Meeting the Requirements

Contracts and Agreements

PECYN CYMORTH LLYWODRAETHU GWYBODAETH CYMRU

WELSH INFORMATION GOVERNANCE TOOLKIT

Introduction

Contracts and agreements may come in many formats ranging from employment, system and service suppliers, third parties, etc. and encompass joint working in the sharing of systems and personal information with likeminded organisations providing services for their service users.

The UK GDPR now makes written contracts between controllers and processors a requirement, rather than just a way of demonstrating compliance with the seventh data protection principle (appropriate security measures) under the former Data Protection Act 1998. Previously, the contract would have required the processor to only act upon the controller's instructions and to take appropriate measures to keep the personal information secure. Under the UK GDPR, there is a separate responsibility to have a contract. The requirements in a contract are now more wide-ranging and are no longer confined to just ensuring the security of personal information. These contracts should ensure that processing of personal information, by a processor, will protect the rights of individuals and comply with all the requirements set out in the UK GDPR.

Contracts must now include specific terms as a minimum. These terms are designed to ensure that processing carried out by a processor meets all the UK GDPR requirements, not just those related to keeping personal data secure.

Whenever a controller uses a processor to process personal data on their behalf, a written contract needs to be in place between the parties. Similarly, if a processor uses another organisation, for example, a sub-processor, to help it process personal data for a controller, it needs to have a written contract in place with that sub-processor. See 'Table One' for the expectations the ICO has on Processors doing work on your behalf.

Contracts between controllers and processors ensure they both understand their obligations, responsibilities and liabilities. Contracts also help them comply with the UK GDPR and assist controllers in demonstrating to individuals and regulators their compliance as required by the accountability principle.

Note: See the 'ICO website' for more information, and their draft guidance on 'Contracts and liabilities between controllers and processors'.

How do we reach Attainment Level 1?

Organisations must ensure any contracts which were in place as of 25th May 2018 meet the UK GDPR's requirements. Existing contracts should have been reviewed to ensure they contain all the required elements to meet UK GDPR, not forgetting any template contracts which may be in use. Every time a controller uses a processor to process personal information, there must be a written contract that binds the processor to the controller in respect of its processing activities.

The UK GDPR sets out specific terms that must be included in the contract, as a minimum. The contract must state details of the processing and must set out the obligations and rights of both

the controller and the processor. It must also include the standards the processor has to meet when processing personal information.

Contracts must set out:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the controller's obligations and rights.

Contracts must also include specific terms or clauses regarding:

- processing only on the controller's documented instructions;
- the duty of confidence;
- appropriate security measures;
- using sub-processors;
- data subjects' rights;
- assisting the controller;
- end-of-contract provisions; and
- audits and inspections.

Note: See the ICO website for further information on 'controllers and processors'

Employment contracts should reference the organisation's Confidentiality Code of Conduct as a source of further information about how the organisation expects its staff to behave in respect of maintaining the confidentiality and security of health and care information. See 'Table Two' for further information.

For staff members that do not have a contract of employment, for example locums, volunteers or university students on temporary placement, organisations should put in place an agreement that obligates the individuals to safeguard personal information and refers to the confidentiality code of conduct. The individual could be asked to sign a stand-alone confidentiality contract or, where it exists, be asked to sign a written locum contract. See 'Table Three' for further information on Professional Obligations.

How do we reach Attainment Level 2?

Contract requirements are more wide-ranging under the UK GDPR and are no longer confined to just ensuring the security of personal information. The Regulation imposes a legal obligation on

controllers and processors to formalise their working relationship. See 'Table Four' for the ICO's expectations on Controller-Processor contract requirements. Processors may only process personal information in line with the controller's documented instructions. Therefore, by having a contract in place with the required terms, controllers and processors are:

- ensuring they each comply with the UK GDPR;
- protecting the personal information of individuals;
- ensuring both parties are clear about their role regarding the personal information that is being processed and can demonstrate this.

The organisation should conduct satisfactory due diligence checks to ensure all potential suppliers, contractors, data processors and third parties are compliant with data protection legislation, industry standards and relevant Welsh Health Circulars. Checks should guarantee that data processors will implement appropriate technical and organisational measures to meet UK GDPR requirements. The ICO expects that:

- The procurement process builds in due diligence checks proportionate to the risk of the processing before you agree a contract with a processor;
- The due diligence process includes date security check, for example, sire visits, system testing and audit requests;
- The due diligence process includes checks to confirm a potential processor will protect data subjects' rights.

