How to comply with ADISA and the UK GDPR when operating as a sub-processor or using a sub-processor

What is a sub-processor?

A sub-processor is any organisation who a data processor uses to perform part of their own data processing activities.

For an ADISA member this might be the use of a separate organisation to provide additional services such as hard drive repair, shredding or tape incineration. If an ADISA member uses any other organisation for a service which includes any aspect of data sanitization then the relationship is data processor to sub-processor and must be operated in accordance with the UK GDPR, UK Data Protection Act and the ADISA 2021 Standard version 8.0.

An ADISA member might also act as a sub-processor to a data processor in situations where the processor is operating as a reseller for their services (channel) or for another ITAD who wishes to use them to offer ITAD services to its customers.

This guidance note firstly explains what how to identify if you are a sub-processor or if you use a sub-processor and then reviews the legal aspect of the UK GDPR before overlaying the new ADISA 2021 8.0 Standard.

Identifying if you use sub-processors

If you use any other organisation to deliver part of your service and that organisation performs anything to do with data sanitisation then they are a sub-processor.

Examples of sub-processing activities for an ADISA Member are:

1. COMPANY A is the data processor for client y. Client y wants an urgent job for onsite hard drive shredding for which they have a contract in place with COMPANY A but COMPANY A's shredder is already committed. COMPANY A engages COMPANY B to provide the service.
    In this instance COMPANY B is a sub-processor to COMPANY A
2. COMPANY A is permitted within their contracts with their customers to send drives which fail a wipe to a specialist hard drive repair centre ran by COMPANY C. COMPANY C offers a service whereby the drives are repaired and re-wiped using a software equivalent to that offered by COMPANY A to its customers. If the drive cannot be repaired COMPANY C destroys it in an equivalent way to the terms agreed by COMPANY A and their customers. In this instance COMPANY C is a sub-processor to COMPANY A.
3. COMPANY A is permitted within their contracts with their customers to store tape and to send for incineration once a month. The process for managing this is agreed in writing

with their customers. COMPANY A uses an incineration service offered by COMPANY D which includes secure collection, containment and segregation at the facility and then destruction which is recorded, and evidence submitted back to COMPANY A.
In this instance COMPANY D is a sub-processor to COMPANY A.

4. COMPANY A uses two third party logistics companies to make their pick-ups. COMPANY E only does pick-ups whereas COMPANY F offers onsite shredding as well.
In this instance COMPANY E is NOT a sub-processor to COMPANY A and COMPANY F will NOT be a sub-processor when only making collections. However, COMPANY F will be a sub-processor when they are being used for shredding services.

5. COMPANY A consolidates all smart phones and sends them to COMPANY G who sanitizes them. COMPANY A's contract with their customers says, "All Smart Phones have factory reset".
In this instance, COMPANY A is breaking the law as they have no written authorization to use a sub-processor. In this instance, COMPANY G would be viewed as a Data Processor to COMPANY A as COMPANY A has assumed Controller responsibility by making a processing decision without written authorization.

For ADISA, if the sanitization undertaken on the media is done by the member then any downstream actions taken are NOT sub-processing. For example; within your contracts with your customers if it states "All hard drives are punched before being sent for recycling" then the company doing the recycling is NOT a sub-processor even if they shred the drives sent to them from you. This is because the processing activities undertaken by you can only have WRITTEN AUTHORISATION from the client, and therefore that written authorization ends with the punching. However, if the contract said "All hard drives are punched before being sent for further shredding to 22mm" then the company collecting the drives IS a sub-processor. Again, because the written authorization includes a further sanitization process on the hard drives to 22mm.

LITMUS TEST: If you use any other company to perform a data sanitization service then they are a sub-processor.

Identifying if you are a sub-processor

If you sell your services to another organisation (COMPANY Z) who utilizes them on behalf of one of their customers AND the contract is formed between you and COMPANY Z, then you are a sub-processor. If COMPANY Z, introduces you to their customers (COMPANY Y) and you engage directly with COMPANY Y and provide all documentation to COMPANY Y directly then you are a Data Processor to COMPANY Y.

Examples of sub-processing activities which as ADISA Member might perform are:

1. COMPANY X is an ADISA Member based in Scotland and rings COMPANY V who is also an ADISA member, to make a collection on their behalf at Client y and ask COMPANY V to provide all reports to COMPANY X.
COMPANY X is the data processor for client y and COMPANY V is the sub-processor.

2. COMPANY X has an on-site shredding vehicle and is asked by COMPANY Y to do an on-site job at one of COMPANY Y's clients but provide reports to COMPANY Y
COMPANY X is a sub-processor to COMPANY Y.

