Cefnogir gan
Lywodraeth Cymru
Supported by
Welsh Government

Wales Accord on the Sharing of Personal Information

Guide on the development of Joint Controller Agreements

For organisations involved in the protection, safety, health, education and social welfare of people in Wales

(including statutory, private and third sector organisations)

Version 1

Contents

Section 1 – The Development Process

Introduction

1.1 This guidance has been prepared to support the development of **Joint Controller Agreements (JCAs)** under the national framework provided by the Wales Accord on the Sharing Personal of Information (WASPI). This document specifically relates to the JCA 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. The WASPI Website has other information sharing based templates. As well as guidance on choosing the appropriate agreement.

1.3 A Joint Controller agreement (JCA) is an agreement between multiple Controllers that jointly determine the means and the methods of processing data, compliant with Article 26 of the UK General Data Protection Regulation.

1.4. A JCA sets out the determined purposes and means of processing personal data that all controllers within this agreement carry out. It also sets out the rights and obligations of all controllers.

1.5 A JCA is intended to help practitioners understand what decisions have been made about the processing of Personal Data between a number of data controllers and to provide assurance that the partners have considered the requirements of data protection legislation as joint controllers and that each have identified their roles and responsibilities for processing Personal Data jointly.

1.6 A JCA should not be developed in isolation. A JCA should be developed collaboratively with all parties involved in the agreement.

1.7 Take advice if you are unsure whether a JCA is required; this could be from your Data Protection Officer or other suitably qualified person within your organisation.

Considerations before developing a JCA

1.8 Before starting the development of a JCA 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 JCA?	**Prior to starting the development of a JCA, 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 / Privacy Impact assessment?	Information Commissioner'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 identify individuals?	If data to be disclosed does not identify individuals, a JCA is not required.
Does two or more controllers jointly determine the purposes and means of processing the same personal data?	If yes, then a JCA might be applicable and advise should be sought.
Are partners to the JCA data controllers or are any data processors involved?	Data processing activities must be underpinned by a UK GDPR compliant contract. A Data Processing Agreement template is available on the WASPI website.

1.9 Data Protection Impact Assessments (DPIA), also known as Privacy Impact Assessments, 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 JCA) to be identified.

1.10 Take advice if you are unsure whether a JCA is required; this could be from your Data Protection Officer or other suitably qualified person within your organisation.

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

1.12 Organisations who use the WASPI JCA template need to ensure that any completed JCA 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.

1.13 Organisations who use the WASPI JCA template need to ensure that any completed JCA is legally binding from their own organisational requirements. WASPI provide a template agreement which can be used.

<u>The template JCA was developed in partnership with Blake Morgan LLP. Whilst other organisations may use this JCA template, neither WASPI nor Blake Morgan shall owe any duty of care to any other entities and all liability of WASPI</u>

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.

Preparing to develop a JCA

1.14 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 JCA but is strongly recommended. The 'Declaration of Acceptance and Participation' is available on the WASPI website.

1.15 Relevant contracts at partner organisations should be established and the need for a JCA agreed. Roles and responsibilities during the JCA development process should be agreed at an early stage; eg who will lead in the JCA development, will representatives of partners meet to discuss the JCA or will the JCA be developed by one organisation and feedback provided by email.

JCA development

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

1.17 The agreed JCA template is available on the WASPI website.

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

1.19 JCAs 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 JCAs are developed.

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

Section 2 - Populating the JCA template

Front Sheet

2.1 The WASPI JCA template has been pre-populated with standard text and clearly indicates where additional information is to be inserted. The format and standard wording can be changed to meet any specific additional requirements, however we would encourage prior consultation with your information governance teams. 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 JCA.

2.2 Organisations keeping the standard text should ensure they comply with these requirements, otherwise these should be amended and agreed by all partners as necessary. This guidance focuses on the highlighted sections which needs to be completed.

2.3 The template JCA has been designed so that most information specific to the arrangement expected by the JCA is to be included in the Front Sheet. The Front Sheet of the template JCA includes the following details:

- **Section A:** The Parties involved in the agreement – this cross refers to Appendix D. Details of the parties involved will be outlined in Appendix D (at the end of the JCA – see below).

- **Section B:** the agreement administrators, being the individual appointed by the Joint Controllers collectively to be responsible for administering this JCA for and on behalf of the Parties.

- **Section C:** The Purpose of the agreement – 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 DPIA, if completed.

