

Union Education Online

Personal Data Flows and Institutional Interrelationships Document

**Andrew Charlesworth
Centre for IT & Law
University of Bristol**

V1.0 - 28/02/05

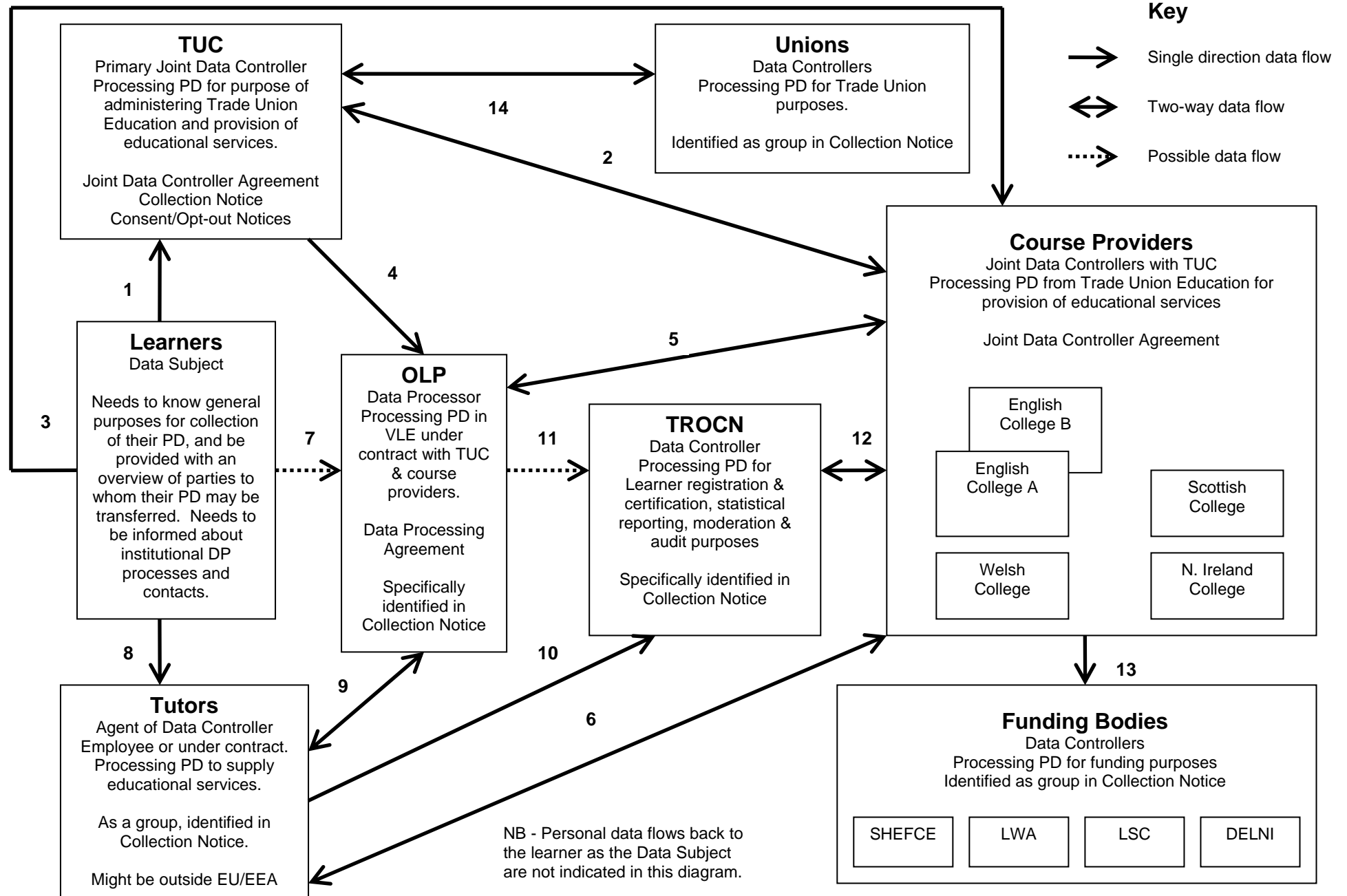


Table 1 - Flows of Learner Personal Data

No.	Parties & Direction	Roles	Purpose of Processing	Processing Criteria for Data Controller	
				Schedule 2 DPA	Schedule 3 DPA
1	Learner to TUC	Learner - Data Subject TUC - Data Controller	Administration of UEO Education Services Provision	Contract or <u>Consent</u>	Explicit consent Reason - Trade Union membership Reason - Physical or mental health Reason - Race/ethnicity Reason - Religion
2	Between TUC & Course Provider	TUC - Joint Data Controller CP - Joint Data Controller	Education Services Provision	Contract or <u>Consent</u>	Explicit consent Reason - Trade Union membership Reason - Physical or mental health Reason - Race/ethnicity Reason - Religion
3	Learner to Course Provider	Learner - Data Subject CP - Joint Data Controller	Education Services Provision	Contract or <u>Consent</u>	Explicit consent Reason - Trade Union membership Reason - Physical or mental health Reason - Race/ethnicity Reason - Religion
4	TUC to OLP	TUC - Data Controller OLP - Data Processor	VLE Service Provision	Contract or <u>Consent</u>	Explicit consent Reason - Trade Union membership
5	Between OLP & Course Provider	CP - Data Controller OLP - Data Processor	Education Service Provision	<u>Contract</u> or Consent	No sensitive personal data
6	Between Course Provider & Tutor	CP - Data Controller Tutor - Employee or Data Processor	Education Service Provision	If tutor is employee - the transfer is within the DC. If Tutor is a Data Processor the processing will be subject to a data processing agreement which will reflect the CP's processing criterion.	If tutor is employee - the transfer is within the DC. If Tutor is a Data Processor the processing will be subject to a data processing agreement which will reflect the CP's processing criteria.