3. COMPANY X used COMPANY Y to repair drives which they are not permitted to do in writing from their customer. In this instance, COMPANY X is breaking GDPR rules and

ADISA Certification. In this instance COMPANY X has assumed Controller responsibility and COMPANY Y is the Data Processor.

It's really important to understand if you are a sub-processor or a data processor. If you have a company reselling your services and you provide that client with all the reports for THEIR customer, then you might be a Data Processor or a Sub Processor depending on whether or not the channel partner has themselves complied with GDPR.

LITMUS TEST: If you provide your services to a company OTHER than the company whose equipment you are collecting and processing then you are most likely a sub-processor, unless you have a relationship directly with the company you are collecting the equipment from.

UK GDPR requirements for the Processor / Sub-Processor relationship.

The UK GDPR requirements are clear for the use of sub-processors.

- Article 28 (2) which states that the processor shall not engage another processor without prior specific or general written authorization of the controller. In the case of the general written authorization, the processor shall inform the control of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.
- Article 28 (4) which states that it is the Data Processor's responsibility should they appoint a sub-processor to ensure that the sub-processor is engaged using an equivalent contract to one which the data processor has in place with each of its clients.

ADISA requirements for the Processor/Sub Processor relationship.

ADISA Requirements for a Member acting as a sub-processor as per the ADISA 8.0 Standard are that they MUST have the ADISA Sub-Processor Form complete. Please see Appendix A.

ADISA ITAD Standard 8.0 New Criterion-

Section 2: Module 8. Sub Processor Disclosure

Essential

REF	Criteria
2.8.1	Applicants shall complete the sub-processor disclosure form and revalidate and submit to ADISA every six months
2.8.2	The use of a sub-processor shall be disclosed to and approved in writing by the customer prior to work being carried out.
2.8.3	When a sub-processor is changed or new sub-processor appointed, the applicant shall disclose the change to the customer prior to the change occurring in order to permit the customer to object

Section 2: Module 9. Using a Sub Processor

Essential

Ref	Criteria
2.9.1	Sub-processors shall be controlled by a contract which has the same explicit data protection obligations which the applicant has agreed with the customer. This is to include all aspects in 2.1.2.
2.9.2	Any sub-processor used to perform any part of the data processing service shall be audited by the applicant to ensure conformance with ADISA Standard. This can be done by a third-party or by the applicant but shall involve a physical audit and result in a written record. Self-validation by the sub-processor is not permitted

Highly Desirable

Ref	Criteria
2.9.3	Any sub-processor used to perform any part of the data processing service should be ADISA certified.

Section 2 Module 10 – Operating as a Sub Processor

Essential

Ref	Criteria
2.10.1	Where applicant operates as a sub-processor, they shall record how they inform the data processor of the obligations under Article 28(4) that the data processor must put in place the same data protection obligations with the sub-processor as set out in their own engagement with their customer.

Appendix A ADISA Member's Sub-Processor / Third Party Disclosure Form

Example

Supplier Name	Address	Service Offered	Use of Sub-Processor approved by Customer? If so, how is this achieved?	* Contract compliant with Criterion 2.9.1	ADISA Certified?	* Audit Done compliant with Criterion 2.9.2
e.g. ABC Shredding	*Shredtown, Birmingham*	*Shredding*	*Customer contract*	*Yes*	*No*	*Yes*

*Copies to be provided to ADISA

Appendix B ADISA Member operating as a Sub Processor

This is to be used by the ADISA Member when operating as a sub-processor as per requirements below.

2.10.1
Where ITAD operates as a sub-processor they shall record how they inform the data processor of the obligations under Article 28(4) that the data processor must put in place the same data protection obligations with the sub-processor as set out in their own engagement with their customer.

Name of ADISA Member	
Name of Data Processor*	
Brief note on relationship between Data Processor and ADISA Member**	

*Data Processor would be the channel partner.

** This should include details of whether the channel partner white labels the service OR whether they introduce the ITAD to their customers. Who issues the reports and to whom they are sent?

We confirm that the data processor wishes to engage with ADISA Member to provide data sanitisation services on behalf of one or more data controllers. Data Processor is aware that under Article 28 of the General Data Protection Regulation 2018, that there is a need for a contract to be in place between both parties and that the terms of that contract should be equivalent to the terms entered with the data controller.

Signed on behalf of Data Processor

Sign   _____

Name   _____

Title   _____

Date   _____

Signed on behalf of ADISA MEMBER

Sign   _____

Name   _____

Title   _____

Date   _____