information commissioner
Barrantagh Fysseree

Data protection compliance

Part 2: Accountability -

A questionnaire for senior management

Information is an important and valuable asset to any organisation. **Personal data** may be used for many different reasons, for example staff administration, the provision of goods or services to customers, marketing strategies, prevention of money laundering, a revenue stream etc.

Complying with the data protection legislation

The exercise of proper control and management of **personal data** is fundamental to ensure, and be able to demonstrate, compliance requires both personnel and financial resources.

Taking a positive approach, and embracing compliance with the data protection legislation, will improve customer trust, records management and business opportunities, such as those associated with the digital economy.

Using this resource

This resource is intended to be a non-legal tool to assist in the creation of an inventory of personal data processed, map the processing of personal data and analyse the legal basis of the processing.

Staff at all levels should be involved to establish what processing occurs – front line staff may well have a different experience to that of senior management.

In-depth knowledge of the data protection legislation is <u>not required</u> to use this resource.

However, an honest analysis is required, and if the answer to a question is "Don't know" or "Not sure" – write that down.

The more honest and comprehensive the analysis is, the easier it will subsequently be to identify processing that may require review and evaluation against the data protection principles and whether/how the accountability and risk-based security requirements are to be implemented. (Further resources on these areas are available on our website)

NOTE:
The data protection legislation does not apply to data that is anonymised in such a way that an individual can no longer be identified from the information on its own.

This resource is in five sections:

Questions may require more than one response, depending on the size, scale and structure of the business. For example, larger businesses may have separate client administration, HR, and IT sections each with varying obligations, policies and procedures.

This resource has been developed from a questionnaire produced by the European Data Protection Supervisor (EDPS) in June 2016, as part of its GDPR 'Accountability Initiative' for the European Union institutions (for which the EDPS is the regulatory body).

https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Accountability_initiative

Section 1 – Data Protection management and governance

Responsibility at the highest level for monitoring implementation and assessing, and demonstrating, the quality of the implementation to external stakeholders and supervisory authorities

Data Protection Activity	**Assign data protection responsibility to Data Protection Officer (if appropriate)** Articles 37 to 39		
Question	Whilst senior management remains ultimately responsible for compliance, has responsibility for monitoring data protection compliance been formally assigned to a DPO?		
Response *Examples include:* *If a DPO is needed, what has been done about it?* *If a DPO is not needed, why not?*		**Evidence** *Examples include:* *How and by whom were they appointed?* *Date of appointment?* *Duration of office?*	
Response created by:	[Department/division/section name where appropriate]	**Date**	

Data Protection Activity	**Assign data protection responsibility throughout the organisation** Articles 24, 32		
Question	Have data protection responsibilities been identified in operational units, sectors and specific roles within the organisation?		
Response *Examples include: Which roles/areas? Who? How was this determined? Are staff aware of their role in protecting personal data?*		**Evidence** *Examples include: Job descriptions, organogram, minutes*	
Response created by:	[Department/division/section name where appropriate]	**Date**	

Data Protection Activity	**Enable communication among staff accountable for data protection** Article 39		
Question	Do DPO and senior management communicate and work together for ensuring data protection compliance?		
Response *Examples include: Description of reporting mechanisms, communications channels in place*		**Evidence** *Examples include: Policies, procedures, job descriptions, organogram, minutes*	
Response created by:	[Department/division/section name where appropriate]	**Date**	

Data Protection Activity	**Report on data protection management in the organisation** Article 39		
Question	Does the DPO regularly report directly to the highest level of management?		
Response *Examples include: Frequency, reporting lines*		**Evidence** *Examples include: Policies, procedures, meeting minutes*	
Response created by:	[Department/division/section name where appropriate]	**Date**	

Section 2 – Documentation relating to operations processing personal data

Transparent internal data protection and privacy policies, approved and endorsed by the highest level of management

Data Protection Activity	**Integrating data protection into the access to and processing of personal data required in the workplace**		
Question	Do you have policies and procedures for the protection of personal data used in the workplace? In particular, is there internal practical guidance for staff to follow for jobs or functions that involve the processing of personal data?		
Response *Examples include: What policies and procedures are there? Where are they available? Are they regularly reviewed and updated? Do you have separate policies for differing business areas?* *Are they applied/followed?*		**Evidence** *Examples include: Policies, procedures, review schedules, staff training schedules. Internal practical guidelines*	
Response created by:	[Department/division/section name where appropriate]	**Date**	

Data Protection Activity	**Integrating data protection into the use of IT devices**		
Question	Do you have policies and procedures for the protection of personal data in the use of mobile devices/BYOD for work-related purposes?		
Response *Examples include: What are they? Where are they available? Are they regularly reviewed and updated? Do you have separate policies for devices issued by the organisation and BYOD? Are they applied/followed?*		**Evidence** *Examples include: Policies, procedures, review schedules, staff training schedules*	
Response created by:	[Department/division/section name where appropriate]	**Date**	

Data Protection Activity	**Integrating data protection into the use of IT infrastructure**		
Question	Do you have policies and procedures for the protection of personal data in the use of IT infrastructure for personal purposes?		
Response *Examples include: What are they? Where are they available? Are they regularly reviewed and updated? Are they applied/followed?*		**Evidence** *Examples include: Policies, procedures, review schedules, staff training schedules*	
Response created by:	[Department/division/section name where appropriate]	**Date**	

Data Protection Activity	**Integrating data protection into practices for monitoring employees' communications**		
Question	Do you have procedures to integrate data protection into communications monitoring practices, such as the personal use of e-mail, internet and telephone?		
Response *Examples include: What are they? Where are they available? Are they regularly reviewed and updated? Are they applied/followed?*		**Evidence** *Examples include: Policies, procedures, review schedules, staff training schedules*	
Response created by:	[Department/division/section name where appropriate]	**Date**	

Section 3 – Managing information security risks

Transparent internal data protection and privacy policies, approved and endorsed by the highest level of management

Data Protection Activity	**Maintain an information security policy** **Article 32**		
Question	Do you have an information security policy to protect personal data?		
Response *Examples include: Does the policy identify the level of risk to the individual posed by the processing? Level of security? System and data resilience? Actions to maintain access in the event of a technical or physical incident? Regular testing and evaluation of measures?*		**Evidence** *Examples include: Security assessments, evaluations ,policies, procedures,*	
Response created by:	[Department/division/section name where appropriate]	**Date**	

Section 4 - Managing data breaches and other incidents

Procedures for reporting and redressing personal data breaches and other information security/cyber security incidents

Data Protection Activity	**Maintain a documented data protection incident/breach response protocol** **Article 33 - 34**		
Question	Do you have a personal data breach response procedure?		
Response *Examples include: What is it? Where is it available? Is it regularly reviewed? Who maintains the internal record?*		**Evidence** *Examples include: Policy/protocol/procedures*	
Response created by:	[Department/division/section name where appropriate]	**Date**	

Section 5 – Data protection training and awareness

Informing and training all people in the organisation on how to implement the policies

Data Protection Activity	**Maintain awareness of data protection responsibilities** **Article 5 and/or 39 if a DPO is appointed**		
Question	Do you raise awareness and train staff in the data protection policies and procedures implemented by the organisation, for example to manage information security risks, and in the internal practical guidance for staff?		
Response *Examples include: How often? Means of communication? Where available? Records of training maintained?*		**Evidence** *Examples include: Training records/schedules*	
Response created by:	[Department/division/section name where appropriate]	**Date**	