A closer look at Accountability
Accountability

It is now the explicit responsibility of organisations to be accountable and demonstrate compliance. This will require organisations to develop and embed a culture of data protection into their processing activities, with compliance supported, demonstrated and led from the top.

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 this means that all processing of personal data should be subject to overview and governance.

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, as part of effective governance and oversight, is mandated in some cases.

All these requirements apply to controllers; many requirements, such as the appointment of a DPO and maintenance of records, apply to processors also.
Accountability

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

Each of the areas listed below are interdependent and all form a part 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, together with links to the relevant Commissioner’s compliance resources and Article 29 Working Party Guidelines available at the date of publication.
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
- A closer look at data protection officer
- Improve practice
- General compliance resources
- Getting ready for the new data protection laws - guide for small businesses, charities and voluntary organisations
- Ten things you need to know and do
- Article 29 Working Party Guidelines
  - data protection officers
  - application and setting of administrative fines
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
- A closer look at records of processing
- General compliance resources
- Getting ready for the new data protection laws - guide for small businesses, charities and voluntary organisations
- Article 29 Working Party Guidelines
  - Consent
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

RESOURCES

- A closer look at principles
- A closer look at transparency
- A closer look at records of processing
- General compliance resources
- Getting ready for the new data protection laws - guide for small businesses, charities and voluntary organisations
- Article 29 Working Party Guidelines
  - Transparency
  - Consent
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

- A closer look at rights and remedies
- A closer look at transparency
- A closer look at records of processing
- General compliance resources
- Getting ready for the new data protection laws - guide for small businesses, charities and voluntary organisations
- Article 29 Working Party Guidelines
  - Transparency
  - Consent
  - Automated decision-making and profiling
  - Right to data portability
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

- A closer look at rights and remedies
- A closer look at principles
- A closer look at transparency
- A closer look at records of processing
- A closer look at data protection officer
- General compliance resources
- Getting ready for the new data protection laws - guide for small businesses, charities and voluntary organisations
- Article 29 Working Party Guidelines
  - Data protection impact assessments
  - Personal data breach notification
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
- 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

- A closer look at rights and remedies
- A closer look at records of processing
- A closer look at data protection officer
- General compliance resources
- Article 29 Working Party Guidelines
  - Data breach notification
  - Data protection impact assessments
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.
Resource URLs

The following URLs were correct at the date of publication:

Information Commissioner's GDPR guidance can all be found in the General Data Protection Regulation Library:


Article 29 Working Party Guidelines:

http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360