European Union European Social Fund Northern Ireland

Department for the Economy www.economy-ni.gov.uk

Northern Ireland European Social Fund Programme 2014 - 2020

ESF Promoter Guidance on GDPR and Data Retention ESF Projects Funded under Call 3 of Priority Axis 1 & 2 - April 2018

Project Delivery Branch

Guidance Note 4

Version 1 – April 2022

Review Date – As required in 2022/2023

Content

1 INTRODUCTION

The European Commission (EC) regulations require member states to collect and store data on each participant that benefits directly from ESF support. This has a number of implications in respect of data collection, data storage and the reporting of indicators. This document has been produced by the Northern Ireland ESF Project Delivery Branch (ESF PDB) to provide practical guidance to ESF operations (projects) on data collection and validation of participant eligibility and performance. The content of this document complies with EC guidance issued in May 2016.

2. PROTECTION & STORAGE OF PERSONAL DATA

2.1 Guidance to Projects on General Data Protection Regulations (GDPR)

The Data Protection Act (DPA) 2018 came into effect on 25 May 2018. It sets out rules for processing "personal data", particularly that held on computers, but it also applies to some manual records. The essential features of the DPA are that it:

- requires organisations holding personal data to notify the Information Commissioner's Office (ICO) in broad terms of what they hold;
- requires organisations holding personal data to comply with the data protection principles; and
- provides for individuals to be told, on request, what data is held on them and gives them the opportunity to correct any errors.

In practical terms, personal data means any information relating to an identifiable living individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Anyone who holds and processes personal data must comply with the data protection principles and the other requirements of the DPA. This means that anyone in a Project who is responsible for personal data must ensure that it is processed in a way that conforms to data protection legislation, and is registered, where appropriate, with the ICO.

Personal data should be:

(a) processed lawfully, fairly and in a transparent manner,
(b) collected for specified, explicit and legitimate purposes,
(c) adequate, relevant and limited to what is necessary,
(d) accurate and where necessary kept up to date,

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed, and

(f) processed in a manner that ensures appropriate security of the personal data - data must always be held securely.

All Projects must be fully aware of, and abide by, their duties and responsibilities under the Act. Projects are required to collect and use personal data for a wide range of people in order to carry out their business and provide their services. These may include participants, current, past and prospective employees. Projects must ensure that all personal information, however it is collected, recorded and used, and whether it is on paper, in electronic records or recorded in other formats, on other media, or by any other means must be handled and dealt in line with the Act.

Projects should ensure that all their employees take responsibility for handling of personal information correctly through appropriate training and good management practices. All new staff should be made aware of their responsibilities during induction.

All projects should have a Data Protection Policy, approved by a senior member of staff, which sets out how the Project will meet the data protection principles, listed above, and the other requirements of the DPA.

All projects should also have a Data Breach Policy. A data breach is a breach of security leading to the destruction, loss, alternation, unauthorised disclosure, or access to, personal data. A breach is more than just losing personal data. If there is a data breach in your Project you should notify the Performance Monitoring mailbox immediately at esfperformancemonitoring@economy-ni.gov.uk Staff in the Performance Monitoring Team will get advice on the best way to handle the breach from staff within the Department's Information Management Unit.

Projects must ensure that access to personal data is only available to those staff within the organisation who need to see it. User names and passwords for the ESIF database must only be provided to essential staff and these must not be written down. Hard copies of documents must be security stored. Periodic checks on record security should be carried out.

In accordance with Article 140 CPR, beneficiaries must ensure that all documents relating to each operation, its implementation and financing are retained until 31 December 2030 or otherwise instructed by the Managing Authority. However, Projects must securely dispose of all hard copies of documents when they upload them to the ESIF database.

2.2 General Data Protection Regulation (GDPR)

GDPR came into effect on 25 May 2018 and the collection and storage of personal data on participants by operations must comply with these regulations in accordance with Article 140 CPR. This is not intended to be a definitive guide to the GDPR, however projects should be aware of 4 key elements of the regulation:

- Privacy Notices
- Conditions of Consent
- Right to Erasure
- Data Minimisation.

2.3 Privacy Notices (PN)

Being transparent and providing accessible information to individuals about how their personal data will be used is a key element of the GDPR. The most common way to provide this information is through a PN. Letters of Offer set out the roles and responsibilities of the beneficiaries and provides a template which operations may find useful to develop a clear and effective privacy notice. For all enrolments in Call 2, projects will be obliged to provide participants with a privacy notice which will let them know what will happen with their personal data. A copy of a project's privacy notice will be asked for during on the spot checks.