7	Learners to OLP	Learner - Data Provider/Controller OLP - Data Host	Possible creation of personal webpages via WebCT	No personal data transfer except by learner action.	No sensitive personal data transfer except by learner action.
8	Learners to Tutor (Course Provider)	Learner - Data Subject Tutor - Employee or Data Processor	Pastoral/Educational Services	Contract or <u>Consent</u>	Explicit consent Reason - physical or mental health

9	Between OLP & Tutor (Course Provider)	OLP - Data Processor Tutor - Employee or Data Processor	Education Service Management	<u>Contract</u> or Consent	No sensitive personal data
10	Tutor (Course Provider) to TROCN	Tutor - Employee or Data Processor TROCN - Data Controller	Moderation & Audit Purposes	<u>Contract</u> or Consent	No sensitive personal data
11	OLP to TROCN	OLP - Data Processor TROCN - Data Controller	Moderation & Audit Purposes	<u>Contract</u> or Consent	No sensitive personal data
12	Between Course Provider and TROCN	CP - Data Controller TROCN - Data Controller	Learner registration and certification Moderation & Audit Purposes Statistical reporting Success Data for Funding Purposes	<u>Contract</u> or Consent	No sensitive personal data
13	Course Provider to Funding Bodies	CP - Data Controller FB - Data Controller	Funding Administration	<u>Contract</u> or Consent or DC legitimate interests	No sensitive personal data
14	Between TUC and Union	TUC - Data Controller Union - Data Controller	Notification of need for and completion of training for admin. purposes.	<u>Consent</u> or DC Legitimate interests	No sensitive personal data

Glossary

CP Course Provider
 DC Data Controller
 DPA 1998 UK Data Protection Act 1998
 PDP 1995 EU Data Protection Directive 1995
 FB Funding Body
 OLP Open Learning Partnership

PD Personal data
 TROCN Open College Network
 TUC Trades Union Congress
 UEO Union Education Online
 VLE Virtual Learning Environment

