Accountability

It is now the explicit responsibility of an organisation to be fully accountable for any processing of personal data and to be able to demonstrate compliance with the data protection legislation. Articles 5(2) and 24 of the Applied GDPR impose such obligations.

Organisations need to develop, embed and maintain a culture of data protection in their processing activities, with compliance demonstrably supported from the top of the organisation.

Accountability is a wide-ranging concept including:

- managing privacy effectively through relevant, responsive, and regularly updated, procedures including proportionate safeguards, governance and oversight;
- maintaining relevant records about the processing, including appropriate policies, procedures and security measures;
- the ability to demonstrate to regulators the efficacy of, and compliance with, those procedures etc.;
- the ability to notify the regulator, and/or individuals of personal data breaches.

BEING ACCOUNTABLE

In practical terms, being accountable means that all processing of personal data should be subject to overview, governance, and demonstrable compliance.

- Effective data protection policies and procedures, in particular regarding the security arrangements, together with records of processing activities, will be required in most cases.

- Ongoing review and testing of security arrangements, and compliance with policies and procedures, will also need to be undertaken and recorded. This is not merely a tick-box exercise, however, and organisations must be able to demonstrate, for example, that systems are routinely tested and staff have received appropriate and regular training in the relevant policies and procedures or subsequent updated versions.

- The appointment of an autonomous data protection officer (DPO), as part of effective governance and oversight, is mandated in some cases.

Each of the areas listed below are interdependent and all form part of the concept of **accountability**.

Accountability therefore requires organisations to look at and consider all these areas, in isolation and as a whole, and understand the interdependencies.

Documenting processes and procedures etc. is an integral part of demonstrating how compliance is achieved. In some cases, it is mandatory for certain records to be created and maintained.

The following pages contain suggestions of compliance matters which organisations may take into consideration, examples of the types of documentation which may evidence compliance.

Resources suggested on the following pages are available on the Commissioner's website.

In addition, the European Data Protection Board's guidelines, including those of Article 29 Working Party Guidelines on the GDPR have been formally adopted, can be found at:

https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_en

Further resources are also available, for example on the UK Information Commissioner's website (ico.org.uk) and the Irish Data Protection Commission's website (dataprotection.ie).

Internal governance

CONSIDERATIONS

- Managerial responsibilities
- Data protection officer (DPO)
- Resources
- Employee training
- Processor arrangements

DOCUMENTATION

- Job/role descriptions
- DPO contact details
- Internal data protection policies
- Training records
- Processor contracts

RESOURCES

- Accountability - A questionnaire for senior management
- Data protection officer
- General compliance resources
- Introduction to the new Isle of Man data protection law
- Ten things you need to know and do
- EDPB / Article 29 Working Party Guidelines
    - data protection officers
    - application and setting of administrative fines

Know your data

CONSIDERATIONS

Does the organisation know and understand why all the personal data is currently being processed and how/where that personal data flows?

- Purposes
  - Lawful basis for processing
- Categories of data subjects
- Categories of personal data
  - Identification of special categories of personal data
- Categories of recipients
- Transfers to third countries
- Retention periods
- General description of the risk-assessed security measures
- Details of processors

DOCUMENTATION

- Records of processing activities or similar
- Record of consent where required
- Appropriate safeguards for international transfers

RESOURCES

- Know your data - Map the 5 W's
- Records of processing
- General compliance resources
- Introduction to the new Isle of Man data protection law
- EDPB / Article 29 Working Party Guidelines
  - Consent

Compliance with principles

CONSIDERATIONS

How well placed is the organisation to ensure that the processing of personal data complies with the principles?

