Sheffield Hallam University

Data Protection for Researchers:
Sharing Personal Data with Partners and Suppliers

Roles and responsibilities – Data Controller or Data Processor?

Definitions:

- '**controller**' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- '**processor**' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

The University is normally a data controller for research purposes as we determine the means by which, if not the purpose for which, the personal data is processed, even where we are commissioned and funded to conduct research by another organisation. When conducting consultancy or evaluation projects for another organisation, we may still be a data controller as we are bringing specialist skills which involve professional judgement and mean that we determine which data is processed and how it is processed. The University is a registered controller and this is a corporate role, covering all employees of the University. Employees carrying out their normal duties and fulfilling their employment contracts are not separate controllers or processors. Processing by postgraduate research students for their programme of studies/research will also fall within the University's controller role and registration.

The University does occasionally take the **role of a data processor** when conducting research and in these instances, would need to act on the instructions of controller and would have less control over the processing and the data.

There is usually a **lead organisation in a funded collaborative research project** who may serve as the principal point of contact with the funding body, receive and distribute the funding between the partners and take responsibility for reporting and administrative arrangements etc. This would not automatically make them the controller and the other collaborators the processors for all the processing. It would be more likely that all are controllers with equal responsibilities and decision-making responsibilities for the research data that is collected, shared, and analysed.

The ICO has published checklists to help determine whether an organisation is a data controller or a data processor and we have included this in some more detailed guidance about controller and process roles.

In the course of a project, we might **appoint data processors** to act on our instructions and to process personal data on our behalf. Examples would include hiring transcribers, outsourcing some data collection work, buying in an IT platform hosted by another company.

Data Sharing Agreements and Data Processing Agreements

Data sharing and processing agreements – why are they important?

- To comply with GDPR legal obligation
- To formalise working relationship between the two parties
- To clarify the role of each party
- To set out the obligations and liability of each party
- To protect the personal data and rights of data subjects
- To help demonstrate compliance to individuals and regulators

Do I need a data agreement and how do I do this?

Data Processing agreements are required by law when engaging a data processor. The University has a template agreement and can vary this if there are specific processing requirements that need to be added. We try to use this

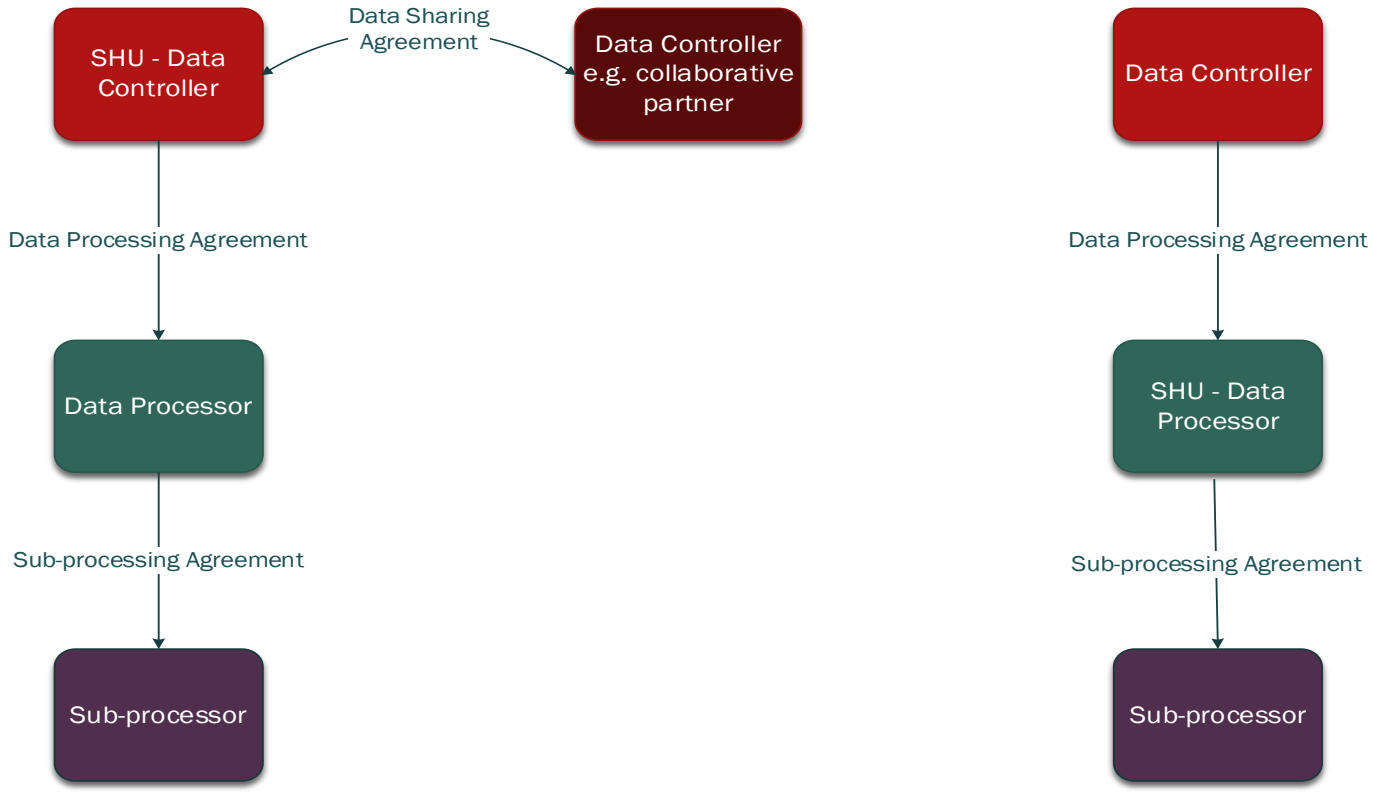
wherever possible, but some suppliers may insist on using their own terms. You should seek advice from the IG team to ensure that supplier terms are compliant, fair, not overly onerous on the University and give adequate recourse and liability should there be a problem or a data breach on the part of the supplier. Processors have liability for their sub-processors but controllers retain some liability for whole of the processing or supply chain, so it is really important that a written agreement covering all requirements is in place to protect data subjects, the University, and its financial assets.