Table 2 - Flows of Learner Personal Data

Number	Parties & Direction	Purpose of Processing	Notice given & necessary consents obtained	Withdrawal of consent	Subject Access to Data
1	Learners to TUC	Education Services Provision	TUC Registration	Inform TUC	Via TUC as Data Controller
2	Between TUC & Course Provider	Education Services Provision	TUC Registration	Inform TUC	Via TUC & CP as Joint Data Controllers
3	TUC to OLP	Provision of VLE Services to Learner	TUC Registration	Inform TUC	Via TUC as Data Controller OLP is only a Data Processor
4	Learner to Course Provider	Education Services Provision	CP Registration	Inform CP	Via TUC & CP as Joint Data Controllers
5	Between OLP & Course Provider	Education Services Provision	CP Registration	Not applicable - contract	CP as Data Controller OLP is only a Data Processor
6	Between Course Provider & Tutor	Education Services Provision	CP Registration	Not applicable – contract If tutor not employee then CP.	CP as Data Controller Tutor is employee or Data Processor
7	Learner to OLP	Creation of personal webpages via WebCT	Not applicable	Not applicable	Not applicable as Learner has access, edit and delete control.
8	Learners to Tutor (Course Provider)	Pastoral/Educational Services	CP Registration	Inform CP	CP as Data Controller Tutor is employee or Data Processor
9	Between OLP & Tutor (Course Provider)	Education Services Provision	CP Registration	Not applicable - contract	CP as Data Controller Tutor is employee or Data Processor
10	Tutor (Course Provider) to TROCN	Moderation and Audit Purposes	CP Registration	Not applicable - contract	TROCN as Data Controller
11	OLP to TROCN	Moderation and Audit Purposes	TUC Registration	Not applicable - contract	TROCN as Data Controller
12	Course Provider to TROCN	Moderation and Audit Purposes Success Data for Funding Purposes	CP Registration	Not applicable - contract	TROCN as Data Controller
13	Course Provider to Funding Bodies	Organisation of Funding Issues	TUC Registration	Not applicable - contract	Funding Bodies as Data Controllers
14	TUC to Union	Notification of need for and completion of training for union internal administration purposes.	TUC Registration	Inform TUC	Union as Data Controller

Definition of terms

Collection Notice	A collection notice is used by a Data Controller to provide a Data Subject with information relevant to the processing of their personal data, at the time of its collection. It will describe the purposes for which the Data Controller intends to process their personal data, and should also include details of Joint Data Controllship, as well as indications of third parties to whom the data may be disclosed or transferred, and the purposes served by those transfers or disclosures. As such, the collection notice does not need to cover every specific eventuality, but must provide sufficient information to demonstrate that a data subject could have 'reasonably expected' their data to be processed in the manner the Data Controller intends. The collection notice should provide enough information to the Data Subject to allow them to utilise effectively the rights provided to them by the DPA 1998 (e.g. subject access). The Data Subject should be able to re-access the collection notice at a later date in hardcopy or electronic form. Changes to a collection notice should always be notified to relevant Data Subjects. Collection notices are often provided in conjunction with consent forms where the Data Controller is seeking consent as a Sch.2 or Sch.3 criterion for lawful processing. In schemes like UEO, which involve a mix of Joint Data Controllers and Data Controllers in common, there may be more than one collection notice, and care should be taken to ensure that the information these provide to Data Subjects is consistent. See Data Controller, Joint Data Controller, subject access and consent .
Contract	The DPA 1998 Sch.2 s.2 provides, as a criterion for lawful processing a Data Subject's personal data, the fact that the processing is necessary for the performance of a contract to which the Data Subject is a party, or for the taking of steps at the request of the Data Subject with a view to entering into a contract. <u>This criterion applies to circumstances where the personal data to be processed does not contain sensitive personal data</u> . Where sensitive personal data is to be processed, the Data Controller must satisfy both a Sch.2 and a Sch.3 criterion and, as performance of a contract is not a listed criterion for lawful processing under Sch.3, an additional Sch.3 criterion will be required. As the range of Sch.3 criteria are limited, it is likely that in cases involving sensitive personal data UEO Data Controllers will need to have the explicit consent of the Data Subject in order to process that personal data. However, there are several aspects of UEO's operations where personal data will be processed or disclosed, but where the obtaining of consent would probably be of little value, as without the ability to process or disclose the personal data essential UEO services could not be provided and thus the learner could not participate in the UEO. Where there is no issue of sensitive personal data, such processing or disclosure may be carried out without requiring consent, e.g. under the Sch.2 s.2 heading. See consent, explicit consent and contract
Consent	The DPA 1998 does not contain a definition of consent. Article 2 of the DPD 1995 defines consent as "any freely given specific and informed indication of his wishes by which the Data Subject signifies his agreement to personal data relating to him being processed." If a Data Subject's consent is to be relied on to provide a Sch.2 criterion (Sch.2, s.1) for lawful processing, then the fact of consent cannot be simply assumed by a Data Controller (e.g. where a Data Controller sends out a form stating that in the absence of a negative response from a Data Subject their consent will be assumed). Where there is obvious inequality of bargaining power between the Data Controller and Data Subject, it may also be difficult to demonstrate the 'freely given' element of consent. Equally, consent may be withdrawn by the Data Subject at any point, a fact that may prove problematic for UEO Data Controllers where consents are obtained for data processing purposes without which the Data Controller cannot provide an essential UEO service - in other words where the learner's consent cannot be withdrawn without in effect ending the learner's involvement in the UEO. In such circumstances, the use of the contract criterion (Sch.2 s.2) will be more appropriate. See contract and explicit consent .