- **Section D:** the authorised users – these are, in relation to each Joint Controller, each member of its Staff who a) falls within any one of the categories specified in (as applicable) the Privacy Notices and b) is authorised by Joint Controller to process the relevant Shared Personal Data for the purposes stated in such Privacy Notices.

- **Section E:** The Commencement Date. The start date of the agreement, which will serve as when the agreement to process information commences.

- **Section F:** The Duration of the processing. How long the agreement is set to last.

- **Section G:** Categories of Personal Data. The categories of information involved in the agreement, such as demographic data, health data, criminal offence information.

- **Section H:** Legal Bases – see Appendix B.

- **Section I:** Agreed Mechanisms for sharing – these are the technical measures means by which the parties shall transmit Shared Personal Data between each other.

- **Section J:** Security – This should set out the security arrangements in place to ensure that data is being processing via secure means and complies with data protection legislation.

- **Section K:** Confidentiality compliance – This should set out how data minimisation is being achieved.

- **Section L:** Review Date and Frequency – how often this agreement will be reviewed as well as the date the agreement will next be reviewed.

- **Section M :** Governance. – any additional governance or agreements that may support the JCA can be included into Appendix C (e.g, this may include operational details of how the information governance arrangements are managed between parties, or could include any applicable Memorandum of Understanding between parties in relation to the joint controller arrangements).

Section 4 - The Joint Controller Partner Organisations and Responsibilities

2.4 The table requires all controllers as part of this agreement to be listed, as well as the individual job role responsible for upholding said agreement and the division that their role is under. This is to ensure that there is a clear list of the organisations and responsible individuals. The table requires every row to be completed. Additionally, for each partner, the job title should be put in the table rather than a named individual. Further Detail is below:

Column A: Controller Organisations – The name of each partner organisations

Column B: Owner/Point of Contact - the role of the individual within said organisations, responsible for their participation in the JCA (this should be job title, not name)

Column C: Department/Divisions/Teams – This typically are those involved in the processing activities.

Column D: Organisation's Role and Responsibilities / Activities – this should clearly set out each party's responsibilities under data protection law.

2.5 Following agreement on the JCA. Organisations can use Appendix C to ensure that all partner organisations have signed the JCA. Where the JCA author has added additional appendices, references to appendices through the JCA should be checked and updated.

2.6 The person responsible for reviewing the JCA should be agreed at the initial development stage.

2.7 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.

Glossary

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

Appendix B – Lawful Basis

2.9 There are four tables within Appendix B of the JCA document that outline legal basis for information sharing.

- **Table 1:** Article 6 Personal Data
- **Table 2:** Article 9 Special Category Data
- **Table 3:** Article 10 Personal Data relating to criminal convictions
- **Table 4:** Competent Authorities for Law Enforcement Purposes

2.10 These tables evidence which lawful bases and, in relation to special category data and criminal convictions data, which conditions are relied upon to process the personal data pursuant to this JCA. Which table(s) will be applicable and need to be completed depends on the nature of the personal data being processed pursuant to this JCA and the nature of the parties processing data pursuant to this JCA. For example, if the personal data relates to personal data which is not special category data or personal data relating to criminal convictions ***and*** is not being processed by a "competent authority" for law enforcement purposes, then it likely that only Table 1 will be applicable. If, however, the personal data is special category data then Table 2 will also need to be completed and similarly if the personal data is criminal conviction data then Table 3 will need to be completed.

2.11 The tables – the legal bases for sharing have paraphrased for the purposes of the template. Full details 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 by competent authorities, further details are available at part 3 of the DPA 2018. Guidance is available on the Information Commissioner's Office website.

2.12 Typically, only one lawful basis from each table should be selected but there may be instances where separate exchanges within the same service rely on different legal bases. An explanatory note should be provided to clarify where different partners rely on different lawful bases. There is no need to list all partners, eg 'Local Authorities rely on Article xx, Police rely on Article xx'.

2.13 The notes sections of the tables explain the additional information to be provided, which varies depending on the relevant lawful basis. Where prompted to explain or provide detail, this should be completed.

Appendix C – Governance and Decision Making

2.13 Authors may add any additional data protection governance and or applicable memorandums of understanding, which may be relevant to the agreement.

Appendix D – Signatories

2.14 Once the JCA 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 JCA. Accepting the agreement by signing it is a key element of demonstrating ‘accountability’ under UK GDPR.

2.15 It is for partners to determine how to manage the signatory process; ie whether ‘does the hard copy of the JCA need physically signing or are electronic signatures are sufficient.

2.16 The signatory should be an individual person with authority to sign the JCA 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.