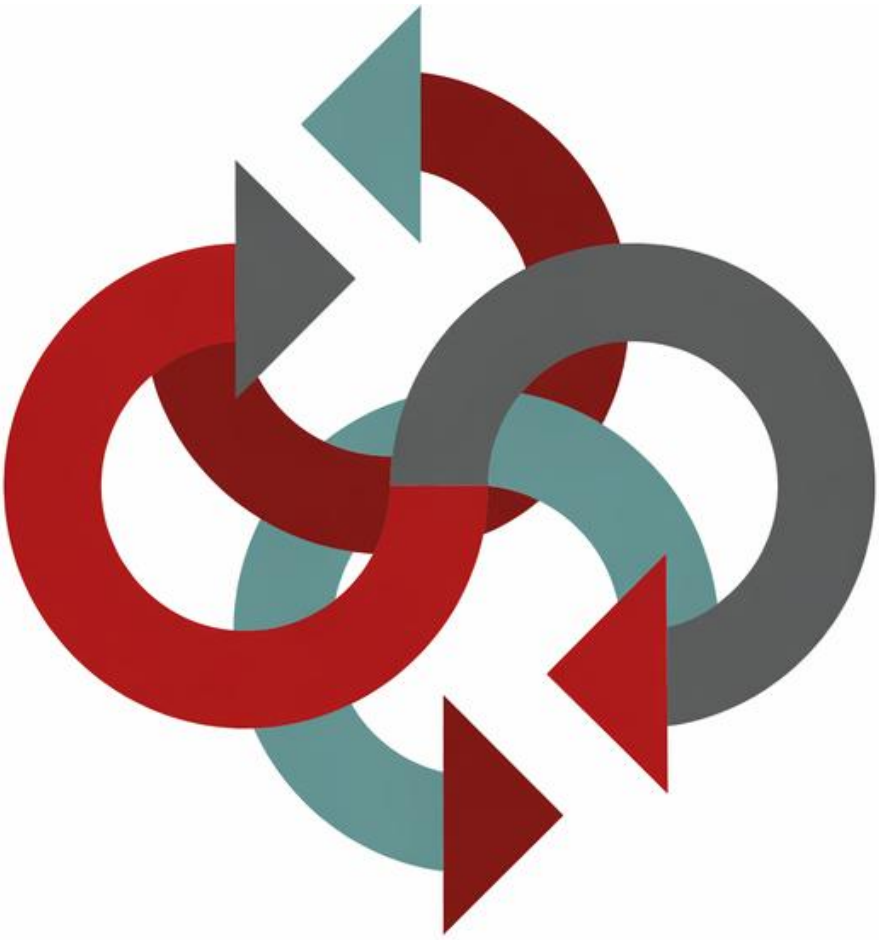

Cefnogir gan
Lywodraeth Cymru
Supported by
Welsh Government

Guide on the development of Data Sub-Processing Agreements

Wales Accord on the Sharing of Personal Information

DRA

Version 6

Contents

Section 1 – The Development Process **2**

Introduction 2

Considerations before developing a DSPA 2

DSPA development 3

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

Part 1 - Front Sheet 4

Date of agreement (Section I) 4

Principal Agreement (Section II) 4

Controller, Initial Processor and Sub-Processor (Sections III, IV and V) 5

Data Processing Activities (Section VI to XI) 5

Sub-contractors(Section XII) 6

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

Security details (Section XIV) 6

Plan for return/destruction (Section XV) 6

Locations for processing the personal data (Section XVI) 7

DRAFT CONSULTATION

Section 1 – The Development Process

Introduction

1.1 This guidance has been prepared to support the development of **Data Sub-Processing Agreements (DSPAs)** under the national framework provided by the Wales Accord on the Sharing Personal of Information (WASPI). This document specifically relates to the DSPA 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 **DSPAs do not replace the requirement for a contract between the Initial Processors and Sub-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 DSPA

1.4 Before starting the development of a DSPA 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 DSPA?	**Prior to starting the development of a DSPA, 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?	Information Commission's 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 DSPA 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.
Has the Initial Processor entered into a contract with the Controller for the providing of a service which involves the processing on personal data?	Data Sub-Processing Agreements are intended for use where a sub-processor carries out processing of personal data *on behalf* of an initial processor, where the initial processor has a contract with a Data Controller for the processing of Personal Data for the provision of a service.

DRAFT CONSULTATION

	Articles 28(3) and 28(4) of the UK GDPR requires there to be a binding contract between the initial processor and the sub-processor containing certain mandatory provisions.

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

1.6 A DSPA 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 Initial Processor and Sub-Processor will have.

1.7 Organisations who use the WASPI DSPA template need to ensure that any completed DSPA 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 DSPA was developed in partnership with Blake Morgan LLP. Whilst other organisations may use this data sub-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.

DSPA development

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

1.10 When the final draft of the DSPA 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 DSPAs 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 DSPAs are developed.