Data Controller	The DPA 1998 defines a Data Controller as “a person who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data are, or are to be, processed”. The fact that an individual or institution holds or processes personal data does not make them a Data Controller, if they do not determine the purpose and manner of that holding or processing. For example in this case, OLP has possession of learner personal data and processes it within the VLE. However, OLP does <u>not</u> determine the purpose and manner in which the data is processed, as these issues are determined jointly by the TUC and Course Providers, and so OLP is not a Data Controller. There may also be cases where more than one Data Controller controls the processing of a set of personal data. See Data Controller in Common, Joint Data Controller and Data Processor .
Data Controller in Common	Data controllers who share personal data on Data Subjects for different purposes are referred to as ‘Data Controllers in common’. Each Data Controller remains individually responsible for the processing they have carried out on the personal data. The term does not appear to be widely used. See Data Controller, Joint Data Controller and Data Processor .
Joint Data Controller	Data controllers who share personal data on Data Subjects for the same purpose, and who would be jointly liable for any breach under the DPA 1998, are referred to as ‘Joint Data Controllers’. In the UEO scenario, the TUC and Course Providers will be jointly determining the purpose and manner in which the learners’ personal data is processed, for the purpose of providing educational services within UEO; as such they will be Joint Data Controllers. No other Data Controllers in the scenario have such a relationship, and they are thus not Joint Data Controllers with the TUC and Course Providers, but rather Data Controllers in common. See Data Controller, Data Controller in Common, Data Processor and Data Controller Agreement .
Data Controller Agreement	In this document, a Data Controller Agreement means a contract between two or more institutions which will be entered into before they act as Joint Data Controllers. The Agreement will set out the terms and conditions under which each institution may process the jointly-held personal data. In most circumstances parties to a data sharing agreement will be registered Data Controllers and, as such, one requirement of membership of the Agreement may be the production of the Information Commissioner’s notification number. In the UEO scenario, the TUC and each individual Course Provider will be Joint Data Controllers for the learners’ data. See Data Controller Protocol and Data Sharing Agreement .
Data Controller Protocol	In this document, a Data Controller Protocol means a document which outlines the necessary conditions with which a Data Controller must comply before being eligible to enter into a Data Controller Agreement. This will detail the types of measures required to meet the terms and conditions of the Data Controller Agreement, for example a condition that requires member institutions to have ‘appropriate technical and procedural security’. The Protocol allows the current and prospective members of a Data Controller Agreement to adhere to a consistent set of measures, which are capable of change over time without requiring continual changes to the Data Controller Agreement, e.g. when new technologies require alterations to what is commonly understood by ‘appropriate technical and procedural security’. In the UEO scenario, this will also enable the efficient incorporation of additional Course Providers into the Data Controller Agreement by providing a data protection benchmark for their administrative processes. See Data Controller Agreement and Data Sharing Agreement .
Data Processor	The DPA 1998 defines a Data Processor as any person, other than an employee of the Data Controller, who processes the data on behalf of the Data Controller. An employee of the Data Controller is regarded by the DPA 1998 as constituting part of the Data Controller. OLP will be a Data Processor within the UEO, processing data on behalf of the TUC and the Course Providers. Additionally, in the UEO scenario, where a tutor is not an employee of the Course Providers, but is instead independently contracted to supply educational services, if s/he does not determine the purpose and manner in which the learners’ data is processed, s/he will be a Data Processor and not a Data Controller. A Data Processor has no statutory obligations under the DPA 1998 as regards processing it carries out on behalf of the data Controller. The DPA 1998 places the burden for ensuring that Data Processors do not

allow breaches of the Act upon the Data Controllers who use them. Data Controllers will thus need to ensure that their relationship with a Data Processor is governed by a formal Data Processing Agreement. See **Data Controller, Data Controller in Common and Joint Data Controller**.

