act permits information to be shared only with registered DVS providers. Prior to sharing information with a DVS, public authorities must verify that the DVS is registered in the DVS register.

47. A DVS provider may register as an identity service provider, attribute service provider, holder service provider, component service provider or orchestration service provider, as defined in the trust framework. They may fulfil more than one of these roles. For example, an organisation can be both an attribute service provider and an identity service provider.

48. It is possible for a DVS provider to have some DVS registered on the DVS register, and other services that are not registered on the DVS register. Public authorities should only share information under section 45 with services that have been certified and are registered on the DVS register.

49. In accordance with section 45, public authorities must not share information with DVS providers who hold a certificate from an accredited conformity assessment body but are not registered on the DVS register.

### 4.1.2 How to check the DVS register

50. The DVS register is publicly available on GOV.UK. Public authorities must check a DVS is registered on the DVS register before entering into any data sharing or contractual agreements.

51. Public authorities must also check the DVS requesting the information is on the DVS register immediately before the information is shared. Public authorities need to consider the most appropriate way to check the DVS register at each relevant stage. This can include using the machine readable infrastructure of the DVS register. Technical guidance on this is provided by the Office for Digital Identities and Attributes ("**OfDIA**").

### 4.1.3 Considerations when preparing to share information

52. The UK GDPR requires public authorities to put in place appropriate technical and organisational measures to implement data protection measures effectively and safeguard individual rights. This is known as "data protection by design and default". This means data protection is integrated into processing activities and business practices, at the design then throughout the lifecycle of a system, service, product or process. The ICO has issued guidance on data protection by design and default.[6]

53. Data protection by design and default starts before any personal data is shared. When preparing to share data or starting to set up processes and guidance, public authorities should consider what the intended processing activity is and the risks that could be posed by this process. Public authorities should also consider what possible measures are available to ensure the data protection principles are implemented effectively and individuals' rights are safeguarded.

[6] ICO guidance: data protection by design and default

54. The following outlines key considerations for public authorities before setting up processes to share information with registered DVS. The following points draw on existing legal obligations and data sharing best practices. A public authority may choose to include some of this information in a Data Protection Impact Assessment ("**DPIA**") (see 4.1.4 of this Code).

55. **Assessing limitations to data sharing:** The purpose of this is to ensure information sharing is necessary, with the principles of lawfulness, fairness and transparency, accuracy and data minimisation in mind. This assessment should include some of the following:

    - what personal data the public authority holds that could appropriately be used for digital verification purposes;
    - whether the data the public authority holds accurately addresses the requests posed by registered DVS; and
    - whether the sharing of information meets the intended purpose of providing DVS.

56. **Technical considerations:** Before any information sharing, public authorities should assess the technical and security measures which need to be implemented to share information securely. This includes:
    1. whether the public authority has a secure mechanism for ensuring that they will only share information with services on the DVS register;
    2. whether the public authority has a sound process for checking that the registered DVS has received a request from the individual to provide DVS;
    3. whether that information is in a state that can be shared (i.e. has it been digitised, is it in a machine-readable format, has it been contextualised); and
    4. how that information is labelled.

    The ICO has issued guidance on data security.[7]

57. When considering whether to share information, the public authority must be satisfied the registered DVS provider has been authorised to make the request to deliver DVS to the particular individual.

[7] ICO guidance: guide to data security

58. To be sure that they are interacting with the right individual, registered DVS providers must follow the methodologies described in Good Practice Guides 44 and 45, or in the trust framework attributes guidance, depending on which is applicable to their service(s). These guides underpin the trust framework and describe how to carry out authentication, identity checking, and attribute binding respectively, assigning different quality levels depending on how rigorously checks are conducted.

59. Public authorities should engage with the DVS provider making the request on how it has implemented these methodologies to determine whether the appropriate level of authentication, identity checking, or attribute binding has taken place so they can be sure the request for their service(s) has in fact come from the individual before information is shared.

60. Where a DVS provider is based overseas, public authorities must ensure they comply with Chapter V of the UK GDPR regarding overseas transfers. The ICO has issued guidance on international transfers.[8]

### 4.1.4 Data Protection Impact Assessment (DPIA)

61. Before sharing any information with a registered DVS under section 45, the public authority must consider whether a DPIA is needed. A DPIA is a key part of accountability obligations under the UK GDPR.

