**What is a Data Sharing Agreement (DSA)?**

* The Data Sharing Agreement (DSA) is a non-legally binding Agreement between two (or more) Data Controllers, where personal data is shared (given) from one Data Controller to another, for them to use for their own purposes.
* The DSA should not be confused with a *contractual agreement* which is required when a data controller uses a data processor to process personal information on its behalf. Unlike a contract, the DSA neither addresses nor prejudices the legal ability and indemnity of the parties to the agreement[[1]](#footnote-1).
* If you are acting as a joint controller, there is a legal obligation to set out your responsibilities in a joint control arrangement, under both the UK GDPR / Part 2 of the Data Protection Act 2018 and under Part 3 of the Data Protection Act 2018.
	+ The DSA defines the parameters under which the recipients agree to use the personal information that has been shared by the data owner. It defines roles and procedures for dealing with security incidents, and for the exercise of data subject rights.
* For joint controllers, Article 26 of the UK GDPR and Section 58 of the Data Protection Act 2018 for part 3 processing require you to state in the agreement which controller is the contact point for data subjects.
* It is intended that the shared data will be provided to the recipient organisation in accordance with the [ICO’s Data Sharing Code of Practice](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/about-this-code/), the data protection legislation. The DSA covers the need for routine or recurring transfers of information (including access) where personal data is included in the transfer/access. It will not be appropriate for all one-off transfers of personal data.
* The DSA should be administered by the originating Data Controller (‘data owner’) who will monitor compliance with the DSA and review the agreement periodically.

**DSA Data Sharing Principles**

**The principles underpinning this Data Sharing Agreement are that:**

1. Data shall be processed in accordance with the principles under Article 5 of the UK GDPR, underlying the lawful processing of personal data.
2. The shared data shall only be used for the purposes agreed as defined within the DSA and shall not be used for any other purpose unless required by another law.
3. The shared data will be provided to the recipient organisation in accordance with the [ICO’s Data Sharing Code of Practice](https://ico.org.uk/media/for-organisations/data-sharing-a-code-of-practice-1-0.pdf) and the UK GDPR and as detailed within this agreement. The shared data will be processed in accordance with the UK GDPR and the DPA.
4. The shared data will be supplied to the recipient organisation in a secure manner for example by encrypted email attachment. Details to be included within the DSA.

**Data Sharing Agreement**

The representatives signing this agreement accept that the procedures laid down in this document provide a secure framework for the sharing of information between their organisations in a manner that is compliant with their statutory and professional responsibilities.

As such they undertake to:

* Implement and adhere to the procedures and structures set out in this agreement
* Ensure that where these procedures are complied with, then no restriction will be placed on the sharing of information other than those specified within this agreement
* Treat this document as “live” and subject to regular review and update in the first two years of the agreement due to the nature and complexity of the information flows between each organisation
* Engage in a review of this agreement with partners at least annually

**We, the undersigned, agree as representatives of the organisations below that we will adopt and adhere to this data sharing agreement.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Organisation** | **Name of representative** | **Position** | **Signature** | **Date** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## **1. Introduction and Overview**

[Enter the details of a general introduction and overview here]

## **2. Parties to the Data Sharing Agreement**

2.1 This agreement is between the identified departments of the below organisations

|  |  |
| --- | --- |
| Organisation name |  |
| Organisation address |  |
| ICO registration number |  |
| DPO name |  |
| DPO contact details |  |

|  |  |
| --- | --- |
| Organisation name |  |
| Organisation address |  |
| ICO registration number |  |
| DPO/DP Lead name |  |
| DPO/DP lead contact details |  |

|  |  |
| --- | --- |
| Organisation name |  |
| Organisation address |  |
| ICO registration number |  |
| DPO/DP Lead name |  |
| DPO/DP lead contact details |  |

2.2 All parties to the agreement must agree to the inclusion of any new party.

2.3 If a new organisation joins the agreement, a party wishes to include another department in the data sharing, or a party leaves the agreement, [enter name of data owner] will issue an updated version of the data sharing agreement as soon as possible, certainly within one month, and circulate it to all participating organisations to re-sign.

2.4 [Delete if not applicable]This data sharing agreement is made under [name of over-arching agreement or sharing charter, eg Tier 1 agreement between…]

## **3. Purpose**

3.1 The purpose of this agreement is to enable information to be shared between the named organisations in support of the following objectives:[………………………………]

3.2 [What are the benefits of sharing this information?]