Data Processing Agreement	In this document, a Data Processing Agreement means a contract between a Data Controller and a Data Processor, which will be entered into before the Data Processor begins processing personal data on behalf of the Data Controller, and will set out the responsibilities of both parties in respect of that processing, as well as any indemnities required by the parties. In the UEO scenario, a Data Processor Agreement will be required between the TUC and Course Providers as Joint Data Controllers, and OLP as a Data Processor. Exceptionally a Data Processor agreement may be required between Course Providers and tutors, in circumstances where tutors are engaged on a contractual rather than employee basis.
Data Sharing Agreement	In this document, a Data Sharing Agreement means a contract between Data Controllers who are not Joint Data Controllers, which will be entered into before the disclosure or transfer of personal data from one to another, or between them, with each Data Controller making disclosures to others as and when required. The Data Sharing Agreement will set out the responsibilities of both parties in respect of those transfers and current/future processing. In the UEO scenario, this could cover the transfer of learner personal data from the TUC to individual unions, or from Course Providers to TROCN.
Data Subject	The DPA 1998 defines a Data Subject as an individual who is the subject of personal data. In this document the Data Subject at issue is the UEO learner. See subject access .
Opt-in	The Data Subject must provide a positive response to a proposal that their data can be used in a particular manner (e.g. tick here if you want your data to be processed for this purpose). This is effectively a consent mechanism. See consent and opt-out .
Opt-out	The Data Subject must provide a negative response to a proposal that their data can be used in a particular manner (e.g. tick here if you don't want your data to be processed for this purpose). Many Data Controllers like to use opt-out solutions because Data Subjects are prone to not reading opt-out/opt-in agreements and often skip over tick boxes. However, the more likely the use of the personal data is to cause distress or damage to the Data Subject if it is used in the manner proposed, the more likely it is that opt-in will be the appropriate mechanism if opt-in/opt-out is considered. Note that opt-out will normally be used independently of the use of consent as a Sch.2 criterion (due to the fact that Data Controllers cannot assume consent from a non-response) – e.g. if the Data Controller intends to use another Sch.2 criterion such as the Sch.2 s.6 legitimate interests criterion, but wishes to allow Data Subjects to indicate that they do not want their data used for the stated purpose. See consent, legitimate interests and opt-in .
Legitimate interests	The DPA 1998 Sch.2 s.6 allows, as a criterion for lawful processing a Data Subject's personal data, the fact that the processing is necessary for the purposes of legitimate interests pursued by the Data Controller, or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the Data Subject. <u>This criterion applies to circumstances where the personal data to be processed does not contain sensitive personal data.</u> Where sensitive personal data is to be processed, the Data Controller must satisfy both a Sch.2 and a Sch.3 criterion and, as legitimate interests of the Data Controller or a third party is not a listed criterion for lawful processing under Sch.3, an additional Sch.3 criterion will be required. In UEO, the provision of non-sensitive learner personal data to Funding Bodies and to the learner's Union could potentially be justified under this head and thus be carried out without requiring the learner's consent. However, in order to avoid prejudice to the rights and freedoms or legitimate interests of the Data Subject, it would be sensible to provide an opt-out for the learners in circumstances where Sch.2 s.6 is used. In practice, it is not currently envisaged that this criterion will be used within the UEO process. See consent, opt-out and opt-in .

Personal data

The DPA 1998 defines personal data as any information that relates to an identified or identifiable person (the Data Subject), or which in combination with other information in the possession of, or that is likely to come into the possession of, the data controller would permit their identification. The DPD 1995 further defines an identifiable person as one who can be identified by reference to 'an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'. The meaning of the term 'personal data' was considered by the UK Court of Appeal in the case of *Durant v Financial Services Authority* (2003). In *Durant* the Court of Appeal did not consider the issue of the identifiability of an individual, but concentrated on the meaning of "relate to". The Court decided that data will relate to an individual if it: "is information that affects [a person's] privacy, whether in his personal or family life, business or professional capacity". The Court identified two issues that may aid in determining whether information "is information that affects [an individual's] privacy" and, thus, "relates to" an individual:

- "The first is whether the information is biographical in a significant sense that is, going beyond the recording of [the individual's] involvement in a matter or an event which has no personal connotations..."
- "The information should have the [individual] as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest ..."

If an individual's name appears in information the use of the name implicates 'personal data' only where its inclusion affects the named individual's privacy. Thus, the fact that an individual's name appears on a document, does not mean the information contained in that document will necessarily be personal data about the named individual. It is more likely that an individual's name will be 'personal data' where the name appears together with other information about the named individual such as address, telephone number or information regarding his hobbies.

The Information Commissioner considers that the following examples of information will not normally be personal data: "mere reference to a person's name where the name is not associated with any other personal information; incidental mention in the minutes of a business meeting of an individual's attendance at that meeting in an official capacity; or where an individual's name appears on a document or e-mail indicating only that it has been sent or copied to that particular individual - the content of that document or e-mail does not amount to personal data about the individual unless there is other information about the individual within it."

