Skills Funding Agency

OFFICIAL

# Skills Funding Agency Data Sharing Agreement Terms & Conditions

## 1. Introduction

The Skills Funding Agency ("the SFA") is an executive agency of the Department for Business, Innovation and Skills ("the Department"). The Department is a data controller of personal data processed by the SFA (except where such data is processed for the purposes of another party). This Agreement is made between the requesting party ("the third party") and the Department for Business, Innovation and Skills through the SFA.

## 2. Purpose

The purpose of the agreement is to provide a framework for the sharing of personal data between the Department (the data controller) through the SFA, and a third party requesting access to the data, to ensure that the following are all clearly defined, understood and agreed by each party to the agreement:

- the purposes for, and legal basis on which the personal data are to be processed by the third party, and any data processor acting for and on the third party's behalf, and
- the personal data to be shared, and
- the proposed processing of the personal data (for example, shared, used, retained and destroyed) by the third party, and any data processor acting for and on the third party's behalf, and
- the respective responsibilities in relation to the data and the proposed data processing

The agreement has been written with due attention to relevant legislation, together with guidance and Codes of Practice issued by the Office of the Information Commissioner, and requirements for the protection of personal data under the Cabinet Office Security Policy Framework.

References to personal data are as defined under the Data Protection Act 1998.

This includes data which might be described as 'depersonalised': for example, where some personal markers have been removed, but where individuals might still be capable of being identified either from the data itself or by manipulation, for example, by 'depersonalised' data being joined up with other information to enable individuals then to be identified.

## 3. Making requests for personal data

Requests for personal data from the SFA must be made by third parties in writing, and to be agreed under the terms and conditions of this agreement. Except where there is a defined legal requirement, there is no obligation to share any data with third parties.

### 3.1 Signed documents

A signed hard copy of this agreement, fully completed, should be submitted to the SFA before data will be issued.

### 3.2 Scope of purpose for processing personal data and agreement period

A request for data may be made for a single purpose or multiple uses of the same data over a period of time. Agreements will usually run for a maximum of twelve months or for any shorter period specified and agreed in relation to one or more of the specified uses, and then be subject to review and renewal of the agreement.

### 3.3 No routine issue of data

Data requests are the responsibility of the requestor and all requests made of the SFA for data are considered on their own merits. Unless previously agreed, the SFA does not send out new data as a matter of course to a third party. Each set of data has to be requested from the SFA at a time when available.

### 3.4 SFA process for considering requests

The SFA will consider a request for data in light of the use to which the data are to be put and the suitability of the data elements requested for that use. SFA staff may contact the third party requesting the data for further information.

Each request will be dealt with on its own merits and the SFA commits to no timescale for the handling of the request. The more detailed the information provided in the application, the more quickly each request can usually be processed.

### 3.5 Refusal to supply data

In considering any request for data, the SFA will take into account the use to which the data are to be put. The SFA has the right to refuse to share data with third parties and refusal does not have to be explained.

### 3.6 Supply of data – type and media

Where data is supplied, it will normally be encrypted and pass phrase protected using WinZip, then delivered by File Transfer Protocol (FTP). Except where legally obliged, the SFA will supply the data in Comma Separated Values format (CSV).

## 4. Control of data

This section deals with the legal distinction between a data controller and a data processor in relation to the processing of personal data under the agreement.

### 4.1 Data Controllers

A data controller is a person or organisation that either alone or jointly with another controller, determines the purposes for which and the manner in which any personal data are processed.

#### 4.1.1 The Department as Data Controller

To the extent that the Department processes the personal data for its own purposes, the Department is the data controller of any personal data that it provides to a third party under the Terms and Conditions of the agreement. At no time upon providing third parties with the personal data does the Department cease to be a controller of that data for the purposes that the Department processes that data.

#### 4.1.2 Third Parties as Data Controllers

Where the third party seeks sharing of data controlled by the Department for the third party's own purposes (for example, where the third party requires the data to fulfil its own statutory function), the third party will also become a data controller of that data, for the purposes that it will process the personal data. It will be required to specify these in the agreement request.

Any agreement to supply of personal data requested by the third party is limited to the third party processing the data only for the specified purposes that are agreed. Where it is exercising a statutory function, the third party will be required to specify the function it is exercising and the statutory instrument under which it is exercising that function.

