Cefnogir gan
Lywodraeth Cymru
Supported by
Welsh Government

Wales Accord on the Sharing of Personal Information

The Accord

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

(including statutory, private and third sector organisations)

Version 5.1

Contents

Forewords

Sharing personal information to deliver effective and efficient public services is an essential element of Welsh Government policy. We are also acutely aware that third sector and commercial organisations also need to share personal information to enable effective service delivery.

Empowering staff to share appropriate information with the right person at the right time, is a key principle to delivering effective services; we must ensure that these staff can focus on providing care and support with the confidence that they can do so correctly, legally and with the support of their employers. Similarly, the public must have the confidence that the staff are sharing appropriately and organisations need to have assurance that relevant legal considerations are addressed, and risks identified and mitigated.

The further development of the Wales Accord on the Sharing of Personal Information (WASPI) has been driven by the changing legislative environment and feedback from those who use the framework. It continues to provide an established, recognised and robust good practice approach to information sharing which staff, citizens and all service partners can have confidence.

The Information Commissioner's Office has been integral to the review and update of the WASPI framework, working alongside the various partners to provide an improved and versatile framework that meets the needs of the new legislation and those who use it. I would urge all organisations involved in the delivery of services to people to commit to its use, to make the most of the resources provided and to engage in its community of practice. The WASPI framework is an essential enabler for staff and organisations to provide the best service possible, through sharing information effectively and legally and I am pleased to endorse it.

Julie James
Leader of the House and Chief Whip
August 2018

I am delighted to offer the continued support of the Information Commissioner to the WASPI programme and resources. Wales took a positive and proactive approach many years ago in developing WASPI, and I am pleased that my office has been able to contribute to updating the resources to reflect the new requirements of GDPR and the Data Protection Act 2018.

Sharing personal data appropriately, legally and securely is a vital component of effective public services. And yet I know from speaking and meeting with organisations that they face many cultural barriers within and outside their organisations to the safe and proportionate sharing of data. Clear guidance and commitments assist in meeting some of these cultural barriers head on.

One of my key aims as Information Commissioner is to increase public trust and organisational confidence in sharing data. WASPI helps to ensure that organisations in Wales plan their data sharing carefully, and provide the necessary accountability and transparency to their service users that will help build that trust and confidence.

The General Data Protection Regulation, and the Data Protection Act 2018 are a response to citizens' growing concerns about information rights, and control of their personal data. The new laws require additional accountability and transparency in data handling, and data controllers of all sizes must ensure that they have effective policies and procedures in place. WASPI will help organisations with those responsibilities in the context of data sharing. My office's website is also a good source of advice and guidance www.ico.org.uk.

I look forward to hearing about the continued progress of WASPI.

Elizabeth Denham
Information Commissioner
August 2018

1.1 Introduction

1.1.1 The Wales Accord on the Sharing of Personal Information (WASPI) is supported by the Welsh Government as the 'single' information sharing framework for Wales.

1.1.2 The purpose of the framework is to enable service-providing organisations to share relevant personal information in a lawful and safe way, therefore supporting risk management. In particular, it concerns those organisations that hold information about individuals and who may consider it appropriate or necessary to share that information with others.

1.1.3 This framework applies to all public sector organisations, third sector organisations and private organisations contracted to deliver a public service.

1.1.4 Adoption of the framework across Wales will help ensure compliance with common law and statutory requirements. It also helps organisations meet the considerations set out in the Information Commissioner's statutory 'Data Sharing Code of Practice' and legal requirements for accountability.

1.1.5 The Accord applies to personal identifiable information, which can include pseudonymised data.

1.1.6 The Accord identifies the commitments required by each organisation to enable sharing of personal information. Sign up and ownership is at the highest level.

1.1.7 The Accord's implementation adds significant value to the delivery of effective and efficient services that meet the needs of those receiving them.

1.1.8 The Accord is a statement of the principles and assurances that govern the activity of information sharing. It ensures that the rights of all those involved in the process are protected.

