European Union
European
Social Fund

2014-2020 ESF Programme

Action Note

Reference Number:	**018/18**
Date Issued:	**2 May 2018**
Review date:	**1 May 2019**

The General Data Protection Regulation (GDPR) and ESF

Who

All ESF beneficiary organisations, European Social Fund Division and Greater London Authority.

What

The UK is updating its data protection legislation and it will come into force on 25 May 2018. The new laws aim to update current data protection legislation including the Data Protection Act 1998, increase the privacy protection of all UK and EU citizens and reduce the risk of data breaches. It will apply to all public and private organisations processing personal data.

Established key principles of data privacy will remain relevant in the new data protection laws but there are also changes that will affect commercial arrangements, both new and existing, with suppliers.

The new General Data Protection Regulation 2018 ((EU) 2016/679) (GDPR), which forms part of the new data protection legislation, specifies that any processing of personal data, by a data processor, should be governed by a contract with certain provisions included.

All ESF projects and partners should check Annex A: Q&A Briefing on General Data Protection Regulation (GDPR) and ESF to find out more about what action they will need to take.

Projects will need to comply with new GDPR regulations / requirements from 25 May 2018 and should, in the first instance, refer to Annex A: Q&A briefing for further details.

Cleared

Janet Downes / Dan Mumford

Action

Please read the supplementary Annex A: Q&A Briefing on General Data Protection Regulation (GDPR) and ESF.

Contact

For questions please contact: ESF.2014-2020@dwp.gsi.gov.uk

Annex A: Q&A Briefing on General Data Protection Regulation (GDPR) and ESF

Introduction

This briefing note aims to answer the following broad questions.

NB: This note aims to provide a brief overview of GDPR and some of its implications for ESF; it does not constitute formal legal advice. Readers are advised to consult the Information Commissioner's Office (ICO) website at: https://ico.org.uk/ and/or legal advisers in relation to any legal / technical queries they may have with regards to GDPR.

What is the General Data Protection Regulation?

The General Data Protection Regulation (GDPR) is a new, Europe-wide law that replaces the Data Protection Act 1998 in the UK. It is part of the wider package of reform to the data protection landscape that includes the Data Protection Bill.

The EU's GDPR legislation aims to "harmonise" data privacy laws across Europe as well as give greater protection and rights to individuals.

What is new?

- New rights for people to access the information organisations / companies hold about them.
- New requirements for data controllers and data processers to improve data management.
- A new regime of fines.

What about Brexit?

The UK's new Data Protection Bill largely includes all the provisions of the GDPR. There are some small changes but our own law will essentially cover GDPR requirements post-Brexit.

What information does the GDPR apply to?

The GDPR applies to 'personal data', which means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

When does the new regulation become law?

The GDPR sets out requirements for how organizations will need to handle personal data from 25 May 2018.

Who does the GDPR apply to?

The GDPR applies to data 'controllers' **and** 'processors'.

What is a data controller?

A controller determines the purposes and means of processing personal data. The GDPR places obligations on controller to ensure that contracts with processors comply with the GDPR.

What is a data processer?

A processor is responsible for processing personal data on behalf of a controller. If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach

Can an organisation be a controller and a processer?

Yes – this is possible.

Who is the data controller for ESF personal data – and what data do they control?

Department for Work and Pensions (DWP) ESF Managing Authority is the controller for all personal data required to help deliver the ESF programme under the terms of its ESF Funding Agreement.

Some organisations may collect other / additional data about their participants which is not essential for delivering the ESF programme (and possibly data on other people not supported by ESF). The ESF Managing Authority is **not** the controller for such additional data. In this scenario, individual organisations must ensure they understand and are compliant, with their responsibilities under GDPR, as the data controller. We recommend that organisations undertake their own data audit, to support and demonstrate, decision making in this area.

DWP will not act as controller for personal data that would normally be collected *anyway* by the organisation – regardless of delivering ESF supported activities.

Who is ultimately responsible – the controller or processer?

When processing personal data, you must have a written contract (Funding Agreement) in place between you and the controller, or another legal act must apply.

The contract is important so that both parties understand their responsibilities and liabilities.

Although the controller is ultimately liable for overall compliance with the GDPR and for demonstrating that compliance, processors also have some direct responsibilities and liabilities of their own.