### 4.2 Data Processors

A data processor is any person or organisation that processes data on behalf of a data controller. A data processor can only act on the instructions of the data controller or controllers.

#### 4.2.1 Third Parties as Data Processors

When a third party is required to process personal data for and on behalf of the Department (for example, where there is a contract between the Department and a third party to undertake a survey of learners on the Department's behalf), the third party enters into this agreement as a data processor in respect of such data, and agrees to process data solely according to instructions as set out in the contract and under the agreement.

### 4.2.2 Other 'subsidiary' parties as Data Processors

Any further parties processing data on behalf of a third party described under section 4.2.1 above, for purposes determined by the SFA under a contract between the Department and a third party described under section 4.2.1, will only be a data processor of the data. This includes any external contractor or consultant engaged by a third party.

Where personal data is provided by the SFA, written contractual conditions between the third party, as described in section 4.2.1 and any other party described in this section must regulate how the data are used and what they are used for in accordance with this agreement.

As a minimum, these conditions shall require that the third party:

- agrees only to process personal data in accordance with the disclosing organisation's instructions and only within the purposes and to the extent that the Department has agreed for the data to be processed by the third party
- takes appropriate technical and organisational measures to keep data secure at all times
- agrees to delete the data securely by the agreed date, or when the use is fulfilled, if sooner
- notifies the SFA of any potential or actual breach of security in relation to the shared data as soon as possible and, in any event, within three working days of identification of any potential or actual loss of the shared data
- accepts that they are a Data Processor only in regard to the agreed data
- agrees that data will be kept confidential and not be disclosed to any other parties.

The Department reserves the right to request a copy of the written contractual terms and conditions between a third party as described under section 4.2.1 and any other third party relating to any processing of the shared data.

### 4.3 Commissions of Work

Any third party using the data to produce work for another party must still only process the data supplied by the SFA as a processor and in accordance with any agreements made with the Department.

## 5. Conditions of data supply

Personal data held by the SFA and shared with a third party are subject to the following conditions.

### 5.1 Annual review and retention of data by third parties

In accordance with the Data Protection Act 1998, personal data should only be processed for as long as is necessary. Requests to share data should be limited accordingly and retained for no longer than 12 months under this agreement, unless otherwise specified. Justification for processing of the data beyond one year is required.

The SFA recognises that third parties may wish data to be retained for further use in the future. These parties may request permission, using this agreement, to keep data for specified purposes in anticipation of further use. At the end of the specified period, the data must be securely deleted unless further agreement is given.

### 5.2 Sharing with other third parties

Personal data must not be shared by the third party with other organisations or individuals without the prior written agreement of the Department. This includes consultants, contractors, sub-contractors and other agencies.

### 5.3 Processing only for agreed purposes

Data shall only be processed (including stored) for the purpose(s) for which the request has been made, and must be deleted once that purpose has been fulfilled.

Third parties must seek agreement under a new Data Sharing Agreement for processing the data for purposes other than previously agreed.

### 5.4 Data Protection Registration (notification to the Information Commissioner's Office)

Where the Department agrees to share data with a third party which will be processing the data for its own purposes, the third party will become a data controller in relation to the shared data and the Department will require the third party to provide details of an appropriate and valid entry in the Register of Data Controllers section of this agreement. The Register of Data Controllers is managed by the UK Information Commissioner's Office (ICO), and it is mandatory for most organisations handling data as a data controller to maintain a valid registration.

Failure by such third parties to include a valid registration number and / or be registered for suitable purposes (i.e. unless they are exempt from registration) will result in any requests being rejected. The purposes for which an organisation must be registered may vary depending on the proposed use the data, and so a definitive list cannot be provided.

### 5.5 Mortality

It is important that anyone dealing with personal and sensitive data, understands that the Data Protection Act 1998 does not cover deceased persons.

Any research or surveys using Agency information should always be done via a dataset of individuals that has been checked for deceased people, to avoid unnecessary upset to the deceased's family.

"Mortality files" are available to purchase for organisations who wish to do regular checks on their datasets, and the Agency recommends the use of these.

### 5.6 Data matching

Data are provided on the understanding that they will not be matched to any other data, even on depersonalised or aggregated datasets, unless otherwise agreed with the Department.

Where any new data has been generated by a third party as a result of matching or other analysis, and which is dependent upon the continued processing of data supplied by the Department, the new data may only be kept for the length of time agreed and then securely destroyed.

