Building Better Opportunities Essential update January 2022 - Reporting Data Breaches

Reporting Data Breaches

This email is to remind all grant holders that as the Data Controller for BBO all Data Breaches **must be reported to the Managing Authority** using the email address ESFDATA.BREACH@DWP.GOV.UK.

Please note, you should report any data breach to the Managing Authority, not the ICO.

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.** This reference to 72 hours is the **deadline for the MA, as the data controller, to report the incident to the ICO** if necessary, and the time starts as soon as the breach is discovered. Breaches therefore need to be reported to the MA without undue delay as soon as you become aware of these, even if not all of the information is available. This enables the ESF Data Breach Team to escalate the incident to its Security Incident Response Team for a decision on whether it needs to be reported to the ICO, which must happen within 72 hours.

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. 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.

Full details of the process can be found in Action Note 020/18 Annex C.

We also advise all lead and partner organisations to review storage arrangements for both paper and electronic records and carefully consider this in relation to mobile workers, and to ensure staff understand the organisational requirements.