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

DOCUMENTATION

- Principles compliance procedures
- Transparency information
- Records of processing activities or similar
- Record of consent where relevant
- Retention and destruction policy
- Technical and organisational measures
  - E.g. *"How to…"*procedure notes or guides for staff to follow to ensure personal data is processed correctly

RESOURCES

- Principles
- Transparency
- Records of processing
- General compliance resources
- Introduction to the new Isle of Man data protection law
- EDPB / Article 29 Working Party Guidelines
  - Transparency
  - Consent

Compliance with rights

CONSIDERATIONS

How well placed is the organisation to comply with the rights of individuals?

- Transparency
- Access
- Retention
- Data portability
- Restriction of processing
- Rectification
- Erasure
- Objection to processing
- Subjection to automated decision making and profiling

DOCUMENTATION

- Rights compliance procedures
- Transparency information
- Records of processing activities or similar
- Record of consent where relevant
- Retention and destruction policy
- Technical and organisational measures

RESOURCES

- Rights and remedies
- Transparency
- Records of processing
- General compliance resources
- Introduction to the new Isle of Man data protection law
- EDPB / Article 29 Working Party Guidelines
    - Transparency
    - Consent
    - Automated decision-making and profiling
    - Right to data portability

Risk to individuals

CONSIDERATIONS

What risks to individuals, including the risks to their rights and freedoms, could the processing cause?

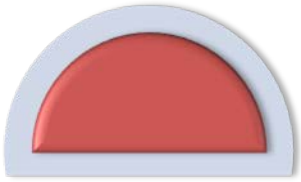
- 'risky' processing
- 'compatible' purpose for processing
- Special categories
- Reliance on 'legitimate interests'
- International transfers
- Likelihood and severity of risks
- Accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data
- Personal data breaches
- Processors
- Employee monitoring

DOCUMENTATION

- Records of processing activities or similar
- Internal policies and procedures
- Principles compliance procedures
- Technical and organisational measures
- Processor contracts
- Risk assessments
- Data protection impact assessments
- Appropriate safeguards for international transfers

RESOURCES

- Rights and remedies
- Principles
- Transparency
- Records of processing
- Data protection officer
- General compliance resources
- Introduction to the new Isle of Man data protection law
- EDPB / Article 29 Working Party Guidelines
    - Data protection impact assessments
    - Personal data breach notification



Technical and organisational measures

CONSIDERATIONS

Measures should be based on the risk to individuals and take into account the nature, scope, context and purposes of processing.

- Purposes for processing
- Special categories
- Encryption
- Pseudonymisation
- Ongoing confidentiality, integrity, availability and resilience of processing systems and services, including regular testing of the effectiveness of measures
- Access control
- Codes of conduct/certification
- Privacy by design and default
- Personal data breach identification and management
- Data protection impact assessment (DPIA) for new processing/ prior consultation with authority if required
- Insider threats

DOCUMENTATION

- Records of processing activities or similar
- Principles compliance procedures
- *"How to…"*procedure notes or guides for staff to follow to ensure personal data is processed correctly
- Processing risk evaluations
- Retention and destruction policy
- Information security framework - i.e. policy, controls and operating procedures
- Physical security framework - i.e. policy, controls and operating procedures
- Incident response plan
- Personal data breach policy and response plan
- DPIA where necessary
- Adherence to other standards, such as ISO27001

RESOURCES

- Rights and remedies
- Records of processing
- Data protection officer
- General compliance resources
- EDPB / Article 29 Working Party Guidelines
  - Data breach notification
  - Data protection impact assessments

Example of Accountability Model

The individual elements of accountability must also be considered as a whole; documentation developed for one particular element may, in turn, refer to documentation pertinent to other elements. For example, technical and organisational measures may refer to the documentation for internal governance, risk to individuals etc., whilst compliance with principles documentation may refer to the 'know your data' documentation.

Regular monitoring, review and revision is required to ensure that processes, procedures and documentation remain fit for purpose, reflect the realities of the processing undertaken, and are adhered to by staff, processors and others. Accountability is, therefore, a continuous process of evidencing compliance and not a one-off exercise. An example of an accountability model is set out below.

Example of Accountability Model

Pub: November 2019