Data sharing agreements between two or more controllers should be considered particularly for large quantities of sensitive data or regular data sharing as these help the parties to agree who does what and to act consistently. We sometimes enter into a joint controller agreement/relationship where both parties are jointly responsible, accountable, and liable for all the processing and make decisions together throughout the project.

Data sharing and data processing agreements should be made between the University and the other party, not an individual member of staff or a specific research institute or centre (although you can include the name of the research institute or centre in the agreement), as the University is the registered data controller and is the legal entity that will accountable and liable for the fulfilment of the agreement. Data agreements should be signed by a senior member of staff, usually Director level.

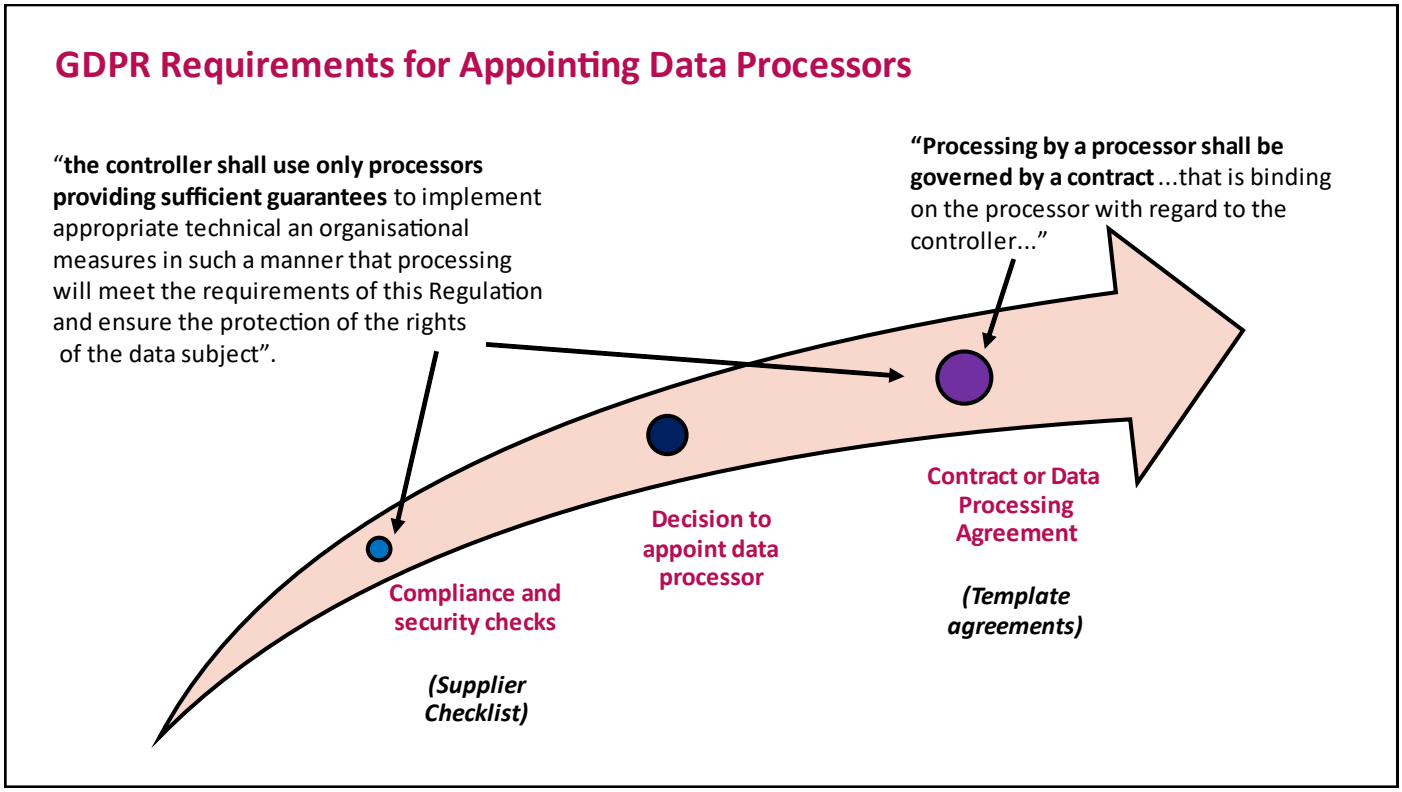
You may need some additional sections to an agreement if you are **sharing data with an overseas partner or using a supplier in another country**. This is generally still straightforward for partners and suppliers in the EEA post-Brexit, but is more complex for some countries. Agreements with international partners or suppliers may need to include additional privacy in the other party's country. See section on international data transfers below.