3.3 [What are the limits? What is not covered? Are there any agreements in related areas that will operate in parallel?]

## **4. Basis for Sharing**

4.1 In writing this agreement due attention has been paid to the views of partners where possible, and has been written taking into account relevant legislation and guidelines where applicable including:

* The UK General Data Protection Regulation and the UK Data Protection Act 2018
* Human Rights Act 1998
* Equality Act 2010
* Freedom of Information Act 2000
* [Add relevant legislation where necessary]

4.2 We are relying on the following Article 6(1) basis for sharing personal data: (tick all that apply)

1. **Consent -** the data subject has given consent to the processing of his or her personal data for one or more specific purposes; [ ]
2. **Contract -** processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; [ ]
3. **Legal obligation (*state relevant law)* -** processing is necessary for compliance with a legal obligation to which the controller is subject; [ ]
4. **Vital interest -** processing is necessary in order to protect the vital interests of the data subject or of another natural person; [ ]
5. **Public Task** - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; [ ]
6. processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. [ ]

4.2.1 [Delete if not applicable] Condition (c) / (e) is lawful based on our statutory requirements under [state all relevant legislation]

4.2.2 [Delete if not applicable] Our legitimate interests, in accordance with condition (f) are […]. Failure to share would result in […].

4.3 We are relying on the following Article 9 basis for sharing of special category data: (tick all that apply)

1. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; [ ]
2. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; [ ]
3. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; [ ]
4. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects; [ ]
5. processing relates to personal data which are manifestly made public by the data subject; [ ]
6. processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity; [ ]
7. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; [ ]
8. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3; [ ]
9. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; [ ]
10. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with [Article 89](https://gdpr-info.eu/art-89-gdpr/)(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject [ ]
11. No special category data [ ]

4.3.1 [Delete if not applicable]Conditions (b), (h), (i) and (j) are only lawful if we can also meet at least one condition within [Schedule 1](http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted), Part 1 of the Data Protection Act 2018. [state how the sharing meets these condition(s)]

4.3.2 [Delete if not applicable]Condition (g) is only lawful is we can also meet at least one of the conditions within [Schedule 1](http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted), Part 2 of the Data Protection Act 2018. [state how the sharing meets these condition(s)]

4.4 We are relying on the following Article 10 basis for sharing of information relating to criminal convictions or offences: (tick all that apply)

1. No information relating to criminal convictions of offences [ ]
2. We have [official authority](http://www.legislation.gov.uk/ukpga/2018/12/schedule/7/enacted) or statutory functions for law enforcement purposes [ ]
3. The activity meets the following conditions(s) within [Schedule 1](http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted), Parts 1,2 or 3 of the Data Protection Act 2018 [ ]

[state how the sharing meets these conditions]

4.5 This agreement sets out the responsibilities for each party to ensure all processing of shared data is accurate, necessary, legal and ethical.

## **5. Information to be Shared**

5.1 [How did you determine what information would be shared?]

5.2 Summary of information supplied by [ORGANISATION] to [THIRD PARTY]

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Type of Information** | **How it will be shared** | **Frequency of sharing** |
| A1 |  |  |  |
| A2 |  |  |  |
| A3 |  |  |  |

5.3 Summary of information supplied by [THIRD PARTY] to [ORGANISATION]

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Type of Information** | **How it will be shared** | **Frequency of sharing** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

5.4 Other data sharing

Future requirements to share information not captured in 5.2 and 5.3 above will be added to the table here and this data sharing agreement will be adopted as a new version.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Type of Information** | **How it will be shared** | **Frequency of sharing** |
| C1 |  |  |  |
| C2 |  |  |  |
| C3 |  |  |  |

5.5 If there is a need to share information on a “one off” basis, the parties should consider whether the sharing is necessary for the purpose set out in the agreement and document their decisions.

5.6 If additional information is required on a repeated basis, over and above what is defined in the agreement, to enable the agreement to achieve its aims, the parties should agree an addition to the sharing agreement, ensuring that the new information sharing has a legal basis. This addition should be added to the agreement and all parties should re-sign.

5.7 A variety of information will continue to be shared for other purposes, covered by existing legislation and guidance.

5.8 The terms of this agreement will apply to such additional information sharing, except to the extent that they conflict with any statutory or otherwise existing arrangements.