62. A DPIA is always required where the processing is likely to result in a high risk to the rights and freedoms of individuals. It is also good practice to do a DPIA for all other information sharing activities involving personal data, even if it is not legally required. This is to ensure that appropriate technical and organisational measures are in place to implement the data protection principles effectively and safeguard individual rights. Public authorities should also document how they considered whether a DPIA was needed and the reasons it was or was not needed. The ICO has issued guidance on DPIAs.[9]

63. The completion of a DPIA will help to identify potential risks in relation to the implementation of any new data-sharing schemes involving personal data and aid the adoption of a data protection by a design and default approach. A DPIA may cover a single processing operation or a group of similar processing operations and should be reviewed regularly. As referenced above, a DPIA can be a useful

---

[8] ICO guidance: guide to international transfers

[9] ICO Guidance: data protection impact assessments

place to record other factors considered as part of a decision to disclose information under section 45.

### 4.1.5 Data evaluation

64. Public authorities hold information in various formats. When planning to share information, it is strongly recommended that public authorities should consider whether the format of the data follows all the relevant standards and consider whether it would be best released via an API, as a credential, or via other means. These standards have been set out in the open standards for government data and technology[10] and the API standards.[11]

## 4.2 Step 2: Deciding what to share and why

### 4.2.1 Digital verification purposes

65. A registered DVS provider may request access to information about an individual under section 45 where they need that information to deliver DVS to the individual at their request.

66. Public authorities receiving such requests are encouraged to share information with the registered DVS if possible. Requests under Section 45 should not be refused unless there is a reasonable justification for doing so, in line with public law principles.

67. If considering refusal, it is recommended a public authority seeks legal advice before making a decision. If a public authority decides to refuse a request, it should provide an explanation for this decision.

68. Furthermore, when considering information sharing, public authorities should consider that the DVS provider can be asked to meet the costs, including upfront costs or the costs of necessary technical expertise. Cost or lack of resources should therefore generally not be an obstacle to sharing information under section 45.

69. If relevant, public authorities can explore this, and any other requirements for information sharing, as part of discussions about establishing the data sharing agreement (see 4.2.4) that should be in place before sharing any information. If a public authority uses the information sharing power under the Data Act, the public authority should make relevant information available for all registered DVS.

---

[10] Open standards for government data and technology – found on GOV.UK

[11] API technical and data standards – found on GOV.UK

Public authorities must not exclude any one registered DVS provider unless there are specific commercial or legal grounds to do so. For example, if a public authority creates an API to enable information sharing with registered DVS and charges a fee for access, the public authority should allow all other registered DVS equal access to the API (for the same fees), unless there are legal reasons not to.

70. Public authorities must have regard to the ICO Data Sharing Code, which sets out guidance for organisations on how to comply with data protection legislation when sharing personal data. This guide is extensive and public authorities should consider it carefully when preparing to share information with a DVS under section 45.

### 4.2.2 Data minimisation

71. Public authorities disclosing personal data must design and structure information sharing processes to avoid disclosing more information than is strictly required. This is referred to in the data protection legislation as the "data minimisation" principle. The ICO has set out guidance on the data minimisation principle.[12]

72. Public authorities must ensure data shared with registered DVS is adequate, relevant, and limited to what is necessary for the purpose for which it is being disclosed.

73. For example:

    1. this could mean only permitting a yes/no check against a specific data point such as date of birth to prove age.

    2. whether a DVS needs an entire credential for the service it is providing (e.g. an attribute service provider might have different requirements to a holder service provider)

74. Public authorities could use data sharing agreements to define how information requests should be structured by DVS. This will help ensure that the data disclosed is limited to what is necessary in the circumstances.

### 4.2.3 Data accuracy

75. Public authorities must ensure the data they hold is accurate, where necessary kept up to date, and not misleading. This is known as the data "accuracy"

[12] ICO Guidance: data minimisation principle

principle (see 3.2.2 of this Code). The ICO has published guidance on the data accuracy principle.[13]

76. When deciding to share information public authorities must consider, in accordance with this principle, how the information was collected, for what purposes, how it has been recorded and what that information represents. Having considered that, when the information is shared with the DVS, data should then be labelled in a way that is clear and accurate, taking into account the purpose for which it is being requested.

77. For example, this means that if a DVS provider requests data to verify a person's legal sex, the public authority must only share data that includes this attribute, rather than data which may include other attributes as well, such as gender. By way of further example, if a DVS provider requested data to verify sex at birth (where this was considered necessary and proportionate for the use case), public authorities must not share data that records legal sex or gender more broadly.

