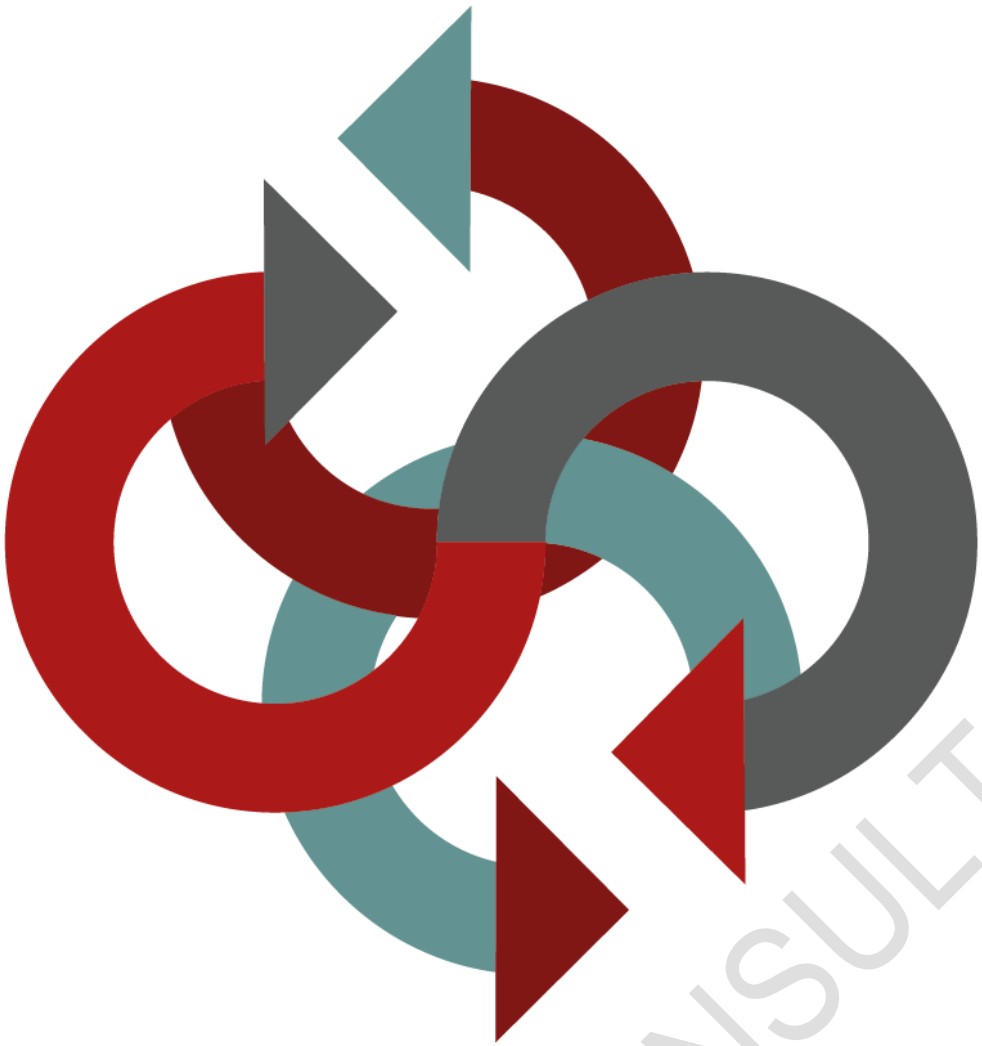

Cefnogir gan
Lywodraeth Cymru
Supported by
Welsh Government

DRAFT CONSULTATION

Wales Accord on the Sharing of Personal Information

Guide on the development of Data Disclosure Agreements

Version 6

Contents

Section 1 – The Development Process **2**

Introduction 2

Considerations before developing a DDA 2

Preparing to develop a DDA 4

DDA development 4

Section 2 - Populating the DDA template **5**

Introduction 5

Title page 5

Section 1 - Introduction to this DDA 5

Section 2 - Purpose of the disclosure 5

Section 3 - Partners to this agreement 6

Section 4 - Lawful basis 6

Section 5 - Data disclosed 6

Section 6 - Information security 7

Section 7 - Detail of disclosure 7

Section 8 - Data Subjects' Rights 7

Section 9 – Review, Breaches and Termination of this Agreement 7

Section 10 - Agreement Signature 8

Appendix A – Glossary of Terms 8

DRAFT CONSULTATION

Section 1 – The Development Process

Introduction

1.1 This guidance has been prepared to support the development of **Data Disclosure Agreements (DDAs)** under the national framework provided by the Wales Accord on the Sharing Personal of Information (WASPI). This document specifically relates to the DDA template available on the WASPI website – www.waspi.gov.wales

1.2 The principles set out in the Accord are put into practice through a collaborative approach to the development of agreements using WASPI templates. Separate guidance is available on the other types of WASPI agreements.