Processers failing to meet any of these obligations, or act outside or against the instructions of the controller, may be liable to pay damages in legal proceedings, or be subject to fines or other penalties or corrective measures.

In terms of data processing – what do I need to do?

Organisations should read and, where appropriate, act upon ICO guidance on action to take in relation to data processing, for example:

- documentation (info audit)
- accountability
- individual rights
- data security

The guidance is available at the following website:

https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/processors-checklist/

Are there any changes to data retention periods?

No, the requirements for data retention in relation to ESF projects are not changing. Further information on data retention is available on GOV.UK at https://www.gov.uk/government/publications/european-structural-and-investment-funds-document-retention

What are the 6 lawful bases for processing personal data?

(i) Consent: the data subject has given clear consent (e.g. opt-in **not opt-out**) for personal data to be processed

(ii) Contract: processing necessary for a contract

(iii) Legal obligation: necessary in order to comply with the law (this does not include contractual obligations)

(iv) Vital interests: required to protect life (e.g. medical records)

(v) Public task: the processing is necessary for performing a task that is in the public interest or official function and has a clear basis in law;

(vi) Legitimate interests: of organisation or third party.

What is the lawful basis for controlling or processing personal data under ESF?

- **Lawful basis for processing personal data in ESF**

  The DWP ESF Managing Authority, will be processing personal data in the ESF programme according to the following lawful basis:

- **Article 6 (1) (e) GDPR**

‘processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller’.

What is the lawful basis for controlling or processing `special category’ data under ESF (e.g. health, ethnicity)?

Article 9(2) (b) GDPR

This article of the GDPR provides DWP with the lawful basis for processing `special category’ (sensitive) data:

“processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of **employment** and **social security** and **social protection law** in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;”

How does the Data Protection Bill (forthcoming “Data Protection Act 2018”) relate to the GDPR?

ESIF legal advisers have explained that the forthcoming DPA 2018 will supplement the GDPR in areas where the GDPR is `silent’ or requires further detail. This means that we will need to comply **with both the GDPR and the new DPA 2018 in terms of processing data**.

In respect of the Article 6 (1) (e) GDPR option, the forthcoming DPA 2018 (currently the Data Protection Bill) sets out further detail and a basis for relying on public functions for processing data (S8 C of the DPA 2018):

Lawfulness of processing: public interest etc.

In Article 6(1) of the GDPR (lawfulness of processing), the reference in point (e) to processing of personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of the controller’s official authority includes processing of personal data that is necessary for:

(a) the administration of justice,
(b) the exercise of a function of either House of Parliament,
(c) the exercise of a function conferred on a person by an enactment or rule of law,
(d) the exercise of a function of the Crown, a Minister of the Crown or a Government department, or
(e) an activity

At the time of writing, the Data Protection Act 2018 (Data Protection Bill) has yet to be passed in Parliament. The numbering of the Articles / Schedules in the current Bill

will change once it becomes an Act. Our guidance will eventually need to include specific references to the Data Protection Act 2018 (once the current Data Protection Bill is passed by Parliament).

Why are we taking this approach?

The DWP privacy notice will be updated on the DWP Personal Information Charter section of Gov.uk and it is likely that this will be considerably expanded. We suggest our partners check the updated website. It will be updated before the 25 May but we do not have a specific date when the updated details will be available to share with partners.

We understand that, although the content of the DWP personal Information Charter will be updated to reflect the new GDPR requirements, the URL for the website will remain the same: www.gov.uk/dwp/personal-information-charter.

Organisations should make use of the new DWP privacy notice in relation to ESF personal data once it becomes available. They should also offer a brief summary of the additional information available on the site and provide a web link to participants which will enable them to access the full site.

Organisations may **also** need to notify their participants of **an additional privacy notice** covering monitoring and evaluation. They should check published guidance on GOV.UK regarding the requirement for all ESF and YEI providers to report and share individual participant contact details to support monitoring and evaluation. This guidance should be updated in time for the GDPR.

What are the implication of ESF's lawful basis as far as individuals' rights are concerned?

ESF participants **cannot claim** the following rights in terms of ESF personal data:

- right to erasure ("right to be forgotten")
- right to portability of their data

What about the individual's `right to object'?

