European Union
European
Social Fund

2014-2020 ESF Programme

Action Note

Reference Number:	**20 /18**
Date Issued:	**24 May 2018**
Review date:	**23 May 2019**

The General Data Protection Regulation (GDPR) and ESF – Additional Advice

Who

All ESF national and local CFOs, IBs beneficiary organisations, European Social Fund Division and Greater London Authority

What

This Action Note provides an update to information provided in Action Note 018/18 – and includes details on action to take with regards to data right of access requests (RARs) (formerly known as subject access requests or SARs) and personal data security breaches.

Cleared

Janet Downes / Dan Mumford

Action

Please read the supplementary Annex A which provides a briefing update on GDPR and ESF.

Please also read about the new arrangements for handling Right of Access (RAR) Requests (Annex B) and Data Security Breaches (Annex C) in the ESF programme.

Contact

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

Annex A: Update to Briefing on the General Data Protection Regulation (GDPR) and ESF

Privacy Notices (a reminder) and the additional need to inform ESF participants of DWP's ESF `right of access' arrangements and ESF data retention arrangements

Action Note 018/18 explained that the DWP privacy notice will shortly be updated on the following website / URL:

https://www.gov.uk/government/organisations/department-for-work-pensions/about/personal-information-charter

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

In addition to this, ESF participants should be notified of their rights with regards to data under GDPR (also **you** should read Annex B). Participants should also be informed about **data retention arrangements in ESF**. Please ensure that your ESF participants are aware of these rights and arrangements and provide them with the following website addresses for Rights of Access Requests (RAR) and data / document retention policy links:

https://www.gov.uk/government/publications/dwp-request-for-personal-information

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/591617/ESF_Guidance_on_document_retention.pdf

Do we need to notify existing ESF participants with regards to DWP's new privacy notice and arrangements for subject access request and data retention policy?

You should try to notify existing participants about the changes caused by GDPR. It is not a requirement that you notify participants on an individual basis, however, you should use existing channels of communication to update as many participants as you can. You do not need to do this by the 25 May 2018, but should try to do this as early as is reasonably possible.

Right of Access Requests (RARs) – formerly known as Subject Access Requests (SARs)

Please read Annex B – which sets out new arrangements for handling data subject access request (SARs)

Action to take if there is a data breach.

Please read Annex C – which explains what a data breach is and the action that needs to be taken in response to a data breach.

ESF Funding Agreements

The DWP ESF Managing Authority will not be automatically replacing existing funding agreements in light of GDPR, since our legal advisers have explained that the existing clauses already `capture' the GDPR requirements (as explained in Action Note 018 / 18).

For brand new ESF projects, wording covering the new GDPR regulations will be included in new Funding Agreements. These will be introduced in the ESF Programme over the coming weeks.

Memoranda Of Understanding (MOU) Update

The DWP GDPR team has advised the DWP ESF Managing Authority, that existing MOUs will need to be updated to include new clauses or references to GDPR requirements. These updates will be informed by a new Public Services Framework which is currently being developed and should be available by the time of the next parliamentary summer recess.

A general reminder to read the ICO website

The ICO website contains a wealth of good practice with regards to data handling and GDPR and all ESF partners are encouraged to check the site regularly.

https://ico.org.uk/

Annex B

Handling ESF Data Right of Access Requests (RARs) and other Individuals Rights under GDPR

1. What is a Right of Access Request (RAR)?

It is a request from an individual who is asking for:

- Confirmation that you are processing their personal data;
- A copy of their personal data
- Other supplementary information (which largely corresponds to the information covered in the privacy notice that they are referred to)

2. How do you recognise a RAR?

See above. It should be noted that a request for access to personal data does not have to include the specific phrase `right of access request' or refer to `Article 15 of the GDPR', as long as it is clear that the individual is asking for their own personal data.

The ICO recommend that staff be trained to understand what a RAR request is – especially those who are `customer-facing'.

3. How can a RAR request be made?

The GDPR does not specify how a valid request must be made. An individual can make a right of access request verbally or in writing. It can also be made to any part of your organisation (including by social media) and does not have to be made to a specific person or contact. Please see below for details of how DWP intends to handle RARs.