1.1.9 The conditions, obligations and requirements set out in this Accord and supporting documentation apply to all staff who handle and share personal data. This includes direct employees, agency workers, those with honorary contracts and others working on behalf of the partner organisations including agents and sub-contractors.

1.1.10 This Accord will be reviewed by the WASPI Management Board bi-annually, or as changes to legislation dictate.

1.2 Framework documentation

1.2.1 The Accord is supported by template agreements with a focus on the purposes and legal basis for sharing personal information between organisations. Completed agreements are intended for operational use and will document the 'what, when, why, how and who' of information sharing practices for specific, lawful purposes.

1.2.2 A range of supporting documentation has been developed to assist organisations in implementing the framework and is available on the WASPI website - www.waspi.org

1.3 Adoption of the Accord

1.3.1 Formal adoption of this Accord is the responsibility of the Chief Executive or Chief Officer of either a statutory body, private or third sector organisation.

1.3.2 Each signatory organisation agrees to support the adoption, dissemination and implementation, monitoring and review of the Accord and its requirements in accordance with its own internal and any other jointly agreed and authorised information governance standard and/or operational policies and procedures.

1.3.3 Each organisation will identify a "Designated Person" to take responsibility for ensuring the requirements of paragraph 1.3.2, above, are met. This should be each organisation's Data Protection Officer or, where the requirement for this role does not exist, an individual with an equivalent level of seniority.

1.3.4 The Designated Person must satisfy themselves that their organisation will work towards the principles and assurances set out in this Accord.

1.3.5 The 'Declaration of Acceptance and Participation' should be completed and signed by the Chief Executive, Chief Officer, or equivalent to confirm adoption of the Accord. A copy of the declaration is available on the WASPI website.

2.1 Introduction

2.1.1 This section outlines the principal commitments that each signatory organisation will make by adopting this Accord. When fully implemented these should ensure that the organisation's treatment of data subjects' information is compliant with relevant legislation and good practice. Each partner is responsible for complying with the 'Accountability' provisions of data protection law.

2.2 Data Subjects' Rights

2.2.1 Each organisation will allow data subjects to exercise their rights fairly and consistently, and in accordance with any specific legislative requirements, regulations or guidance.

2.2.2 Each organisation must have in place appropriate policies and procedures to facilitate both the protection, and the exercising, of these and other rights.

2.2.3 Each organisation must be clear, open and transparent with data subjects about the collection and use of their personal information, paying particular attention to the 'right to be informed'.

2.2.4 All data subjects have the right to expect that information about them will be protected, managed and processed with the appropriate degree of privacy and confidence.

2.2.5 Each organisation when sharing data about children, will only share children's information where there it has been demonstrated that there is a compelling reason to do so, taking into account the relevant legislation, guidance and the best interests of the child.

2.3 Lawfulness

2.3.1 Before sharing personal data, each organisation shall ensure it has **a general legal power** to do so. Public sector organisations should consider the source of their functions and legal powers. For example, legislation or other laws that set out their functions, and which create an obligation to share personal data, or provide express or implied statutory powers to share. Part 5 of the Digital Economy Act 2017 provides public bodies with gateways to share personal data for specified purposes. Public bodies in Wales should consider whether these powers apply, taking account of relevant codes and guidance. Private and social sector organisations should consider constitutional documents, legal agreements or other regulatory requirements that may restrict or prevent the sharing of personal data. Prior to sharing personal data, each organisation shall ensure it meets any common law duties, for example, the common law duty of confidentiality.

2.3.2 WASPI standard templates require sharing partners to document a **specific lawful basis** for sharing personal data. These are the specific provisions of data protection legislation, such as UK GDPR and the Data Protection Act 2018, that clarify the conditions under which processing personal data is considered lawful. Different lawful bases may be relevant to different sharing partners.