### 5.7 Data security

All third parties entering into this agreement and processing personal and sensitive personal data must have in place prior to receipt of the data, and continue to take, appropriate technical and organisational measures against unauthorised or unlawful processing of personal data, and against accidental loss, destruction or damage to personal data.

All organisations must follow the advice and guidance contained within the government's 10 Steps to Cyber Security:-

https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary

All organisations must pay particular attention to the following areas:-.

- Appropriate technological and security measures are applied, ensuring that all equipment/devices are up to date "patched".
- Secure physical storage and management of non-electronic data
- Password protected computer systems, ensuring that passwords are of the appropriate length and complexity, and require regular renewal.

- Restrict access to data to those that require it, and take reasonable steps to ensure the reliability of employees who have access to data, for instance, ensuring that all staff have appropriate background checks.
- Appropriate security on external routes into the organisation; for example, internet firewalls and remote access solutions.

### 5.7.1 Destruction of data

Once the data have been used for the purposes for which they were required, the data should be deleted, using appropriate software where necessary, unless there is an agreement with the Department that the data may be retained for longer. The Department requires third parties to delete data securely to a standard that accords with the protective marking that applies to the data.

### 5.7.2 Security incidents

The Department requires the third party to advise the SFA of any potential or actual losses of the shared data as soon as possible and, in any event, within three working days of identification of any potential or actual loss, whether in relation to its own processing of the data or in relation to data processed on its behalf, in order that the Department can consider what further action is required in relation to such an incident and the continued and future sharing of data.

All third parties entering into this agreement and who will be data controllers of the shared data will be required as part of this agreement to provide details of an appropriate valid entry in the Register of Data Controllers. Notification requires that the data controller must provide to the UK Information Commissioner a general description of the measures it will take for the purposes of protecting against unauthorised or unlawful processing of personal information and against accidental loss or destruction of, or damage to personal information.

## 5.8 Suppression of personal data

Where the SFA shares personal data with a third party, groups identified as having fewer than five individuals as a result of data analysis should not be published, except with the prior agreement of the Department. Further guidance may be issued regarding suppression to prevent identification.

## 5.9 Rights to inspection and withdrawal of data sharing

If the Department shares data with a third party for the purposes of the third party processing data as a data controller, the Department reserves its rights under contract between the Department and the third party to inspect arrangements for the processing of the shared data and withdraw agreement to the shared data where it considers a third party (or other parties with whom it has shared the data) is not processing the data in accordance with this agreement.

### 5.10 Data Subject Access Rights

Individuals have a right to see what data are held about them, and to know why and how it is processed.

The Department as a data controller has an obligation to respond to these requests. Requests made of a third party who becomes a data controller should be honoured by them under the terms of the Data Protection Act 1998.

Third parties with whom the Department shares data for the purposes of processing on behalf of the Department should refer such requests in accordance with its contractual obligations with the Department.

### 5.11 Transfer of data outside of the UK and EEA

Data shared with third parties will not be transferred outside of the UK unless explicitly agreed by the Department.

The Department has an obligation to seek authorisation from central government for transfer of data outside of the UK.

The Data Protection Act 1998 bans the transfer of personal data to a country or a territory outside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of the data subjects in relation to the processing of their personal data.

When the Department collects personal data from an individual such as a learner, it does not inform them that their data will be transferred outside of the European Economic Area.

When the SFA shares data under this data sharing agreement, the other parties to the agreement agree that no data will be transferred outside of the UK, unless the SFA explicitly agrees to the transfer.

### 5.12 Prohibition of data for other purposes

#### 5.12.1 Commercial purposes

Personal data will not be released or sold for commercial purposes and must not be used for such purposes.

Data which may provide the requestor with commercial advantage may be either refused, or provided on the condition that other organisations that may be affected by the release of these data are also provided with the information.

#### 5.12.2 Processing incompatible with Privacy Notice

The Department will not share data for uses incompatible with the purposes in a Privacy Notice it has issued. This includes, but is not limited to.

- Speculative Investigations – where organisations wish to trawl for names and information without proper cause or purpose
- Snooping – where organisations wish to act on merely a suspicion of information that might be of use to them, with no satisfactory justification.

### 5.13 Changes to agreed processing of personal data

The Department must be kept fully informed of the processing of any personal data it shares with third parties to enable the Department to ensure it is meeting its own obligations in respect of the data.