2.4 Protection of Personal Data

As data controller PDB require assurance that personal data collected from participants is held securely and protected from exposure or loss.

The following controls whilst not exhaustive represents good practice in ensuring the security of participant's personal data and should be shared with all staff with responsibility in this area.

- The enrolment of participants should be carried out in a secure environment and not in a public office or reception. This will ensure that others do not overhear participant's personal information.
- Personal data on participants should be stored in locked, proof cabinets and not be left unattended at workstations or public areas. This is to ensure that personal data does not fall into the wrong hands. Hardcopies of personal data should be shredded when entered on to the ESIF database.
- The Personal Training Plan (PTP) contains personal data of participants as outlined in ESF memo 24/18. Where possible the PTP signed by the project

and the participant should be scanned and held electronically for inspection by PDB on request.

- When transporting personal data secure communication methods should always be used e.g. Globalscape (do not use e mail or internal / external post)
- If laptops or other mobile devices are used to store personal data of participants to allow staff to work remotely, only encrypted devices should be used.
- Access to the ESIF database should be securely controlled – Passwords should be held securely and not be written on noticeboards etc.

This list is not exhaustive and projects may and should apply other controls to ensure the security of personal data.

An essential feature of the DPA provides for participants to be told, on request, what data is held on them and gives them the opportunity to correct any errors. Projects should ensure that the individual rights section of the PN provides assurance that participants have the right to have access to their personal data and that they have the right to have inaccurate or incomplete personal data rectified. Requests from participants to access the personal data or to rectify incorrect or incomplete personal data held either on the ESIF database or on other secure system within the organisation should be actioned promptly and have due regard for the security of that data. Access to data held should be done through a verbal interview with the participant, under no circumstances should ESIF database screen prints or hardcopies of other personal records held be given to participants. Changes to inaccurate or incomplete data on the ESIF database should be carried out by the project where appropriate. Any further issues in relation to access or rectification of personal data held on the ESIF database or other documents within the organisation should be addressed to PDB.

2.5 Conditions of Consent

GDPR provides the legal basis for collection and processing of personal data and there is no requirement for written consent from participants. This is not a criterion for eligibility and a participant who fulfils the eligibility criteria for an Investment Priority but requests that their data is not recorded on the database should not be recorded and reported as a participant in monitoring data, but will still be supported.

Right to Erasure & Public Task

The lawful basis for processing personal data under EC legislation is considered to be that of ‘Public Task’, this means that the right to erasure does not apply. Projects should review all documentation provided to the participant to ensure that this is made clear to them when collecting personal data.

As Data Controller it is the Department's responsibility to ensure that all requests for right to erasure are included on a central register and actioned within the legal timeframe. All right to erasure requests should be forwarded to esfperformancemonitoring@economy-ni.gov.uk for action. Projects should not provide any direct response in relation to these requests or any subsequent correspondence.

System Access Requests (SAR)

It is the responsibility of the Data Controller to respond to SAR received. Projects receiving SAR must forward these them to esfperformancemonitoring@economy-ni.gov.uk for action. Projects should not communicate with individuals or organisation in relation to SAR.

2.6 Data Minimisation

Data Minimisation is a key GDPR privacy principle. In short, it states that organisations should collect only the smallest amount of personal data for the shortest period of time and delete it quickly after it has served its purpose. Less data held means less data to protect. Head of PDB guidance in this area can be accessed here.

2.7 ESIF Database

The EU IGJ Managing Authority has established the ESIF database to record and store the operation data necessary for monitoring, evaluation, verification and audit, including data on individual participants. All information in relation to the participant (including personal data) monitoring should be recorded on the "Participant Monitoring Information" form in the performance monitoring module of the ESIF Database. ESIF database access (log-on) should be limited to key operations staff and log on details should be held securely. EC1/19/0308925 is the guidance on inputting information to the database

2.8 Segregation of Data between Operations

The Managing Authority will normally consider an 'operation' to be any single project/activity for which a distinct Letter of Offer setting out the ESF support that has been awarded by the relevant Intermediate Body as well as the objectives/targets for that operation. Beneficiaries with more than one operation should take special care to ensure data recorded for different operations are adequately segregated.