2.4 Staff and Others with Access to Information

2.4.1 Each organisation must have in place operational policies and procedures to facilitate the effective processing of personal information and support staff to share information appropriately, safely and lawfully.

2.4.2 Staff contracts must contain appropriate confidentiality clauses detailing the possible consequences of unauthorised or inappropriate disclosure of personal information.

2.4.3 Each organisation must have in place disciplinary procedures to be invoked if a member of staff is found to have breached the confidentiality of an individual.

2.4.4 Each organisation must ensure that staff with access to personal information have the necessary level of security clearance.

2.4.5 Each organisation must ensure staff with access to personal information receive an appropriate level of training, advice and support. Consideration should be given to the category and nature of information to which staff have access and whether their role includes any specific requirements to access personal information.

2.4.6 Appropriate contractual, data processing and confidentiality agreements must be in place to underpin the processing of personal information by a third party / processor.

2.5 Records Management

2.5.1 Each organisation is responsible for the confidentiality, integrity and availability of the personal information it processes.

2.5.2 Each organisation will take reasonable steps to advise any other party known to have received or to be holding inaccurate personal information.

2.5.3 All participating organisations will have in place policies and procedures to uphold the confidentiality, integrity and availability of personal information with specific reference to the retention, storage and disposal of records.

2.6 Information Security and Risk Management

2.6.1 Each organisation must have in place a level of security commensurate with the sensitivity and classification of the information it processes. This could include adherence to relevant standards, certification schemes or protocols.

2.6.2 Care must be taken, with all aggregated, depersonalised and anonymised information, to ensure that is not possible to identify individuals, e.g. in areas of low population density/low occurrence, as this would still be personal information.

2.6.3 In order to offer an appropriate level of protection to personal information, organisations must apply appropriate physical, organisational and technical security measures.

2.6.4 Before developing and implementing new systems or working practices that process personal information, each organisation must consider the impact on individuals' privacy. Data Protection Impact Assessments (DPIAs) should be undertaken where necessary.

2.6.5 It is accepted that organisations vary in size and complexity. The application of any relevant standards, processes and security measures should take this into account.

2.7 Complaints and Concerns

2.7.1 Any concerns or complaints received from individuals about the processing of their personal data will be dealt with promptly and in accordance with the internal complaints procedures of that partner organisation.

2.7.2 All partner organisations must put in place processes that allow concerns about non-compliance with this framework to be reported to the Designated Person.

Annex 1 – Glossary of Terms

Term	Definition
Controller	Usually an organisation, but can also be an individual, that determines the purposes for which and the manner in which any personal information is, or will be, processed. Controllers must ensure any processing of personal information for which they are responsible complies with relevant legislation including the UK GDPR, and Data Protection Act 2018.
DPIA (Data Protection Impact Assessment)	Data protection impact assessments, also referred to as Privacy Impact Assessments (PIAs), are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.
Data Protection Legislation	Data Protection Legislation in the UK is applied through two main legislations, the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, which should be read side by side. The Data Protection Act 2018 creates specific provisions, such as exemptions allowed by UK GDPR, and incorporates the provisions of EU Data Protection Directive 2016/680 – the Law Enforcement Directive.
Data subject	A 'data subject' is an identified or identifiable natural person. Organisations may refer to data subjects as service users, patients, clients, citizens, staff etc but for consistency, WASPI framework documentation refers to data subjects.
Personal information / data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Practitioner	An inclusive term to describe an employee, or other person who works for or on behalf of a partner organisation, who is involved in the care of or provision of services for the data subject. For example: police officer, health professional, social worker, volunteer etc.
Processors	Organisations that process personal data under Contract to, and according to instructions from, the Controller(s). It is a legal requirement for Controllers to set out in writing the purpose and extent to which Processors may process personal information and the expected measures required to protect that information.
Third sector	A term used to describe the range of organisations that are neither public nor private sector. It includes voluntary and community organisations, registered charities and other organisations such as associations, self-help groups, community groups, social enterprises, mutuals and co-operatives.