4. What arrangements are the DWP and DWP ESF Managing Authority putting in place to handle RARs? What do CFOs / projects etc. need to do?

DWP have set up a central `RAR management gateway' for RAR requests that relate to ESF personal data as well as other personal data that DWP may control /process.

When you are notifying individual ESF participants of the link to the DWP privacy notice that applies to ESF personal data, you should also share the link to the DWP RAR page on GOV.UK address with them (along with the data retention policy link referred to in Annex A above).

Individuals who wish to make a RAR should be encouraged to make their request directly through DWP's online form, on GOV.UK, using the following link:

https://www.gov.uk/government/publications/dwp-request-for-personal-information

Individuals who are unable or unwilling to make their request online, should write to the following address:

Right of Access Gateway Team
Post Handling Site A
Wolverhampton
WV98 2EF

On receipt of the RAR, DWP will log / record the query and will also ask the individual to verify their identity. Where it is reasonable to do so, DWP may ask for some additional information (for example project details) to help find the personal data that is being processed / retained.

If the RAR request is made directly to the CFO / IB / or project, the organisation concerned should forward the request to the DWP ESF Managing Authority who will liaise with the DWP central RAR management Team and take appropriate action. Requests of this nature should be sent to the following email address:

ESF.SUBJECTACCESSREQUEST@DWP.GSI.GOV.UK

DWP's `central RAR management team' will seek contributions from the DWP ESF Managing Authority who will work directly with ESF delivery partners in order to collate the necessary ESF personal data.

It is essential that CFOs and grant recipients maintain clear lines of communication with the ESF Managing Authority when handling SAR requests and fully assist the Managing Authority in searches for personal data. If ESF partners **know** that an individual is making a SAR request they should **notify the ESF Managing Authority** to help them link the participant to the project.

The DWP `central RAR central management team' will: manage the deadlines for the requests; quality assure any final responses that are to be sent to data subjects; and ensure the information is supplied in a suitable format and is suitably redacted. DWP will also maintain a record / log of the SAR request and the timing of the response from the data controller's perspective so that deadlines can be monitored in line with regulatory requirements.

5. **Can an individual make a request directly to the DWP ESF MA?**

Individuals can make their request directly to the DWP Managing Authority if they wish - although **this is not the preferred route**. The MA will still need to notify the central management team of the query and the individual will still be asked to verify their identity etc. There is the added complication that the individual may not identify the project. If you **know** that an individual is going to make a RAR directly to the MA you should notify the Managing Authority of this likelihood.

6. What about deadlines?

RAR requests should be dealt with as soon as possible (and certainly within a month) - rather than the 40 days that were allowed under the 1998 DPA.

7. What about other rights?

All ESF partners' should familiarise themselves with the other rights of the individual as described in the GDPR / ICO guidelines and ensure they have procedures in place to deal with these – since RARs **we may be handling, could incorporate some of these additional rights.**

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

It should be noted that `right to erasure' and `right to data portability' do not apply to ESF participants because of the particular lawful basis under which ESF personal data is being processed.

8. What else do ESF CFOs / grant recipients / projects etc. need to do?

You should update your own procedures and plan how you will handle requests to take account of the new regulations and the DWP's / DWP MA's RAR procedures described above.

ESF partners should also ensure that they take into consideration the relevant guidance as provided in the ICO website:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

Annex C: Personal Data Breaches in ESF – GDPR Requirements

Introduction

This guidance aims to help ESF partners:

- Identify when a data breach involving personal data has taken place;
- Take appropriate action in the event of a data breach occurring

What is a personal data breach?

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransom-ware, or accidentally lost or destroyed. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Examples of data breaches

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

Recital 87 of the GDPR makes it clear that when a security incident takes place, ESF CFOs, IBs and projects must **quickly establish whether a personal data breach has occurred** and, if so, **promptly take steps to address it, including telling the DWP ESF Managing Authority.**

What role do you have?