## **6. Methods of Data Exchange and Storage**

The information will be shared through a variety of means, including:

* [for example System-to-system electronic file transfer through a secure interface
* Manual file exchange through a secure portal accessible to both parties
* Common access through a single back office system
* Secure e-mail
* Telephone conversations]

6.1 Information should only be shared securely and between identified individuals or job roles.

6.2 Acceptable exchange mechanisms for electronic information are:

* [Option one]
* [Option two]
* […]

6.3 Acceptable exchange mechanisms for hard copy information are:

* [Option one]
* [Option two]
* […]

6.4 The below exchange mechanisms should not be used to transfer information:

* [Option one]
* [Option two]
* […]

6.5 Information that is shared should be clearly marked with the name of the originator.

6.6 Shared information should be stored securely by the receiving organisation.

## **7. How the Information will be Used**

7.1 The parties undertake that information shared under this agreement will only be used for the specific purpose for which it was shared, in line with this agreement.

7.2 The information will be used only for the purposes of delivering and monitoring the services specified in the contract between [ORGANISATION] and [ENTER ALL PARTIES]

7.3 Information shared under this agreement must not be shared for any other purpose than those detailed, or with a third party that is not a party to this agreement.

## **8. Information Management**

8.1 In each case, the originating organisation remains the information owner for the information that is shared. Where information is edited by the recipient party, the recipient party must clearly identify the altered copy.

8.2 The information that has been shared should be retained for [DEFINE ALL RETENTION PERIODS]

8.3 Hardcopy records that are eligible for destruction should be destroyed in accordance with the Data Controller’s policies.

8.4 Electronic records that are eligible for destruction should be destroyed in accordance with national standards.

8.5 If a party leaves the agreement, the information that has been shared will be returned in a useable format, and as per the terms of the contract.

8.6 All parties are responsible for the quality of the information that they are sharing.

8.7 Before sharing information, parties will check that the information being shared is accurate and up to date to the best of their knowledge.

8.8 Any inaccuracies identified in the data must be relayed to all parties in this agreement as soon as possible, and no later than within five working days.

8.9 It is incumbent on all parties that all the information being shared will be protected from inappropriate and unlawful access.

8.10 Parties will ensure that all staff, including temporary and agency staff, are aware of conditions and responsibilities about appropriate sharing and use of data arising from this agreement.

## **9. Specific Points of Contact**

9.1 Each organisation will identify a Specific Point of Contact (SPOC) who will assume ownership of the information sharing interfaces between the organisations.

9.2 The SPOC will be the first port of call for questions about the agreement within their organisation. SPOCs must be contacted if there is a problem, such as an information security breach.

9.3 Access to the shared information should only be given to those organisations and departments that are parties to the agreement.

## **10. Rights of Data Subjects**

10.1 Each party is responsible for responding to data subject access requests (DSARs), and requests submitted under the Freedom of Information Act (if applicable) and Environmental Information Regulations made to their organisation.

10.2 Any complaints made by data subjects will be dealt with by the receiving party, advising the other parties where necessary.

10.2 Where necessary, the parties will assist each other in fulfilling the obligations set out in the relevant legislation.

10.3 Parties will ensure that service users are advised of any purpose for which data will be shared under this agreement, by issuing them with a fair processing notice.

## **11. Information security breach procedures**

9.1 Each organisation confirm they have established Incident Reporting and Management procedures, consistent with the Information Commissioner’s guidance for investigating and handling security breaches.

9.2 In the event of a data security breach, the identifying party will notify all organisations in this agreement as soon as possible, and within 24 hours.

9.3 The data controller responsible for the breach shall assume responsibility for the subsequent handling

9.3 Access to the shared information should only be given to those organisations and departments that are parties to the agreement.

## **12. Indemnity**

No party accepts liability should another party incur a loss as a result of data which it has supplied to that party under this agreement being processed by that other party, or by any person to whom that other party has passed the data.

## **13. Termination and Review of Agreement**

13.1 The terms of the agreement will be reviewed three months after its launch and annually thereafter, or as a result of a formal contract change control document being issued, or following a significant change that could impact the agreement (such as a legislative change).

13.2 The party responsible for initiating review of the agreement is [INSERT PARTY NAME].

13.3 Any party can suspend the agreement for 30 days if they have evidence that that security has been seriously breached.

13.4 This agreement may be terminated by any of the parties giving written notice of at least four weeks.

1. If you are a data controller who is using a data processor to process personal data on your behalf, you are legally required to have a contract containing minimum terms under the UK General Data Protection Regulation (UK GDPR). Contact One West for advice. [↑](#footnote-ref-1)