In cases where a processor uses another processor (sub-processor), there must be a written contract between the processor and sub-processor. The terms of the contract must also offer equivalent levels of protection for the personal information as those that exist in the contract between the controller and processor. See 'Table Five' for further information on sub-processors.

The organisation should consider 'data protection by design' when selecting services and products to use in data processing activities. When you use third-party products or services to process personal data, the ICO expects organisations to make sure they choose suppliers that design their products or services with data protection in mind.

It is important for the organisation to be fully aware of all contracts and agreements they have in place. The organisation should have processes to ensure all new contracts and agreements are compliant with the requirements set out in UK GDPR. Good practice would be to develop a Register of Contracts and Agreements to enable the organisation to keep track of all those which the organisation is party too. This may include Information Sharing Protocols/Agreements, Joint Controller Agreements, contracts with service suppliers including data processors. The register could link into the organisation's Information Asset Register (IAR).

How do we reach Attainment Level 3?

The organisation should ensure regular reviews of its contracts and agreements take place to ensure data processors are compliant with their contracts. Any amendments should be agreed with

all parties involved. These reviews may be fed back to the Senior Management Team and DPO. The DPO may be able to provide advice and support on the development and review of contracts and agreements regarding the processing of personal information, ensuring their compliance with data protection legislation.

Contracts should include clauses to allow your organisation to conduct audits or checks, to confirm the processor is complying with all contractual terms and conditions. The organisation should carry out compliance checks, proportionate to the processing risks, to test that processors are complying with contractual agreements.

Routine reviews are recommended to ensure that permanent and temporary staff contracts comply with IG responsibilities. Should any necessary changes be made these must be appropriately communicated to staff. For example, in writing, staff briefings etc.

Supporting Resources

ICO: Data Sharing Code of Practice

ICO: Practical advice for micro, small and medium organisations

ICO: The Accountability Framework - *Accountability is one of the key principles in data protection law*

ICO: Data Protection by Design and by Default – *The UK GDPR requires you to put in place appropriate technical and organisational measures*

ICO: Guide to the UK General Data Protection Regulation

ICO: Introduction to data protection

NHS Employers: Employment Check Standards - *The NHS Employment Check Standards outline the employment checks employers must carry out before appointing staff into NHS positions, across England. This includes NHS positions for permanent staff, staff on fixed-term, volunteers, students, trainees, contractors, highly mobile staff, temporary workers (including locum doctors), those working on a trust bank, and other workers supplied by an agency*

NHS Wales: Welsh Control Standard for Electronic Health and Care Records - *The standard describes the principles and common standards that apply to systems that share electronic health and care records in Wales for the purpose of providing direct care.*

General Medical Council: Confidentiality: Good Practice in Handling Patient Information 2018 - *Confidentiality (2018) sets out the principles of confidentiality and respect for patients' privacy that doctors are expected to understand and follow. Supplementary guidance explaining how these principles apply in situations doctors often encounter or find hard to deal with is also available*
GOV.UK: Employment Contracts - *Information about employment contracts, rights to a written statement of terms and other employment matters*

GOV.UK: The NHS Terms and Conditions for the Supply of Goods and the Provision of Services

Welsh Assembly Government: Confidentiality: Code of Practice for Health and Social Care in Wales - *This document sets out non-statutory guidance on best practice for those who work within or under contract to NHS or local authority social services authorities operating in Wales concerning confidentiality and the consent of patient and social care service users to the use of their health and social care records.*

The Wales Accord on the Sharing of Personal Information (WASPI) - *A framework to support organisations share personal information effectively and lawfully*

Summary Requirement

Attainment Level	Summary Requirement
1	Data protection and IG contracts and agreements are in place with all suppliers, contractors, third parties and staff, who have access to/process personal data, which include data protection /IG requirements
2	All contracts and agreements are documented to allow easier assessment of current contracts/agreements already in place and due diligence checks are carried out on all potential suppliers, contractors, data processors and third parties
3	A review process is in place to ensure that all contracts and agreements are regularly reviewed, and any changes are communicated appropriately