Guidance on 3rd Party Contracts

Introduction

Social Care Providers are data controllers in data protection law. This is because care providers choose how and why they process data and what data they process.

Any organisation which holds, creates or amends data on your behalf is called a data processor. In the GDPR it is a legal requirement that you have a written contract in place with your data processors.

The requirements for contracts between a controller and processor are set out in GDPR Articles 28-36 and Recitals 81-83. This guide has been designed to tell you what you need to have in your contracts. There is a checklist to follow on page 2.

Responsibility

Under GDPR, data controllers and data processors are both directly responsible for any non-compliance with the law. This means that they can be sanctioned, pay administrative fines or pay compensation to data subjects. This is different to the old Data Protection Act (1998) where only the data controller took responsibility.

Who needs a contract?

You must have a written contract every time you employ a data processor. This is true when you are directly employing the processor and when a processor, with your written permission, employs another processor.

There is a checklist for what you should be including in contracts on the next page.

What must a contract include?

Use the following checklist to check that your contracts comply with data protection legislation:

General Clauses	
Processor provides a guarantee to implement appropriate measures to make sure that they comply with data protection law and protect individuals' rights.	
Processor will only employ a sub-processor with our written permission. If a change is made to a sub-processor, we will be informed and given the opportunity to object.	
The Contract Sets Out:	
The subject-matter of the processing.	
How long the processing will continue for.	
The nature and purpose of the processing.	
The type(s) of personal data which will be processed and the type(s) of data subjects.	
Our organisation's rights and obligations under law.	
Specific instructions on how we want the processor to process our data.	
Processor obligations:	
The processor will only process data with our written instruction (including when making international transfers of data) unless required to do so by law.	
The processor has committed themselves (including their employees) to confidentiality.	
The processor will assist us with our legal obligations.	
The processor will allow audits by ourselves or someone we mandate to fulfil an audit.	
The processor will maintain a record of processing activities.	
At the end of the contract the processor will either destroy or hand-back (up to us) all personal data we have provided.	
The processor will cooperate with our and their supervisory authorities.	
The processor will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. This can include (as appropriate): • Pseudonymisation and encryption of data; • Ability to ensure ongoing confidentiality, integrity, availability and resilience of systems; • Ability to restore availability and access to personal data in a timely manner; or • A process for regularly testing the technical and organisational measures for security.	
The processor must notify us as soon as possible when they become aware of a personal data breach.	
Sub-Processors:	
A processor will not employ another processor (sub-processor) without our specific or general written permission.	
If a sub-processor is employed and makes any changes, our processor must give us the opportunity to object to them.	

If a processor engages another processor, the same data protection obligations are imposed on that data processor.	
If a sub-processor fails to fulfil their data protection obligations, the first processor remains liable to us for the sub-processor's obligations.	

There is more information available on the ICO's website.