Data Security – Data Protection Regulation - Ensuring Compliance

Roles and Responsibilities

In the run up to GDPR you will have considered if you needed to formally appoint a DPO – a necessity if:

- You are a public authority or body; or
- Your core activities require large scale, regular and systematic monitoring of individuals; or
- Your core activities consist of large-scale processing of special categories of data or data relating to criminal convictions and offences.

Many organisations chose to ensure that an individual or department has responsibility for privacy activities without the need for a formal DPO appointment. Ensuring that the roles and responsibilities for data protection are well known and documented in your organisation is a key compliance requirement.

ROPA - Record of Processing Activities

Documentation of the processing activities carried out by the organisation is a requirement of Article 30 of the GDPR (both UK and EU) if your organisation has over 250 employees. It is also a requirement for smaller companies if the data you process:

- are not occasional
- are likely to impact the rights and freedoms of individuals; and
- involve special category data or criminal conviction and offence data.

Your ROPA should contain a data map of your systems that contain personal data along with information on the lawful basis of processing, the purposes and methods of processing data, data sharing and data retention policies and procedures.

It is important to ensure that there are regular reviews of this documentation as updates are likely over time.

There is further guidance from the ICO on ROPA best practice.

Policies and procedures

Your policies and procedures should clearly outline roles and responsibilities in your organisation covering a number of privacy related areas:

- Data Protection and records management
- Information security including breaches and incident management
- The provision of information following individual rights requests – such as subject access requests and information notices
- Data Protection by design and default to ensure issues are considered and documented (Privacy impact assessments) when new systems, services, products and processes are implemented, or existing ones amended
- The privacy policy on your website should be reviewed regularly and the date of last update clearly displayed

Supplier Management

It is essential that contracts are in place with organisations that process data on your behalf. Contracts should set out the details of processing including:

- The subject matter of the processing
- Duration of the processing
- Nature and purpose of the processing
- Type of personal data and categories of data subjects
- If any sub-processors are used.

A framework of due diligence checks to ensure that these organisations are operating the appropriate technical and organisational requirements to meet GDPR is needed.

Regularly reviewing the contracts and data sharing agreements you have in place with other organisations is recommended.

Training

Making sure your staff are aware of their responsibilities with regard to processing personal data is key. Induction and refresher training should include information on data protection, potential security threats and your organisation's information governance policies and structures. Monitoring and documenting training completion is an important element in being able to demonstrate your compliance.

Other laws and regulations

There are various other Acts and regulations in the UK which have a bearing on data security. These include:

- Privacy and Electronic Communications Regulations (PECR) 2003 - which cover 'spam' and mass-marketing mailshots. Regulations under the PECR are also issued from time to time. For example, regulations on the use of cookies on websites, and in 2016 to require anyone making a marketing call to display their number
- Copyright Design and Patents Act - amended in 2002 to cover software theft
- There may be other IT standards and regulations applicable: for example, companies processing credit card transactions need to ensure compliance with the Payment Card Industry Data Security Standards (PCI DSS).

Sources and links:

ICO home page for organisations EU GDPR portal - www.eugdpr.org/

For information of users: This material is published for the information of clients. It provides only an overview of the regulations in force at the date of publication, and no action should be taken without consulting the detailed legislation or seeking professional advice. Therefore no responsibility for loss occasioned by any person acting or refraining from action as a result of the material can be accepted by the authors or the firm.