Durant is a controversial case, because the Court appears to have narrowed the definitions of 'personal data' and 'relevant filing system' in UK law to the point where those definitions are no longer consonant with the definitions in the EU DPD 1995. As such the UK may now be in breach of its obligation under EU law to properly implement the DPD 1995 into UK law. Further re-definition of 'personal data' is thus likely, especially as the EU Commission has threatened formal action against the UK for non-implementation. Changes to the definition of 'personal data' may affect the nature of some of the data flows within the UEO process, for example the flow from OLP to TROCN which may, or may not, include personal data depending on the definition used. See **sensitive personal data**.

Processing

The DPA 1998 defines data processing as 'obtaining, recording or holding the data or carrying out any operation or set of operations on the data.' This includes collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. It is irrelevant whether these actions are manual or automated. The breadth of the DPA 1998 definition effectively means that from the moment of its collection, to the moment that it is destroyed or fully anonymised, personal data is being processed and must thus be treated in accordance with the Act.

Sensitive personal data

The DPA 1998 defines sensitive personal data as personal data relating to racial or ethnic origin, political opinions, religious beliefs, membership of trade union organisations, physical or mental health, sexual life, offences or alleged offences. See **personal data**.

Subject access

The DPA 1998 provides Data Subjects with a number of rights in regard to their personal data held by Data Controllers. Most of these rights are linked to, and/or depend for their usefulness upon, the availability of an effective right of subject access. Subject access means that a Data Subject is entitled to be told by a Data Controller whether personal data about them is being processed by, or on behalf of, that Data Controller. Subject access requests can only be made to Data Controllers, and not to Data Processors. If the Data Controller is processing personal data about a Data Subject, the Data Subject is entitled to a description of that personal data. They are also entitled to know the purposes for which the personal data are being, or are to be, processed, and to be informed about the recipients, or classes of recipients, to whom their personal data have been, or may be, disclosed. Data subjects are also entitled to a copy of their personal data in comprehensible form, as well as any information held by the Data Controller as to the source of those data. As the effective exercise of many subsequent rights (e.g. the rights of correction and erasure) may depend upon the Data Subject obtaining this information, it is critical that the subject access mechanism implemented by Data Controllers operates in an efficient and timely fashion. To this end, it is essential that, in systems like UEO, the roles of the relevant institutions are clearly understood (who is a Data Controller, who is a Data Processor etc.), and that the responsibility for providing effective subject access to Data Subjects to their personal data, at all points in the process, is clearly delineated. See **Data Subject, Data Controller and Data Processor**.

Overseas transfers

In the event that a Data Controller wishes to export personal data outside the EU/EEA, the Eighth Data Protection Principle comes into play. This states that “personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of personal data.” Where a country has an adequate level of protection, personal data transfers are, in principle, automatically permitted. Additionally, there are a number of legislative exemptions from the export ban which are independent of the adequacy rules. These are contained in Sch.4 DPA 1998. In the UEO scenario, there are 5 possible exemptions. Sch 4 s.1 - The Data Subject has given his consent to the transfer; Sch 4 s.2. - The transfer is necessary for the performance of a contract between the Data Subject and the Data Controller, or for the taking of steps at the request of the Data Subject with a view to his entering into a contract with the Data Controller; Sch.4 s.3. - The transfer is necessary for the conclusion of a contract between the Data Controller and a person other than the Data Subject which is entered into at the request of the Data Subject, or is in the interests of the Data Subject, or for the performance of such a contract; Sch 4 s.8. - The transfer is made on terms which are of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of Data Subjects. Sch 4 s.9. - The transfer has been authorised by the Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of Data Subjects. It is unlikely that this problem will arise on a regular basis in UEO – the main (only?) role affected is likely to be that of a tutor, where a tutor is contracted by a Course Provider to provide educational services and that tutor is based outside the EU/EEA. In such circumstances, where the foreign country has an adequate level of protection, there is no additional issue. If the foreign country does not have an adequate level of protection, then Sch 4 s.1 consent or Sch 4 s.2 contract fulfilment would be possible. However, it is worth noting that the Course provider would be expected both to have notified its intention to transfer personal data overseas and to have a suitable contract in place with the tutor as Data Processor to protect the rights and freedoms of learners in respect of their personal data, and that this could itself form the basis for a Sch 4 s.8 or Sch 4 s.9 exemption.