Withdrawn

This publication has been withdrawn

The European Social Fund (ESF) 2007 to 2013 programme has now closed.

This publication is no longer current and is not being updated. It is published here for reference only.

2007 - 2013 ACTION NOTE

Reference Number	**066/12**
Date Issued:	**10 January 2012**
Review date:	**31 December 2013**

Data Protection

WHO

CFO's, Intermediary bodies and all ESF direct bid projects including Higher Education projects in Cornwall, all Technical Assistance projects and all Innovation, Transnationallity and Mainstreaming (ITM) projects.

WHAT

This action note is to remind all ESF providers of the importance of ensuring that proper data security procedures are in place and that all provisions of Data Protection legislation are adhered to. This action note applies mainly to non-CFO funded activity, because CFOs will already have policies and guidance in place.

CLEARED

Ian Chapman

Head of the Managing Authority

Background

1. DWP attaches a great deal of importance to the protection of data that the department holds and ensuring compliance with data protection legislation. For information on Data Protection issues please see www.ico.gov.uk

2. This applies in the same way to all outside organisations that hold contracts with DWP or any of their sub contractors. Any breach of Data security is regarded as extremely serious and may have significant consequences if it is concluded that organisations have not instituted robust data security procedures.

3. Unfortunately there has been a significant data loss from an ESF project. This data loss is deemed so serious that it has been referred to both the Secretary of State and the Information Commissioner.

4. The data loss concerned occurred when an unencrypted memory stick was used to transfer extremely sensitive personal information about participants on both a domestic DWP programme and the ESF project. The information was transferred to an evaluator undertaking research. This memory stick has been subsequently lost.

Action

5. All ESF contractors are responsible for ensuring that ESF data is held securely and that information is not corrupted or lost. All contractors must ensure that they have a data handling protocol and a robust data security process in place

6. Participant information is extremely sensitive and ESF contractors must ensure that any system that is used to hold data (including back up data) is a secure system. This means that any portable external data storage device used for holding ESF data must be encrypted and used at all times if data needs to be transferred. Failure to do so could result in prosecution. The Information Commission's Office can impose fines of up to £500,000 for breaches of these rules.

7. One of the easiest ways to avoid problems is to ensure that organisations only move and share data when it is absolutely necessary. Data which has been anonymised by the removal of sensitive personal information will often be sufficient for analysis and evaluation purposes.

8. Contractors must take reasonable steps to ensure the reliability of any staff that has access to participant data.

9. ESF data must be held separately from any other data.

10. In terms of the Data Protection legislation, DWP (ESFD) is the data controller for all data (including match data) relating to ESF provision.

11. Any loss of data must be reported to ESFD immediately as the Data Controller. It is our responsibility to make a decision on each case as to whether to report the loss to the Information Commissioner.

Contacts

Steve Briggs

Managing Authority – ESFD