

Guidance on the type of clauses to be included in a contract between DCU (including campus companies) & any external party involving the transfer or processing of personal data

Scope

In all cases where a unit of DCU (including its wholly owned campus companies) seeks to engage in any arrangement with an external party for the transfer or processing of personal data the unit's management and/or staff are required to inform the University Data Protection Officer (Ext. 8706) in advance of the drafting or signing of any agreement or contract with the external party.

Definitions

Personal Data (PD): Data relating to a living individual (i.e. the 'Data Subject') who is or can be identified either directly from the data or from the data in conjunction with other information in the possession of the Data Controller.

Data Controller (DC): A person (including legal entities such as companies or trusts) who, either alone or with others, controls the content and use of personal data. In most cases this will be either DCU or one of its campus companies.

Data Processor (DP): A legal entity (i.e. a company, institution, service provider, sole trader etc.) or individual who process personal data on behalf of a Data Controller. Note that this does not include an employee of the Data Controller who processes such data in the course of their own employment.

Legal and Guidance References

- 1) The 1988 & 2003 Data Protection Acts (Data Protection Acts)
- 2) Article 29 Working Party - July 2012 Guidance

Background

The Data Protection Acts require that where a Data Processor is engaged to process personal data on behalf of a Data Controller then the work being done must be the subject of a written contract. The contract must state that the Data Controller will only process the personal data in accordance with the controller's instructions. In addition, the Data Processor must ensure that the personal data is kept safe from unauthorized access, alteration, and destruction and from any other unlawful processing.


If DCU legitimately transfers or shares personal data with an external party without a robust contract in place then DCU will have very limited recourse in law should the external party fail to properly secure the data or protect it from unlawful processing. The type & nature of clauses to be included in a contract should be tailored to each case. The Data Protection Working Party, an independent European advisory body on data protection and privacy, recommended that issues set out below should be considered for inclusion in such a contract.

Issues to be addressed in a personal data related contract

- 1) The subject data of the contract.
- 2) The time frame of the contract.
- 3) The Data Controller's instructions as to what processing is to be performed on the personal data.
- 4) Possible penalties or indemnification of the Data Controller against any losses caused by the failure of the Data Processor to fulfil its obligations under the contract or the law.
- 5) Guarantees of data security, including specific details on the technical and organisational measures to be taken to implement it.
- 6) Specification for the return or destruction of the personal data at the conclusion of the contract.
- 7) Ensuring that only authorized individuals have access to the data and that appropriate confidentiality clauses are included in the employment contracts of the processor's staff.
- 8) Obligations to assist the Data Controller to facilitate the exercise by the Data Subject of their rights to access, correct and/or erase their own personal data.
- 9) Disclosure of details of sub-contractors to be employed in fulfilling the contract, including provision for prior notification of any changes to these arrangements in the course of the contract, with the Data Controller to be given the opportunity to object to the changes or to terminate the contract.
- 10) Obligations to notify the Data Controller of any data breaches.
- 11) A list of the locations in which the data processing may be done.
- 12) Obligations to co-operate with the Data Controller with regard to its right to monitor data processing.
- 13) Notification of relevant changes to the cloud server such as changes in functionality.
- 14) Provision for the logging and auditing of the processing of personal data.
- 15) Disclosure to the Data Controller of any legally binding request for access to personal data by law enforcement agencies except where such disclosure is itself legally prohibited and guarantees that the Data Processor will reject any such request which is non-legally binding.

- 16) A general obligation to provide assurance that the Data Processor and its sub-contractors are compliant with national and international data protection legal requirements and standards.
- 17) Details of which country's courts will have jurisdiction in the event of a dispute between the parties.
- 18) The contract should also refer to how the agreement will be terminated and the consequences of termination.

Version Control

Document Name	Guidance on Personal Data Contract Clauses	
Version Reference	2.0	
Document Owner	Chief Operations Officer	
Approved by	Data Protection Officer	
Date	25th July 2016	