78. Public authorities may wish to refer to the standards, guidance and data schema included in the trust framework.

### 4.2.4 Data sharing agreements

79. A data sharing agreement is not mandatory under the data protection legislation but is good practice and beneficial to all parties involved in sharing.

80. A data sharing agreement allows the public authority and the registered DVS provider to agree a set of common rules that help both parties meet the requirements of the data protection legislation. Public authorities and registered DVS providers can use data sharing agreements to ensure clarity about each party's role in the data sharing process, addressing matters such as the purposes of the data sharing, outlining what happens to the data at each stage of sharing, (including when the agreement ends) and setting standards for the sharing taking place.

81. A particular benefit of data sharing agreements is supporting activity at scale. Some DVS providers may make large numbers of very similar requests, for example if providing a service to many people who use it frequently. A data sharing agreement can establish the framework under which requests will be made and authorised, and the technical means for implementing this; avoiding the public authority having to take large numbers of bespoke decisions where this is not necessary.

---

[13] ICO Guidance: data accuracy principle

82. Public authorities should follow the ICO Data Sharing Code when setting up data sharing agreements with DVS providers. Public authorities should speak to their data protection officers or senior responsible individuals about preparing a template data sharing agreement they may use for this purpose. On their own, a memorandum of understanding (except between government departments and certain other public bodies), a list of standards, or an addendum to a purchase agreement or order do not constitute freestanding data sharing agreements. However, they may include data sharing provisions and fulfil the role of a data sharing agreement such that a separate agreement is not needed.

83. This Code recommends any data sharing agreement includes:

    i. What data is being shared, for what purpose, and why it is necessary for that purpose.

    ii. Any restrictions on further use and onward sharing of data, and the terms for onward sharing of data with third parties, including relying parties (see 4.2.5 of this Code).

    iii. The security requirements and technical method for data transfer, processing and storage. If data sharing at scale is anticipated, the agreement should also include the information to be exchanged programmatically to enable this.

    iv. What the lawful basis for data sharing is to meet the requirements for processing, and additionally, where special category data and/or criminal offence data is shared, the relevant conditions for processing that data.

    v. What governance arrangements are in place; including the process for retaining and deleting shared data items.

    vi. How the individual's request underpinning the data sharing will be recorded by the DVS and demonstrated to the authority.

    vii. Procedures for compliance with information rights.

    viii. Terms for dealing with termination of the data sharing arrangement, including what will happen to any shared data that has been stored by the DVS, and what would happen if the DVS is removed from the DVS register.

    ix. Processes for handling potential data breaches.

84. Public authorities should review data sharing agreements regularly and ensure they are kept up to date.

### 4.2.5 Sharing information with third parties

85. The ultimate outcome of the information sharing power under section 45 of the Data Act is that an individual is able to use a registered DVS to access a product or service that requires an identity or eligibility check. For example, opening a bank account or purchasing an age-restricted product.

86. On that basis, registered DVS need to be able to share the relevant information they receive from public authorities with third party organisations that offer these services. In some cases, the third party will be a separate organisation. In others, the registered DVS provider may be the same organisation, and therefore no onward transfer is necessary.

## 4.3 Step 3: Sharing the information

### 4.3.1 Technical solution

87. The data protection legislation prescribes data protection by design and default, which requires appropriate technical, organisational and security measures to be put in place to be able to implement data protection principles effectively.

88. Public authorities must ensure that an appropriate robust and secure technological solution is in place to share the information under section 45 of the Data Act. This technical solution should be compliant with best practices for sharing information, including but not limited to, what has been set out in this Code.

89. Public authorities must also ensure that sufficient resourcing and technical capability exists within their organisation to manage, maintain and improve such a technical solution. This could include charging a fee for DVS to cover the cost of implementation, enhancement and maintenance of these systems (see 2.2. of this Code).

90. Public authorities should have processes in place to ensure the processes and agreements set out in Steps 1 and 2 of this Code are kept under review.

### 4.3.2 Privacy information

91. When exercising the information sharing power in section 45 of the Data Act, public authorities must ensure that appropriate privacy information is made available to the public in line with the fairness and transparency principles under

the data protection legislation. This could include a privacy notice. The ICO has issued guidance on what privacy information should be provided.[14]

92. When a public authority chooses to exercise the information sharing power in section 45 of the Data Act, the public authority's privacy notice must be updated to reflect this, including the circumstances when personal data may be shared.

[14] ICO Guidance: the right to be informed

E03606945

978-1-5286-6495-0