ESF DWP Managing Authority is the data controller of ESF personal data. CFOs, IBs, Grant Recipients and projects are the data processers. If your organisation suffers a breach, then under GDPR Article 33(2) you must inform the DWP Managing Authority without undue delay as soon as you become aware of the breach. You must keep your own record and copy of the of the breach notification and document it. The Managing Authority will keep its own records of any future data breaches as well.

How much time do we have to report a breach?

You must report a notifiable breach to the DWP MA **as soon as possible**. You must give reasons for any delay. There is a 72 hour deadline for notification.

What information must you include when notifying the ESF Managing Authority (Data Controller) of the data breach?

When reporting a breach, the GDPR says you must provide:

- your full organisation / project details and contact details
- a description of the nature of the personal data breach including, where possible:
- the categories (e.g. staff, participants, etc.) and approximate number of individuals concerned;
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Who do you send the data breach notification to?

You must send your data breach notification to the following address:

ESFDATA.BREACH@DWP.GSI.GOV.UK

What if you don't have all the required information available?

The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. So Article 34(4) allows organisations to provide the required information in phases, as long as this is done without undue further delay..

However, you must **notify the ESF MA of the breach as soon as you become aware of it**, and submit further information as soon as possible. You will also need to **explain why you are unable to supply all of the information required on time**. (The Managing Authority will need to explain this to the ICO).

The ESF Managing Authority expects all partners to maintain **clear and open lines of communication with the MA whilst handling data breaches**. The MA will expect to be provided with named contacts within the CFO / project who can be easily contacted by phone and e-mail. A data breach requires the organisation(s) affected to prioritise adequate resources to help ensure that any data breach can be dealt with promptly and in line with legal requirements.

What else do you need to do?

On becoming aware of a breach, you should also:

(i) act quickly to try to **contain it**, and

(ii) assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

When a personal data breach has occurred, you and the Managing Authority will need to establish **the likelihood and severity of the resulting risk to people's rights and freedoms.** If it's likely that there will be a risk then the Managing Authority is required to notify the ICO; if it's unlikely then it is possible that a decision will be made not to report it. However, any decision not to report to the ICO would need to be justified and the justification should be fully documented by your organisation and the Managing Authority.

What breaches does the DWP Managing Authority need to notify the ICO about?

Any breach that poses risks to an individual's rights and freedoms and which, if not addressed could lead to:

- physical, material or non-material damage to natural persons;
- loss of control over their personal data;
- limitation of an individual's rights;
- discrimination;
- identity theft or fraud;
- financial loss;
- unauthorised reversal of pseudonymisation;
- damage to reputation;
- loss of confidentiality of personal data protected by professional secrecy; or
- any other significant economic or social disadvantage to the natural person concerned.

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.

When do we need to tell individuals about a breach?

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says **you must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible.**

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. Again, you will need to assess both the severity of the potential or actual

impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, you will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. **One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.**

What information must we provide to individuals when telling them about a breach?

You need to describe, in clear and plain language, the nature of the personal data breach and, at least:

- the name and contact details of your data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

Does the GDPR require us to take any other steps in response to a breach?

You should ensure that you record all breaches, regardless of whether or not they need to be reported to the ICO.

Article 33(5) requires you to document the facts relating to the breach, its effects and the remedial action taken. This is part of your overall obligation to comply with the accountability principle, and allows us to verify your organisation's compliance with its notification duties under the GDPR.

As with any security incident, you should investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

What else should we take into account?

Although the following aren't specific GDPR requirements, we may need to consider notifying third parties such as: the police; insurers; professional bodies; or bank or credit card companies who can help reduce the risk of financial loss to individuals.

What happens if we fail to notify?

Failing to notify a breach when required to do so can result in a significant fine up to 10 million euros or 2 per cent of an organisation's global turnover. The fine can be combined with the ICO's other corrective powers under Article 58. So it's important to make sure you have a robust breach-reporting process in place to ensure you detect and can notify a breach, on time; and to provide the necessary details.

Under the GDPR, financial penalties **will not necessarily be limited to the data controller (DWP ESF MA) and organizations acting as data processers may also be fined.**