information
commissioner
Barrantagh Fysseree

Getting ready for GDPR

Part 2:

Accountability -

A questionnaire for senior management

"Accountability is more than simple compliance with the rules - it implies a culture change … organisations and not Data Protection Authorities or Data Protection Officers must demonstrate that they are compliant"

Giovanni Buttarelli
European Data Protection Supervisor

The EU General Data Protection Regulation (GDPR) represents a significant change in the data protection compliance regime for data controllers and data processors.

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.

Transitioning to the new regime

The exercise of proper control and management of **personal data** is fundamental to ensure, and be able to demonstrate, compliance with the GDPR. Transitioning to the new regime will be challenging and require both personnel and financial resources. The level of existing compliance will affect the resources that are required.

However, taking a positive approach, and embracing the changes, will improve customer trust, records management and business opportunities, such as those associated with the digital economy.

Using this resource

Accountability includes:

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

2. Transparent internal data protection and privacy policies, approved and endorsed by the highest level of the organisation's management;

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

4. Procedures for redressing poor compliance and data breaches.

Building on the 'quick review' included in the 'Mapping the 5W's', this resource contains sample questions that senior management and directors can use to assess the basic level of compliance that currently exists within the business. The questions do not go into specific detail, but rather aim to ensure that a business is in control of personal information and its lawful processing.

An honest review should assist a business identify where gaps exist in relation to the new requirements of the GDPR.

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

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

This resource, and the sample questions, will evolve over time. It is intention of the Information Commissioner to review this version by June 2017 to assist businesses in their compliance with the GDPR.

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?		
Response *Examples include: What personal data is processed? 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*	
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 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 redressing poor compliance and data breaches

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?*		**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 to manage information security risks?		
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**	