THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

Operational

Data Protection and contracts

Guidance for staff

This guidance takes you through what you need to include when sharing or sending personal data with someone outside the School.

Why do you need a contract?

The short answer is that even if the other person/organisation has a data breach, the School could end up with the fine.

There are two ways you can be processing personal data, as a data controller or a data processor. The main difference is that the data controller decides what do to with the personal data and the data processor does what the data controller tells them to.[1] For the School's main procurement contracts, data protection clauses are already included in the standard template. However, you may need a separate agreement to ensure that you have covered everything relating to the sharing and processing of personal data.

What sort of contract do I need?

The following is a summary of the contract templates available. More explanation is provided below. This can look complex, but once you know what sort of contract you need, you can pick the template that suits you.

- Controller to Controller – when you are sharing data with another controller but both of you are deciding what to do with it at either end. If you are deciding jointly what to do with the data, that is considered a Joint Controller relationship. From the School's viewpoint this can vary by:
    - The other controller is in the UK – so requires a Data Sharing Agreement. We can use the other controller's template if they have one.

[1] More or less. Sometimes data processors will be given scope to make some decisions e.g. store it in this GDPR compliant cloud rather than another, but they can't decide what to collect and who they can share it with.

    - The other controller is in the EU/EEA, or considered an adequate country, – so requires a Data Sharing Agreement or International Standard Contract depending on the other controller's requirements. We can use the other controller's template if they have one.
    - The other controller is in another country not covered by the above – so requires an International Standard Contract. We must use our template.
- Controller to Processor – when you are sharing or storing data with a data processor. If the School is considered the processor, we would expect that the data controller provides the contract. If we are the data controller, we supply the template which can vary by:
    - The data processor is in the UK – so requires a Data Processor contract. This can be fairly simple like a confidentiality agreement for short term student research workers or a transcription service. For more substantial agreements, the School's main Data Processor clauses need to be put into a contract with the processor.
    - The data processor is in the EU/EEA, or considered an adequate country– so requires the School's main Data Processor clauses.
    - The data processor is in another country not covered by the above – so requires the International Standard Contract.

In all of the above, minimum information security standards should be supplied to help individuals and organisations meet the security requirements.

What does a controller-controller relationship look like?

Types of controller-controller relationships are:

- Academic Partnerships
- Knowledge Transfer Partnerships
- Partnership Agreements
- Studentship Agreements
- Data sharing Agreements
- Research Agreements
- Agency Agreements
- Consultancy Arrangements with corporate entities/Individuals

What does a controller-processor relationship look like?

Types of controller-processor relationships are:

- Supply of Services Agreement (where Service Provider processes personal data on behalf of HEI)

- SAAS Agreements
- IT Processing Contracts
- Agreements with a marketing Services Provider
- Research/collaboration Agreements where the other Party processes personal data
- Using a transcriber, interpreter or local researcher

EU/EEA, Adequate Country, Privacy Shield?

For external to the UK data transfers, it matters whether the country is in the European Union/European Economic Area, considered an adequate country by the EU, covered by the Privacy Shield or in none of those categories.

1. First check the EEA states: The EEA countries consist of the EU member states and the EFTA States. The EU member states are Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom.
   The EEA states are Iceland, Norway and Liechtenstein. The EEA Joint Committee has made a decision that the GDPR applies to those countries and transfers to those countries are not restricted.
   The UK government has stated that we will consider these countries to be adequate to send personal data to.

2. Check if the country where the data is being transferred to is considered by the EU commission to have adequate safeguards and therefore no further consideration of GDPR needs to be made. The EU Commission has made a full finding of adequacy about the following countries and territories:
   Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.
   The Commission has made partial findings of adequacy about Canada and the USA. The adequacy finding for Canada only covers data that is subject to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). Not all data is subject to PIPEDA. For more details please see these FAQs on the adequacy finding on the Canadian PIPEDA.
   The UK government has stated that we will consider these countries to be adequate to send personal data to. All of them have also said the UK is adequate except Andorra.

3. If the country where data is to be transferred is not seen to be adequate-then consideration of whether there will be an international transfer and if so the International Data Transfer clauses produced by the ICO will be used.

How do I fill out the contract?

Most of it is ready to go, but there are some parts that you will need to fill out.