1.3 DDAs should not be used in place of Information Sharing Protocols (ISPs). They are for separate purposes. A flow diagram has been created to help organisations understand what type of agreement is required. The flow diagram is available on the WASPI website. Additional advice should be sought from your Information Governance team / Data Protection Officer.

1.4 ISPs are designed to support reciprocal sharing between data controllers, whereas DDAs are designed to support one-way disclosures between data controllers; i.e. where there is no reciprocal sharing. Both are designed to support regular events, rather than one off instances of sharing or disclosure. It is envisaged that DDAs will usually involve two partner organisations, although there may be instances when multiple partner organisations are involved.

1.5 **DDAs do not replace the requirement for a contract between the controllers and processors.** Queries regarding the appropriate type of agreement or contract should be referred to your Information Governance team or Data Protection Officer and a template Data Processing Agreement is available on the WASPI website.

1.6 Partner organisations can be included in several DDAs but each DDA has a specific context and defined purpose. DDAs are not a substitute for a culture of collaboration and consultation, which is a crucial part of effective public service delivery. As such, DDAs should be prepared with the input of all partners and should not be drafted in isolation.

1.7 If any changes to the standard text of this agreement, organisations will be required to ensure that the WASPI logo is removed.

Considerations before developing a DDA

1.8 Before starting the development of a DDA you should be able to answer yes to the following:

Question / consideration	Further guidance / notes
Have you consulted with your Data Protection Officer, Information Governance lead or equivalent regarding the need for a DDA?	**Prior to starting the development of a DDA, you must take advice from a suitably qualified and/or experienced person.**
Prior to sharing Personal Data, have you considered the need for and, where required,	Information Commission's guidance on DPIAs and Article 35 of the UK GDPR.

DRAFT CONSULTATION

completed a Data Protection Impact Assessment?	The ICO's Data Sharing Code of Practice recommends undertaking a DPIA, even where it may not be mandatory. This should be discussed with your Information Governance team or Data Protection Officer.
Does the data being disclosed identify individuals?	If data to be disclosed does not identify individuals, a DDA is not required.
Is the personal information disclosed one way for a specific purpose?	DDAs are intended for use when personal data is to be **disclosed** (i.e. passed one way) from one Data Controller to another for a specific purpose. Whereas, ISPs should be developed to document practices involving **the regular, reciprocal sharing** (i.e. information flows back and forth between organisations) of personal information between Data Controllers. Separate guidance and templates are available on the WASPI website to assist with the ISP development process. The most appropriate template to use to capture your information sharing should be discussed with your Information Governance department or Data Protection Officer.
Are partners to the DDA data controllers or are any data processors involved?	Data processing activities must be underpinned by a UK Data Protection Law compliant contract. A Data Processing Agreement template is available on the WASPI website.

1.9 Data Protection Impact Assessments (DPIA are a legal requirement in certain circumstances and should be undertaken before sharing takes place. A DPIA allows key risks and mitigations (including the need for a DDA) to be identified.

1.10 Take advice if you are unsure whether a DDA is required; this could be from your Data Protection Officer or other suitably qualified person within your organisation. The central WASPI team can provide general advice.

1.11 DDAs are intended for use when Personal Data is to be **disclosed** (i.e passed one way) from one Data Controller to another for a specific purpose. DDAs are not intended for use in instances where the disclosure is from a Data Controller to a Data Processor and do not replace the requirement for appropriate contracts. Whereas, ISPs should be developed to document practices involving **the regular, reciprocal sharing** (i.e information flows back and forth between organisations) of personal information between Data Controllers. Separate guidance and templates are available on the WASPI website to assist with information sharing agreement development processes.

DRAFT CONSULTATION

1.12 Once it has been determined that a DDA is required, consideration should be given to the identification of the relevant contacts within the partner organisations. It is important that you develop the DDA collaboratively with representatives from all the partner organisations.

