

Breach Reporting Procedure



Scope

This procedure applies in the event of a personal data breach under Article 33 of the GDPR – *Notification of a personal data breach to the supervisory authority* – and Article 34 – *Communication of a personal data breach to the data subject*.

The GDPR draws a distinction between a 'data controller' and a 'data processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. Each organisation should establish whether it is data controller, or a data processor for the same data processing activity; or whether it is a joint controller.

Responsibility

All users (whether Employees, contractors or temporary Employees and third party users) of O&M Pension Solutions Ltd are required to be aware of, and to follow this procedure in the event of a personal data breach.

All Employees, contractors or temporary personnel are responsible for reporting any personal data breach to the GDPR Representatives.

Breach Notification - Data Processor to Data Controller

Breaches in the first instance need to be reported to the GDPR team, who will maintain a register of any reported breaches.

O&M Pension Solutions Ltd reports any personal data breach or security incident to the data controller without undue delay if personal data has been exposed. This could be the clients scheme and the clients financial adviser. These contact details are stored on the clients record. O&M Pension Solutions Ltd provides the controller with all of the details of the breach (see 'Breach Notification - Data Controller to Supervisory Authority' for details of the information we will provide).

The breach notification is made by email.

A confirmation of receipt of this information is made by either an email or phone call.

Breach Notification - Data Controller to Supervisory Authority

O&M Pension Solutions Ltd determines if the supervisory authority need to be notified in the event of a breach.

O&M Pension Solutions Ltd assesses whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach, by conducting data protection impact assessment against the breach.

If a risk to data subject(s) is likely, O&M Pension Solutions Ltd reports the personal data breach to the relevant supervisory authority (currently the Information Commissioners Office (ICO)) without undue delay, and not later than 72 hours upon discovery of the breach.

If the data breach notification to the supervisory authority is not made within 72 hours, O&M Pension Solutions Ltd' GDPR Representatives submit it electronically with a justification for the delay.

If it is not possible to provide all of the necessary information at the same time O&M Pension Solutions Ltd will provide the information in phases without undue further delay.

Breach Reporting Procedure



The following information needs to be provided to the supervisory authority:

- A description of the nature of the breach.
- The categories of personal data affected.
- Approximate number of data subjects affected.
- Approximate number of personal data records affected.
- Name and contact details of the GDPR Representatives / GDPR Owner.
- Consequences of the breach.
- Any measures taken to address the breach.
- Any information relating to the data breach.

The GDPR Representatives / GDPR Owner notifies the supervisory authority (currently the Information Commissioners Office (ICO)). Contact details for the supervisory authority are recorded in the Schedule of authorities and key suppliers.

In the event the supervisory authority assigns a specific contact in relation to a breach, these details are recorded in the Internal Breach Register.

The breach notification is made by email.

A confirmation of receipt of this information is made by email.

Breach Notification - Data Controller to Data Subject

If the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, O&M Pension Solutions Ltd notifies the IFA for the data subjects affected immediately.

The notification to the data subject describes the breach in clear and plain language, and will include all details as specified in the 'Breach Notification - Data Controller to Supervisory Authority' procedure.

O&M Pension Solutions Ltd takes measures to render the personal data unusable to any person who is not authorised to access it using encryption.

The data controller takes subsequent measures to ensure that any risks to the rights and freedoms of the data subjects are no longer likely to occur by monitoring any breaches and taking steps to ensure relevant safeguards/ training is implemented to prevent repeat occurrences.

If the breach affects a high volume of data subjects and personal data records, O&M Pension Solutions Ltd makes a decision based on assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder the O&M Pension Solutions Ltd' ability to appropriately provide the notification within the specified time frame. In such a scenario a public communication or similar measure informs those affected in an equally effective manner.

If O&M Pension Solutions Ltd has not notified the data subject(s), and the supervisory authority considers the likelihood of a data breach will result in high risk, O&M Pension Solutions Ltd will communicate the data breach to the data subject by contacting the data subjects financial adviser and issuing a statement on the website.

O&M Pension Solutions Ltd documents any personal data breach(es), incorporating the facts relating to the personal data breach, its effects and the remedial action(s) taken.