Section A Personal data types

This section lists the likely personal data types that you will be sharing with the other party. For each of them, choose either yes or no from the drop down list. If there is a type of personal data that you want to share that is not listed, let us know and we'll add it to the template, but most of the time you should not need to do so.

Section B Sensitive or Special Category

This section lists any special categories personal data types that you will be sharing with the other party. This list comes directly from the GDPR so cannot be added or changed. For each of them, choose either yes or no from the drop down list.

Section C Lawful basis

This section covers the lawful basis under which you are processing either Section A or Section B personal data. These lawful bases are set out in Articles 6 and 9 of the GDPR. You can use more than one but you must identify at least one lawful basis that covers the data transfer.

For Section A personal data, these are likely to be:

- Contract – in order to fulfil the terms of a contract the data needs to be shared
- Legal – you must share the data because legislation or a court judgement requires it
- Task in the public interest – would cover research or teaching data.
- Legitimate interests – would cover marketing purposes and possibly some research.
- Consent – only where none of the above apply.
- Vital interests – where it is in the vital interests of the individuals whose data you are sharing. This is almost never likely to be used as the purpose for data sharing at the School outside of a medical emergency.

For Section B personal data, it is unlikely you would use all 10 available lawful bases. The ones to consider are:

- Research – for any research related data sharing
- Employment, social protection law – for equalities type data sharing
- Occupational health – for occupational health providers.

If you are sharing Section A personal data, choose at least one of the lawful bases from the drop down list. If you are using more than one, after choosing your first, move down to the next cell, and choose from the drop down listagain.

If you are sharing Section B personal data, choose at least one of the lawful bases from the drop down list.

Section D Additional Legal basis

Section C should cover most of the data transfers you are doing. However, occasionally a legal basis

from Section D will apply as well/instead. These require a bit more explanation.

3 covers situations where the data being shared is going to be used for a different purpose for which it was collected. This will usually be when data is being repurposed for research. Choose yes if this is the case from the drop down list, or no if this doesn't apply to your sharing. You may still have to identify a lawful basis in Section C for this type of data.

4 covers processing of criminal data, which is covered by the separate Data Protection Act 2018. Choose yes if you are processing this data, no if you are not. You do not need to identify a lawful basis above for this type of personal data.

5 covers processing of data that has been deidentified. In other words, you could not identify the individual from the data. Choose yes if you are sharing deidentified data or no if you can identify individuals from the data. Technically, deidentified data if properly anonymised falls outside the scope of the GDPR. If this is the case, you do not need to identify a lawful basis in Section C.

6 covers when you are not sharing personal data, e.g. when you are sharing financial figures but not personal data. Therefore you should only choose yes if no personal data will ever be shared for the contract and no where you are sharing personal data. Obviously if you choose no for this question, you don't need to fill out the rest of the Sections, except for Section E.

Section E Retention period

The contract also needs to say how long the parties need to keep the data once the contract has ended, due to the timeliness principle, so the choice of retention period is mandatory to fill in. If your situation is not covered by the options, get in touch with Legal or the DPO. The options are:

7 the end of the contract. If the sharing can stop completely at this point, with either the School, the other controller and/or processor no longer needing the data, choose yes for this option.

8 once the processing is no longer necessary. This covers situations where the sharing may have occurred at some point, but the data continued to be processed after sharing. At a certain point, it may not be necessary to process any further e.g. the processing was for a conference that has now finished.

9 some years after the processing/contract finishes. Add the number of years e.g. 6 years after the contract finishes. You use this option when you may need to keep the data to prove processing occurred.

10 information will be anonymised. Use this option when after the initial transfer, the data can be anonymised for further use. For example, if you are transferring data into a data archive or can work with anonymised data instead of the full set.

11 exemption for research. Use this option for research data where you may use it in the future, whether you have identified a project or not. This cannot be used for other types of processing, only research.

Review schedule

Review interval	Next review due by	Next review start
3 years	31/05/2025	1/05/2025

Version history

Version	Date	Approved by	Notes
1	29/4/2019	Information Governance Committee	
1.1	06/05/2022	Information Governance Management Board	Minor changes

Links

Reference	Link

Contacts

Position	Name	Email	Notes
Data Protection Officer	Rachael Maguire	r.e.maguire@lse.ac.uk	

Communications and Training

Will this document be publicised through Internal Communications?	**Yes**
Will training needs arise from this policy	**Yes**
If Yes, please give details - inhouse	