Cefnogir gan
Lywodraeth Cymru
Supported by
Welsh Government

Guide on the development of Data Processing Agreements

Wales Accord on the Sharing of Personal Information

Version 6

Contents

Section 1 – The Development Process **2**

Introduction 2

Considerations before developing a DPA 2

DPA development 3

Section 2 - Populating the DPA template **4**

Part 1 - Front Sheet 4

Date of agreement (Section I) 4

Controller(s) and Processor (Sections II and III) 4

Data Processing Activities (Section IV to IX) 5

Sub-processors (Section X) 5

Minimum aggregate limit of indemnity for insurance (Section XI) 6

Security details (Section XII) 6

Plan for return/destruction (Section XIII) 6

Locations for processing the personal data (Section XIV) 6

DRAFT CONSULTATION

Section 1 – The Development Process

Introduction

1.1 This guidance has been prepared to support the development of **Data Processing Agreements (DPAs)** under the national framework provided by the Wales Accord on the Sharing Personal of Information (WASPI). This document specifically relates to the DPA 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 **DPAs 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.

Considerations before developing a DPA

1.4 Before starting the development of a DPA 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 DPA?	**Prior to starting the development of a DPA, you must take advice from a suitably qualified and/or experienced person.**
Have you considered the need for and, where required, completed a Data Protection Impact Assessment?	The Information Commission's (ICO) guidance on DPIAs and Article 35 of the UK GDPR. This should be discussed with your Information Governance team or Data Protection Officer.
Does the data being disclosed directly or indirectly identify individuals?	If data to be disclosed does not identify individuals, a DPA is not required (but this should be discussed with and confirmed by your Information Governance team or Data Protection Officer). Note that data will only be considered not to directly or indirectly identify an individual where it is truly anonymised.
Is the Personal Data disclosed with a third party(ies) for the purposes of supporting the Data Controller with provision of a service?	Data Processing Agreements are intended for use where a Processor carries out processing of Personal Data *on behalf* of a Data Controller, Article 28(3) of the UK GDPR requires there to be a binding contract between the Data Controller and the Processor containing certain mandatory provisions. If, however, the data is being shared with a third party(ies) for that third party(ies)

DRAFT CONSULTATION

	own use (as a Data Controller in its own right or a Joint Controller), then this DPA is not appropriate and either a data sharing agreement or joint controller agreement will be required. This should be discussed with your Information Governance department or Data Protection Officer.

1.5 A Data Processing Agreement (DPA) is a legally binding contract signed between controllers and the processors that will handle their data and is intended to comply with the requirements of Article 28 of the UK GDPR.

1.6 A DPA sets out the nature, purpose and duration of the processing activities that will take place. It also specifies the types of personal data to be processed and the categories of individuals the data belongs to. It defines the rights and obligations the controller and processor will have.

1.7 Organisations who use the WASPI DPA template need to ensure that any completed DPA is legally binding from their own organisational requirements. WASPI provide a template agreement which can be used, but exclude all warranties and representations about the suitability of the document and exclude all liability in respect of the processing or contracts in place. The WASPI service will not provide any opinions on any proposed agreements, data protection advice should be sought from relevant organisation's Data Protection leads.

1.8 The template DPA was developed in partnership with Blake Morgan LLP. Whilst other organisations may use this data processing agreement template, neither WASPI nor Blake Morgan shall owe any duty of care to any other entities and all liability of WASPI and Blake Morgan LLP to all other entities is hereby excluded. Other entities are advised seek their own advice on the contents and use of this template.

DPA development

1.9 Representatives of the DPA organisations should agree the purpose and objectives of the DPA.

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

1.11 DPAs 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 DPAs are developed.

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

DRAFT CONSULTATION

Section 2 - Populating the DPA template

Part 1 - Front Sheet

1.13 This section deals with the population of the DPA template, covering the details of:

- the Data Controller(s) and their registration details where applicable
- the Processor and their registration details where applicable
- the subject matter of the processing
- the purpose, nature and duration of processing
- the outline of the personal data categories processed as part of the arrangements
- any agreed names Sub-processors to the arrangements
- the agreed minimum limit of insurance that the processor is required to hold pursuant to clause **Error! Reference source not found.**
- the security details in relation to the processing
- the plan for return and/or destruction of the Personal Data once the processing is complete (unless required by law to retain the Data)
- the location of the data
- signatures of each party.

1.14 The WASPI DPA has been designed so that all information specific to the arrangement contemplated by the DPA is to be included in the Front Sheet (and therefore avoids the need to insert details into the body of the DPA itself).

