L-Università ta' Malta

University Research Ethics Committee (UREC)

Transferring Personal Data Outside of the EU: Additional information

29 September 2023

1. What is a 'data sharing agreement'?

A data-sharing agreement is a formal contract between two or more data controllers ***(see definitions section below)*** covering the purpose of the data sharing, what happens to the data at each stage, what data is being shared and how the information will be used. It set standards and helps all the parties involved in sharing to be clear about their roles and responsibilities.

It is imperative to set down all arrangements between the data controllers in the data sharing agreement which must be vetted by UM's Legal Services Office and Data Protection Unit and signed by the Rector, the researcher/s and any supervisor/s from UM's side and by the legal representative of the other party.

2. What is a 'data processing agreement'?

A data processing agreement is very similar to a data sharing agreement, but this is an agreement issued by a controller to a data processor ***(see Terminology section below for definitions)***. To ensure a transparent allocation of responsibilities and liabilities, processing by a processor must be covered by a contract or other binding legal act between the controller and processor which documents the instructions of the controller as well as the subject-matter and duration of the processing, then nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller. Regarding the subject-matter, this should refer clearly to the nature, scope and context of the processing. The duration of the processing may be specified by

a start and end data and the purpose should comply with the purpose limitation principle laid down in Article 5(1)(b).

As the processor must only act under the instructions of the controller, it should obtain from the controller prior specific or general authorisation to use sub-processors or to make changes to arrangements with existing sub-processors, in order to give the controller, the possibility to object.

It is imperative to set down all arrangements between the data controller/s and the data processor/s (or between processors and sub-processors) in a data processing agreement, which is to be vetted by UM's Legal Services Office and UM's Data Protection Unit and signed by the Rector, the researcher/s and any supervisor/s from UM's side and by the legal representative of the other party.

3. What should I do if in the frame of my research I require to transfer data to a third country or international organisation, outside the EU/EEA?

One must differentiate between those third countries (including territories or one or more specified sectors within such countries) and international organisations which the European Commission has found to provide an adequate level of data protection, and those that do not. An 'adequacy decision' by the European Commission requires that the legal system of a third country or international organisation be 'essentially equivalent' to that of EU data protection law.

The European Commission has so far recognised Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, and Uruguay as providing adequate protection.

The effect of such a decision is that personal data can flow from the EU (and Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary. In others words, transfers to the country in question will be assimilated to intra-EU transmissions of data.

It is imperative that a data sharing agreement or a data processing agreement as necessary, is filled in by the Researcher and vetted by UM's Legal Services Office and UM's Data Protection Unit and

signed by the Rector, the researcher/s and any supervisor/s from UM's side and by the legal representative of the other party.

4. What should I do if in the frame of my research I require to transfer data to a third country or international organisation, which is not covered by an adequacy decision (such as the USA or Australia)?

When an adequacy decision has not been issued, a controller or processor may transfer personal data to a third country or an international organisation only if it has provided appropriate safeguards, and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available. Such appropriate safeguards are based on a set of protections that apply to the particular data transfer or set of transfers.

Finally, derogations may be used in certain cases when there is no essential equivalence and appropriate safeguards cannot be used.

In such circumstances or for any assistance please contact UM's Legal Services Office and UM's Data Protection Unit for guidance.

Terminology

1. What is a 'controller'?

'Controller' is defined in the law as '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'. The crux of controllership for the purposes of the GDPR is the determination of the purposes and means of the processing of personal data. Therefore, the controller exercises influence over the 'why' and the 'how' of such processing.

The concept of 'controller' must be understood in light of the legislator's aim of placing primary responsibility for protecting personal data on the entity that actually exercises control over the data processing. This entails taking account not simply of legal formalities but factual realities.

Thus, although the UM acts as controller for the research with personal data that is done under its auspices, this is a shared responsibility with the researcher/s involved. Researchers are responsible within their own research projects to thoroughly consider the data protection aspects and to comply with the legal obligations of the **General Data Protection Regulation** ('GDPR'), **UM's Research Code of Practice and UM's Research Ethics Review Procedures**.

2. What is a 'joint controller'?

Controllership may be shared. Where several operators determine jointly the purposes and means of the processing of personal data, they participate in that processing as joint controllers

3. What is a 'processor'?

A 'processor' is defined in the law as 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'. The role of 'processor' results from a delegation or 'outsourcing' of tasks determined by the controller. A processor must be an entity that is legally separate from the controller. An entity is only a processor in so far as it acts within the remit set by a controller.

Article 28(1) GDPR states that 'the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.' Thus, taking on the processor role requires considerable expertise, skills and other resources.