Data Sharing/Transfer Guidance

Scope

This guidance covers all data sharing and data transfer arrangements, including arrangements where third parties collect data on our behalf.

Principles

To ensure that all data sharing with/transfers to third parties comply with the requirements of UK GDPR the following steps should be carried out **before** any personal data is shared.

- ***Classification***
- ***Data Privacy Impact Assessment (DPIA)***
- ***Due Diligence***
- ***Documents Required***
    - ***Contracts***
    - ***Management plan***
- ***Logging***

Responsibilities

The contract owner/person managing the sharing/transfer is responsible for ensuring that the steps in this guidance are done as part of the wider contract preparation. This guidance is addressed to the contract owner and reference to “you” are to the contract owner.

The Data Protection Officer (Legal Services) is responsible for providing advice and specific guidance on implementing this guidance.

Classification of the Sharing/Transfer

As data sharing/transfer can include a wide range of different scenarios which have different risks and requirements, you need to classify the arrangement. You need to answer the following questions:

1.	Who?	Who is the person with whom data will be shared? As with all legal relationships, you need to know actual legal title. Are they an international organisation (e.g. the UN, or another treaty body)?
2.	What data?	A description of the data to be shared. In particular any 'Special Category' data or data relating to criminal convictions should be set out in detail ('Special Category' data is any data relating to racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data (where used for identification purposes); data concerning health, sex life or sexual orientation.)
3.	Which direction?	Will the data flow from the University to the third party, from the third party to the University, or in both directions?
4.	Why?	What is the purpose of the data sharing. As with all data processing, whether internal to the University or involving third parties, we need to have a lawful basis for the processing. You also need to know 'whose' legal basis we are relying on – the University's or the third party's (for example, whose public task, or whose legitimate interest). The permissible bases are: • Consent of the data subject (generally you should avoid relying on this) • Contract (necessary for a contract with the data subject)

		• Legal obligation (not including contractual obligations) • Vital interests • Public task • Legitimate interests In addition if the sharing/transfer involves 'Special Category' or criminal convictions data, additional conditions apply. Please get advice from the DPO.
5.	When?	If the data sharing/transfer is regular or ongoing more formal arrangements are required.
6.	Where?	Will the data stay in the UK? If not, which countries will it go to? • UK only • Country in respect of which adequacy regulations have been made (currently EEA, Andorra, Argentina, Canada (only some data is covered – get advice from the DPO), Faroe Islands, Gibraltar, Guernsey, Isle of Man, Israel, Japan (only private sector organisations), Jersey, New Zealand, South Korea, Switzerland and Uruguay. • Anywhere else.

The key classification of the arrangements are:

1. Controller to Controller (C2C) Exceptional – A one-off arrangement where the third party controls the purpose of the data processing
2. Controller to Controller (C2C) Regular – A regular or recurring arrangement where the third party controls the purpose of the data processing
3. Controller to Processor (C2P) – where the University controls the purpose of the data processing
4. Joint Controller – where both the University and the third party control the purpose of the data processing (this will be rare, so get advice from the DPO if you think this may apply).

Data Privacy Impact Assessment

As with all new data activity a Data Privacy Impact Assessment (DPIA) may be required if the activity poses a high risk to individuals' data. You should complete the standard screening questionnaire to determine whether a DPIA is required. Contact our Data Protection Officer (DPO) for guidance on the need for a DPIA.

Due Diligence

Once you have classified the arrangement complete the following basic due diligence. It is the same regardless of the classification of the arrangement.

	UK	**Outside UK but with adequacy regulations**	**Outside UK with no adequacy regulations**
1. Due diligence - regime	No further steps required	No further steps required	DP risk assessment on regime given context of sharing. Refer to DPO.
2. Due diligence – recipient	• On ICO register • Not registered – refer to DPO	• Registered with relevant government regulator • Not registered – refer to DPO	Refer to DPO

Documents

To demonstrate compliance with our obligations and as a matter of good practice, we need to have in place relevant documents. Generally this will involve a contract setting out each side's obligations in relation to the data. Legal Services can provide templates for standalone arrangements or add-on clauses where the data sharing/transfer is connected to a bigger project (e.g. where data is provided to a contractor who is delivering service to the University). If an existing contract already deals with data protection issues, it will need to be reviewed to ensure that the

provisions are adequate.

	UK	Outside UK, but with adequacy regulations	Outside UK with no adequacy regulations
C2C Exceptional/One-off	written request/written record of request, and decision record	written request/written record of request, and decision record	refer to DPO
C2C Regular	data sharing agreement	data sharing agreement	data sharing agreement with IDTA/SCCs[1] OR data sharing agreement and article 49 derogation[2] decision record (mandatory)
C2P	data processing agreement (mandatory)	data processing agreement (mandatory)	data processing agreement (mandatory) with IDTA/SCCs
Joint Controller	joint controller agreement	joint controller agreement	joint controller agreement with IDTA/SCCs OR joint controller agreement and article 49

[1] International Data Transfer Agreement or Standard Contractual Clauses. These are contractual provisions that the regulators have approved that contractual bind
[2] Limited derogation under the UK GDPR – get advice from the DPO.

			derogation decision record (mandatory)

Ongoing Management

Under the data protection legislation it is not enough to have appropriate agreements in place, they must be managed, especially in C2P and international arrangements.

	UK	**Outside UK, but with adequacy regulations**	**Outside UK with no adequacy regulations**
C2C Exceptional	None	None	None
C2C Regular	None	None	DPA and IDTA/SCCs management plan
C2P	DPA management plan	DPA management plan	DPA and IDTA/SCCs management plan
Joint Controller	None	None	DPA and IDTA/SCCs management plan

The management plan should cover:

- Event based – how we deal with matters as they arise e.g. data breaches, failure to cooperate &c
- Annual – how we check for any change in the type of data and/or purpose
- End of relationship – How we ensure and verify deletion or return of all the personal data to the controller and deletion existing copies.

Please consult with the DPO regarding the creation of management plan.

Logging

So there is a central record of all data sharing, which will allow us to monitor ongoing risk and manage the risks, you must notify the DPO of the following:

- Classification of Arrangement (Exceptional, C2C, C2P, joint)
- Jurisdiction (UK, Adequacy, Elsewhere)
- Recipient

- Data types
- Start date
- End date
- Contract
- Upload Management Plan

Contacts

Data Protection Officer (DPO) – Tracy Brathwaite

dsar@londonmet.ac.uk