1.15 The WASPI DPA template has been pre-populated with standard text and clearly indicates where additional information is to be inserted. Text highlighted in yellow is provided for guidance and as examples and should be reviewed and amended on a case-by-case basis. Please note that the wording provided will not be appropriate for every DPA. **The format and standard wording can be changed to meet any specific additional requirements, however we would encourage prior consultation with your respective Information Governance team or Data Protection Officer.**

1.16 The Front Sheet and the Terms and Condition at Part 2 of the template, record the obligations of the Parties in respect of the specific processing activities.

Date of agreement (Section I)

1.17 This would be the date that the data processing between the Data Controller(s) and processor commenced (and is usually the date upon which the last party signed the DPA).

Controller(s) and Processor (Sections II and III)

1.18 Section II should set out the Data Controller(s). These would be the main decision-makers who exercise overall control over the purposes and means of the processing of personal data.

DRAFT CONSULTATION

1.19 Section III should set out the Processor. This would be the third party organisation who are acting on behalf of, and only on the instructions of, the relevant Data Controller.

Data Processing Activities (Section IV to IX)

1.20 Article 28 of the GDPR prescribes the provisions which must be included in a Data Processing Contract between a Data Controller and a Processor. Where a Data Controller and Processor enter into a Data Processing Agreement, it must, at a minimum, contain the following details:

The subject matter, duration, nature and purpose of the data processing;

The type of Personal Data being processed; and

The categories of Data Subjects whose personal data is being processed. The Front Sheet of the DPA should set out that information as follows:

- **Subject matter of the processing (Row IV)** - this should be a high level, short description of what the processing is about i.e. its subject matter of the contract.
- **Nature of the processing (Row V) –** this should set out what types of processing the Processor shall undertake of the Personal Data.
- **Purpose of the processing (Row VI) –** this should set out the purpose(s) for which the Processor shall process the Personal Data pursuant to the DPA. This is important as it limits the extent to which the Processor can process the Personal Data.
- **Duration of the processing (Row VII) –** this should clearly set out for how long the Processor shall process Personal Data. This is usually for the duration for which the purpose is undertaken, so long as the Processor needs to process the Personal Data for the purpose or for the duration of the DPA (or associated commercial agreement), but can be some other period.
- **Categories of Data Subject (Row VIII) –** this should set out the categories of Data Subject which the Personal Data the Processor is processing relates to.
- **Personal Data (Row IX) –** this should set out the type of Personal Data the Processor is to process under this DPA.

Sub-processors (Section X)

1.21 This should name any Sub-processors engaged by the Processor who would be subject to the same data protection obligations as the Processor.

1.22 Note that the Processor is only permitted to appoint Sub-processors with the Controller(s) prior written consent. Entering the Sub-processors into this table shall be deemed prior written consent. Controllers should undertake sufficient due diligence on proposed Sub-processors to ensure that they are satisfied that it is appropriate for such Sub-processors to be appointed (including that such Sub-processors have appropriate organisational and technological measures in place to protect the Personal Data and that the Processor has entered into a written contract with the Sub-processor).

DRAFT CONSULTATION

1.23 A template Data Sub-processing Agreement is available on the WASPI website.

Minimum aggregate limit of indemnity for insurance (Section XI)

1.24 Clause 14.2 requires the Processor to obtain insurance against liabilities arising under the DPA. Row XI sets out the minimum level of insurance that the Processor is required to obtain. The appropriate amount will depend on the exact circumstances of each DPA and should be considered on a case-by-case basis – such consideration should include consideration of the amount and nature of Personal Data to be processed by the Processor.

1.25 Additionally, the amount of insurance can be set either on an aggregate basis (that is, the amount to cover all claims made under the insurance) or on a "per claim" basis (that is, that each "claim" under the insurance shall have its own limit). Controllers should discuss this requirement with Information Governance team or Data Protection Officer.

Security details (Section XII)

1.26 Controllers need to be satisfied that processors have appropriate technological and organisational measures in place to protect the Personal Data. Controllers should ensure that they undertake some due diligence on the processor's measures in order to satisfy themselves.

1.27 Section XII of the Front Sheet requires the Data Controller(s) and Processor(s) to set out how the information being processed is carried out by appropriate secure means which means the Article 32 requirements under the UK GDPR. Where the Data Controller requires the Processor to have specific/certain security measures in place, these should be listed here.

Plan for return/destruction (Section XIII)

1.28 Section XIII should set out how long the processor will retain the Personal Data and how that personal data will then be returned or destroyed by the processor following the expiry of that period.

Locations for processing the personal data (Section XIV)

1.29 Section XIV should set out the locations at which the Processor (and its Sub-processors) will process the Personal Data pursuant to the DPA.

1.30 Where the Processor (or its Sub-processors) are to process (including storing or accessing the Personal Data) the Personal data from a country which is not an adequate country, then the controller will need to ensure that there are other appropriate safeguards in place in accordance with Chapter V of the UK GDPR and should record those safeguards in Section XIV.

DRAFT CONSULTATION