# Reporting a Personal Data Breach

**A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.**

- Controllers must report personal data breaches to the Office of Data Protection (ODP) unless the breach is unlikely to result in a risk to the rights of individuals.
- Processors must report data breaches to their respective Controllers.

## The steps below describe how a personal data breach should be reported.

### Step 1

Someone reports the personal data breach to a Controller through phone, email, or in-person communication.

OR

A Controller becomes aware of a personal data breach through internal channels.

### Step 2

The organisation assesses the breach and mobilises to notify the ODP if the severity threshold is met. The person responsible for data protection at the organisation (the Data Protection Officer/DPO or equivalent) follows the steps below without undue delay, and within 72 hours of discovering the breach where feasible.

### Step 3

The DPO navigates to the ADGM Online Registry Solution, and click on the "Data Protection" tab. The Personal Data Breach Form is accessible through here.

Insert screenshot(s)

Insert screenshot(s)

### Step 4

The DPO documents fills in the form with the required details regarding the breach and uploads supporting documents as requested in the form.

### Step 5

After verifying that all of the required information has been provided and/or uploaded accurately, the DPO clicks on submit to complete the initial reporting process.

Insert screenshot(s)

Insert screenshot(s)

### Step 6

The organisation receives an acknowledgement of the submission on screen as well as via email. The Office of Data Protection will review the breach report and you may be contacted for clarification, request for further information, or with guidance on the next steps.

If the breach is relatively minor in terms of risk of harm to the Data Subjects or organisation demonstrates adequately implemented measures to mitigate the risk and prevent future occurrences, the ODP may potentially not respond to the breach report.