Preparing to develop a DDA

1.13 All partners should abide by the principles set out in the Accord. This demonstrates a commitment to a consistent approach to sharing personal information. Signing the Accord is not a pre-requisite to developing a DDA but is strongly recommended. The 'Declaration of Acceptance and Participation' is available on the WASPI website.

1.14 Relevant contacts at partner organisations should be established and the need for a DDA agreed. Roles and responsibilities during the DDA development process should be agreed at an early stage; e.g who will lead in the DDA development, will representatives of partners meet to discuss the DDA, will there be a mixture of physical meetings and virtual meetings or will the DDA be developed by one organisation and feedback provided by email.

DDA development

1.15 Representatives of the partner organisations should agree the purpose and objectives of the DDA. Representatives should also confirm whether their organisation has signed the Accord. A list of participating organisations is available on the WASPI website.

1.16 The agreed latest version of the DDA template is available on the WASPI website.

1.17 When the final draft of the DDA has been agreed, each representative should refer it to their respective Information Governance Manager / Data Protection Officer (or equivalent) for comment and agreement.

1.18 DDAs do not need to pass through the WASPI Quality Assurance Process. The check from Information Governance specialists from all organisations involved should be sufficient to ensure robust DDAs are developed.

1.19 Partner organisations should exchange signed copies of the final agreed document.

DRAFT CONSULTATION

Section 2 - Populating the DDA template

Introduction

1.20 This section deals with the population of the DDA template, providing guidance on completion of specific sections.

1.21 The aim of the DDAs is to identify and document:

- the scope and particular purpose(s) for the disclosure of personal information;
- the partner organisations involved;
- the lawful basis;
- the information to be shared; and
- the source, method, destination, frequency and retention period of the transfer.

1.22 Approved DDAs will not be published on the WASPI website. They are intended to be more straightforward agreements that do not require the same formal quality assurance process as ISPs.

1.23 The WASPI DDA template has been pre-populated with standard text and clearly indicates where additional information is to be inserted.

Title page

1.24 Provide the DDA title in the first 'insert details here' box. It should reflect the function of the service / initiative / project / programme.

1.25 The author should maintain version control as the DDA is developed.

Section 1 - Introduction to this DDA

1.26 This section has been pre-populated with standard text. The following details need to be added to expand on the scope and purpose of the specific DDA.

1.27 At paragraph **1.1,** state the name of the particular service / initiative / project / programme to which the DDA specifically relates – for example: The Flying Start Programme – and what it seeks to achieve. Try to be concise; the purpose of the disclosure is to be set out in detail in section 2.

1.28 Any existing information sharing documents, forms or guidance, including local policies and procedures currently used by partner organisations, should be referenced in the DDA.

Section 2 - Purpose of the disclosure

1.29 At paragraph **2.1** explain the specific purpose of the disclosure, what it seeks to achieve and why it is necessary. These explanations should be written in such a way as to allow someone with no knowledge of the function or service to understand what it is about and why it is necessary to disclose the information. The purpose can be taken from your Data Protection Impact Assessment, if completed.

DRAFT CONSULTATION

Section 3 - Partners to this agreement

1.30 At paragraph **3.1** detail the names of the organisations involved in both the disclosure and receipt of the information.

1.31 It is recommended that each partner organisation appoint a Responsible Manager who has sufficient senior authority within their service area. They will have overall responsibility for ensuring the DDA is implemented, disseminated, understood and acted upon by relevant practitioners.

Section 4 - Lawful basis

1.32 Identifying an appropriate lawful basis for disclosing data is crucial. Without a clear basis, organisations cannot demonstrate that they meet the first principle of UK GDPR (Article 5); 'lawfulness, fairness and transparency'.

1.33 Because there is the potential for both the UK GDPR and the Data Protection Act 2018 (DPA 2018) to provide the relevant lawful basis for disclosing Personal Data, it is important that appropriate advice is sought prior to drafting a DDA. Organisations Data Protection Officer's (or equivalent) should be informed of any DDA development.

1.34 A lawful basis should be established prior to entering into any arrangements that involve the regular sharing of information. **This does not prevent personal information being shared in 'emergency situations' or override any existing safeguarding or other procedures and processes established to ensure individuals can be cared for, treated or otherwise protected.**

1.35 A 'How to use the tables' section has been included to aid understanding of this section. This should be read before attempting to fill out this section. If there remain queries on this section after reading this and this guidance, you should contact your Information Governance team / Data Protection Officer for advice.