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

DRAFT CONSULTATION

Section 2 - Populating the DSPA template

Part 1 - Front Sheet

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

- the Data Controller(s) and their registration details where applicable
- the Initial Processor and their registration details where applicable
- the Sub-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-contractors to the arrangements (i.e. any Processors engaged by the sub-processor).
- the agreed minimum limit of insurance that the sub-processor is required to hold pursuant to clause **Error! Reference source not found.**
- 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 DSPA has been designed so that all information specific to the arrangement contemplated by the DSPA is to be included in the Front Sheet (and therefore avoids the need to insert details into the body of the DSPA itself).

1.15 The WASPI DSPA 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 DSPA. **The format and standard wording can be changed to meet any specific additional requirements, however we would encourage prior consultation with your 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 Initial Processor and Sub-Processor commenced (and is usually the date upon which the last party signed the DSPA).

Principal Agreement (Section II)

1.18 The details of the agreement between the Controller and the Initial Processor should be included here in the form of "*the [insert description] agreement between [controller] and [initial processor] dated [insert date*]"

DRAFT CONSULTATION

Controller, Initial Processor and Sub-Processor (Sections III, IV and V)

1.19 Section III 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. The details should be taken from the Principal Agreement – this will likely need to be completed by the Initial Processor.

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

1.21 Section V should set out the Sub-Processor. This would be the party engaged by the Initial Processor to carry out specific processing activities on behalf of the Controller.

Data Processing Activities (Section VI to XI)

1.22 Article 28 of the GDPR prescribes the provisions which must be included in a Data Sub-Processing Agreement between an Initial Processor and a Sub-Processor. Where an Initial Processor and Sub-Processor enter into a Data Sub-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 DSPA should set out that information as follows:

- **Subject matter of the sub-processing (Row VI)** - 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 sub-processing (Row VII) –** this should set out what types of processing the Sub-Processor shall undertake of the Personal Data.
- **Purpose of the sub-processing (Row IX) –** this should set out the purpose(s) for which the processor shall process the personal data pursuant to the DSPA. This is important as it limits the extent to which the Sub-Processor can process the Personal Data. Please note that this may only be a subset of the processing which the Initial Processor can undertake on behalf of the Data Controller.
- **Duration of the sub-processing (Row IX) –** this should clearly set out for how long the Sub-Processor shall process personal data. This is usually for the duration for which the purpose is undertaken, so long as the Sub-Processor needs to process the personal data for the purpose or for the duration of the DSPA (or associated commercial agreement), but can be some other period.
- **Categories of Data Subject (Row X) –** this should set out the categories of Data Subject which the Personal Data the Sub-Processor is processing relates to.
- **Personal Data (Row XI) –** this should set out the type of Personal Data the Sub-Processor is to process under this DSPA.

DRAFT CONSULTATION

Sub-contractors(Section XII)

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

1.24 Note that the Sub-Processor is only permitted to appoint Sub-contractors with the Initial Processors prior written consent. Initial Processors should ensure they have obtained the Data Controllers written consent to the Sub-Processors appointment of any Sub-contractors. Entering the Sub-contractors into this table shall be deemed that the Initial Processor has obtained consent of the Data Controller. The Sub-Processor should provide the Initial Processor with information the Initial Processor requires in order to carry out sufficient due diligence on the proposed Sub-contractors.

Minimum aggregate limit of indemnity for insurance (Section XIII)

1.25 Clause 14.2 requires the Sub-Processor to obtain insurance against liabilities arising under the DSPA. Row XIII sets out the minimum level of insurance that the Sub-Processor is required to obtain. The appropriate amount will depend on the exact circumstances of each DSPA 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 Sub-Processor, and the data protection liabilities the Initial Processor has to the Controller under the Principal Agreement.

1.26 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). Initial Processor should discuss this requirement with Information Governance team or Data Protection Officer.

Security details (Section XIV)

1.27 Controllers need to be satisfied that processors have appropriate technological and organisational measures in place to protect the Personal Data – this includes Sub-processors. In a Sub-processor Agreement the obligation to ensure that Sub-processors have appropriate security measures is passed onto the Initial Processor. Initial Processor should ensure that they undertake some due diligence on the processor’s measures in order to satisfy themselves, and the Data Controller.

1.28 Section XIV of the Front Sheet requires the Initial Processor and Sub-Processor 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 Initial Processor to have specific/certain security measures in place under the Principal Agreement, these should be passed down to the Sub-Processor and should be listed here.

Plan for return/destruction (Section XV)

1.29 Section XV should set out how long the Sub-Processor will retain the personal data and how that personal data will then be returned or destroyed by the Sub-Processor following the expiry of that period.

DRAFT CONSULTATION

Locations for processing the personal data (Section XVI)

1.30 Section XVI should set out the locations at which the Sub-Processor (and its Sub-contractors (if any)) will process the Personal Data pursuant to the DSPA.

1.31 Where the Sub-Processor (or its Sub-contractors) 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, and the Controller will want the Initial Processor to ensure compliance in relation to the Sub-Processor.

DRAFT CONSULTATION