ADGM

MANAGING PERSONAL DATA BREACHES

What is 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 that is being transmitted, stored, or otherwise processed

What must you do in case of a personal data breach?

A Data Controller must notify the Office of Data Protection of personal data breaches which are likely to result in a risk to the rights of the individuals without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach

The Data Controller must document all personal data breaches, covering all the facts relating to the personal data breach, as well as its effects and remedial action taken

A Data Processor must notify their respective Controller about a personal data breach without undue delay after becoming aware of the breach

Data breaches can be reported to Office of Data Protection via the **Online Registry Solution**

What should a data breach notification contain?

Nature of the personal data breach

Measures taken or proposed by the Data Controller

Consequences of the personal data breach

Name and contact details of a point of contact where further information can be obtained

Facts relating to the personal data breach, its effects and the remedial action taken

Note:
Where it is not possible to provide all of the information referred to above simultaneously, the information should be provided in a phased-approach without undue delay.

Communicating with Data Subjects regarding a personal data breach

1. When the personal data breach is likely to result in high risk to the rights of individuals, the Data Controller must inform the data subject of the personal data breach

2. Communication with Data Subjects must be in clear and plain language, and where practical, must include recommendations to mitigate any adverse effects

3. Communication with the Data Subject may not be required if you, as the Data Controller, had implemented appropriate technical and organisational protection measures over the data, or if subsequent measures were implemented to ensure the high risk is no longer likely to materialise, or if communication with individual Data Subjects would involve disproportionate effort