1.36 In the first table, insert the lawful basis being relied upon for general processing. The lawful bases are available at Article 6, 9 and 10 of the UK GDPR and Chapter 2 of part 2 of the DPA 2018. In the case of sharing for law enforcement purposes, please complete table two adding in the relevant conditions. This table will only be relevant where the processing is by a competent authority processing for law enforcement purposes. Further details of the processing for law enforcement purposes are available part 3 of the DPA 2018. Guidance is available on the ICO website.

1.37 Organisations should ensure they can meet the requirements of any legal basis relied upon. Advice should be sought from your Information Governance team / Data Protection Officer on what is required for these legal basis to be met.

Section 5 - Data disclosed

1.38 Partner organisations must be able to explain why disclosure is necessary to achieve the stated purpose(s). Under the principle of 'data minimisation', only the minimum data necessary to achieve the stated purpose must be disclosed. This should be reviewed regularly to ensure the personal information being disclosed is still relevant and required.

1.39 At paragraph **5.1** set out the type of Personal Data that is disclosed. In most cases organisations should be able to list the specific types of information to be disclosed.

DRAFT CONSULTATION

Do not include actual Personal Data in this section or anywhere in the template.

1.40 It is good practice for partner organisations to check the quality of the information before it is shared to avoid inaccuracies spreading across the information systems of other organisations.

1.41 Where information is rectified after disclosure, the data controller must inform partner organisations of the change.

Section 6 - Information security

1.42 This section of the template DDA has been pre-populated with set text therefore, no further population is required. However, partners must ensure they comply with these requirements.

Section 7 - Detail of disclosure

1.43 In the table at Section 7, list:

- The computer system or manual filing structure that holds the information to be disclosed and the relevant directorate / department / team responsible for supplying it;
- The specific agreed methods of secure disclosure from the source to the destination. *E.g. Electronic methods of transfer, such as secure portals, encryption, non- electronic methods of transfer such as recorded delivery, hand delivery, and any forms/letters/paper documents used to transfer data;*
- The specific computer system or manual system that will hold the information at the destination organisation(s) and the responsible receiving directorate / department / team;
- How often the data will be disclosed. Tick boxes have been provided for assistance but please amend where necessary; and
- The retention period or the criteria used to define the retention period. This should be in line with organisational retention policies.

Section 8 - Data Subjects' Rights

1.44 This section of the template DDA has been pre-populated with set text therefore, no further population is required. However, partners must ensure they comply with these requirements.

Section 9 – Review, Breaches and Termination of this Agreement

1.45 DDAs should be reviewed as appropriate, and this period reflected in the agreement.

1.46 Some scenarios that trigger a review include:

- Significant changes to the scope of the service varying the volume or type of data being shared.

DRAFT CONSULTATION

- A significant (i.e reportable) data breach.
- A change to the lawful basis for sharing data.

1.47 The person responsible for reviewing the DDA should be agreed at the initial development stage.

1.48 Where an organisation has breached the terms of an agreement, it should be reported to the partner organisations involved. All organisations party to the agreement should be informed and discuss the implications and next steps. This may result in the organisation being omitted from the agreement or the information sharing set out in this agreement ceasing.

1.49 Where information sharing ends, the Partners involved in the agreement should agree the roles and responsibilities, including whether the information will be deleted or returned.

Section 10 - Agreement Signature

1.50 Once the DDA has been agreed by all partner organisations and reviewed by the relevant Information Governance lead / Data Protection Officer for each organisation, each partner organisation should arrange for a relevant individual to sign the agreed DDA. Accepting the agreement by signing it is a key element of demonstrating 'accountability' under UK GDPR.

1.51 It is for partners to determine how to manage the signatory process; i.e whether the hard copy of the DDA need physically signing or are electronic signatures are sufficient.

1.52 The signatory should be an individual person with authority to sign the DDA on behalf of the organisation and ensure its use if communicated throughout the organisation. Check with your Information Governance department or Data Protection Officer if you are unsure who should sign.

Appendix A – Glossary of Terms

1.53 A glossary defines common references. This can be added to if required but items should not usually be deleted.

DRAFT CONSULTATION