



Building Better Opportunities Essential Update, October 2020, number 2 - GDPR and Clarification on the process for Reporting Data Breaches

GDPR and clarification on the process for reporting data breaches.

Following recent discussions with the MA it has come to our attention that there could be some ambiguity around the timescales for notification of data breaches which we want to clarify. ESF Action Note 020/18 provides guidance on GDPR and the process for reporting data breaches and can be found [here](#).

It has become apparent that one section of the Action Note has caused some ambiguity:

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.**

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.

The Action Note clarifies what is needed if you do not have all the required information.



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.

The MA will be clarifying their guidance, but we wanted to make you aware of this ambiguity now to ensure that any future incidents are reported as soon as you become aware of them. We advise all grant holders to review the Action Note [here](#). Please report all data breach incidents to ESFDATA.BREACH@DWP.GOV.UK and inform your Funding Officer.