SECURITY OF PROCESSING

What is Security of Processing?

Personal data must be processed in a manner that ensures appropriate security of the information. Security of Processing requires that personal data is collected, stored, used, and shared securely by implementing appropriate technical and organisational security measures. These measures help prevent unauthorised or unlawful processing, as well as loss, destruction, or damage to the data.

Who needs to implement Security of Processing?

The obligation to implement appropriate technical and organisational security measures for personal data applies to both Controllers and Processors. The Data Protection Regulations 2021 do not specify any particular security measures, and it is rather the organisation's responsibility to judge what is appropriate in these circumstances, taking into account:

- the nature, scope, context, and purposes of the processing activities
- the current industry best practices and the availability of relevant security products or solutions in the market
- the likelihood and severity of risks to individuals' rights if the security measures are not in place
- the costs of implementing the security measures

What types of security measures should be in place?

Evaluation, testing, and continuous improvement of technical and organisational measures

Measures to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services

Ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident

Ability to perform pseudonymisation, encryption, masking, and access control for personal data

Section 30(1) of the Regulations requires Controllers and Processors to implement "appropriate technical and organisational measures"

Technical measures comprise of physical security measures and IT/cybersecurity measures. These include, but are not limited to:

1

Physical security measures:

- Protection of your buildings and sites, as well as the equipment within, using measures such as alarms, security lighting, CCTV, and security guards
- Access control to the premises, both for staff and visitors
- Shredding of physical documents prior to disposal
- Environmental controls such as fire safety to protect information and systems
- Off-site backups to ensure data is not permanently lost due to a major incident

2

IT/cybersecurity measures:

- Securing your network and information systems with firewalls and anti-malware
- Locking down personal data with access control, encryption, pseudonymisation, and specialised solutions
- Ensuring that documents containing sensitive data are password protected
- Protecting your websites and other online applications and services
- Guarding devices such as laptops and mobile phones with mobile device management solutions and policies

Organisational measures include, but are not limited to:

1 Carrying out an information risk assessment and taking action on any identified risks

2 Building a culture of security awareness across the organisation via regular training and awareness-raising campaigns

3 Designating a person in the organisation to handle information security requirements

4 Ensuring appropriate policies and procedures are in place for data protection

5 Conducting regular audits to ensure measures are effectively implemented

6 Perform due diligence on processors (vendors) to confirm they are implementing the required measures