Individuals do have a right to object to their data being processed – although **data subjects need to give 'grounds relating to their particular situation' – *unless* it relates to the processing for direct marketing purposes (Art. 21(2)) which shouldn't apply to ESF**.

The data controller can always decline to accommodate the right to object but would need to demonstrate 'compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims' (Article 21(1)).

What are some of the implications for grant recipients (current and future) delivering ESF?

Existing Funding agreements:

The ESF Grant Funding Agreement definition of Data Protection includes reference to all **applicable laws and regulations.** (see below).

> **"Data Protection Legislation" means** the Data Protection Act 1998, as amended, the EU Data Protection Directive 95/46/EC, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and **all applicable laws and regulations relating to processing of personal data and privacy**, including where applicable the guidance and codes of practice issued by the Information Commissioner.

We have been advised by our legal advisers that because this clause **already captures the GDPR and new Data Protection Act** new funding agreements will **not** need to be issued to replace existing funding agreements. **From 25 May 2018, all existing grant recipients will need to comply with the new GDPR requirements.** Any new or updated FGAs issued after 25 May will have amended clauses which refer to the new legislation (see below).

-

For New / Updated Funding Agreements Issued After 25 MAY 2018:

Any new / updated funding agreements that are issued after 25 May 2018 will have amended wording covering the new GDPR and new Public Data Bill references in the definition section.

The main clause on Data Protection in the Funding Agreement will (be?) to be amended **for GFAs issued after 25 May**; there is one reference which will be removed (see below):

> **" (a)… not Process Personal Data outside the European Economic Area without the prior written consent of the Secretary of State and, where the Secretary of State consents to a transfer, to comply with:**
>
> (i) **the obligations of a Data Controller under the Eighth Data Protection Principle set out in Schedule 1 of the Data Protection**

Act 1998 by providing an adequate level of protection to any Personal Data that is transferred; and

(ii) **any reasonable instructions notified to it by the Secretary of State."**

Privacy notices relating to ESF: Projects will need to make use of DWP's privacy notice as published in the DWP's personal information charter for all ESF personal data only. ESF participants should also be made aware of the contents of the DWP's personal information charter in relation to all ESF personal data held about them (and this should include a web link or similar to the full site). This will be updated to incorporate the new DWP privacy notice before 24 May (it has yet to be amended at the current time of writing) The URL for this will remain the same as the current URL used for the DWP personal information charter (but the content will change as described). The URL is: www.gov.uk/dwp/personal-information-charter.

At the time of writing, it is possible that projects may also need to refer to **an additional privacy notice** that will be covered in the published guidance on the **requirement for all ESF and YEI providers to report and share individual participant contact details to support monitoring and evaluation**.
Any non-ESF data that the project itself is controlling or is processing on behalf of itself or non-DWP controller(s) will require **additional privacy notices to cover that non-ESF data.** (We recommend that you also look at guidelines and good practice on privacy notices provided on the Information Commissioner's Office website).

Published guidance on the requirement for all ESF and YEI providers to report and share individual participant contact details to support monitoring and evaluation: the guidance and the **privacy notice** contained within it will be updated to reflect the requirements introduced by the GDPR. Grant recipients will need to take these new requirements into account. It is possible that a separate and different privacy notice will be required **in addition to** the generic DWP privacy notice referred to above.

In addition, the DWP ESF Managing Authority is updating its **procurement and business processes – such as applications, project inception visits and on the spot visits and related documentation** to reflect the new data protection laws.

ICO guidelines and good practice: we recommend that all organisations check the ICO website for toolkits and good practice that can help them improve data management.

Costs and Liability:

Any work you undertake to be compliant with the new data protection laws, (including our work with you to update existing contracts if ever required), should not incur additional charges to the contract price. Costs incurred by you to become compliant reflect the associated cost of doing business in the UK and EEA. The required changes are not specific to public sector contracts as the new data protection legislation applies to all commercial contracts involving the processing of personal data.

Who can help small organisations?

The ICO phone service is aimed at people running small businesses and charities. To access the new service dial the ICO helpline on 0303 123 1113 and select option 4 to be diverted to staff who can offer support.

Who do I contact if I have queries about GDPR that specifically relate to ESF?

- ESF Managing Authority
- ESF Contract manager
- ESF Co-Financing Authority (if contracted to a CFO)