If you are already working with RISLegal on contracts and agreements for your project, they will be able to assist with the data agreements, using the templates agreed with the IG Team and with additional advice from the IG Team where required. The IG Team are happy to advise on standalone agreements. It is advised that researchers flag requirements for data agreements as early as possible , particularly where the project requires international partnerships and/or the appointment of new suppliers who are data processors. Please see [further advice on data agreements and appointing data processors] which includes template agreements.



Choosing a data processor

When appointing a data processor to process personal data on behalf of the University, we are required to obtain guarantees and assurances that the processor will comply with data protection laws and keep personal data secure. We obtain contractual guarantees in the contract/agreement, but should also seek assurances before we put a contract in place or sign up to their terms. We have supplier checklists that we ask new suppliers to complete to ensure that we choose suppliers who can fulfil the requirements.



International Data Transfers

The General Data Protection Regulation (GDPR) was a piece of European legislation introduced to establish a consistent approach between member states and to allow data sharing within the EEA. When the UK left the EU, the text of the GDPR was essentially retained, but all references to the EU were removed in order to create the UK GDPR.

The EU GDPR and the UK GDPR work on the basis that some countries have equivalent data protection/privacy legislation and data sharing with organisations in these countries therefore gives data subjects a similar level of protection, and some countries don't have equivalent legislation which means personal data would not have the same level of protection if transferred to those countries. It is possible to transfer data to this second category, but additional safeguards need to be put in place to ensure adequate protection for data subjects.

Following Brexit, the EU and the UK have agreed that each has equivalent data protection legislation and have issued what is known as an 'Adequacy Decision'. The UK has also made adequacy decisions for a number of other countries and is working to agree similar adequacy decisions for other countries (see lists below).

For other countries that do not have an adequacy decision, we need to put in place additional safeguards to allow a data transfer. These usually take the form of additional contract clauses. Prior to Brexit these were known as 'Standard Contractual Clauses'or 'EU Model Clauses'. These are being phased out following Brexit and new international data transfers now require a new UK International Data Sharing Agreement (IDTA). The University is also required to undertake a risk assessment prior to the transfer. The IG Team undertakes these assessments.

Additional Guidance

Information about Contracts and Agreements: https://sheffieldhallam.sharepoint.com/sites/3037/SitePages/Bids-and-Tenders.aspx

ICO guidance on International Data Transfers: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

ICO guidance on contracts: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/ and https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/

Further Information and Support: Information Governance Team

Sharepoint: https://sheffieldhallam.sharepoint.com/sites/3037/SitePages/Information%20Governance.aspx

Email: DPO@shu.ac.uk