CYBER GDPR GUIDANCE

With the GDPR here, should you be considering Cyber insurance?

At RSA, our experts have been exploring why every business in the UK should consider Cyber insurance. As organisations become more IT reliant we have seen an emerging move to buy Cyber Risks insurance. On May 25th 2018 this requirement became crucial when the General Data Protection Regulation landed, meaning that if you hold personal data, you must abide with this legislation.

Through this guide, we explore what the key features of the legislation mean for you, and your fellow board members, and what you will need to consider.

GENERAL REQUIREMENTS

It is expected to have at the minimum a Data Protection Policy in your organisation making it mandatory for every employee to comply with local and applicable cross-border data protection laws.

DATA PROTECTION REQUIREMENTS

The organisation must be able to demonstrate that it is complying with the following principles:

Personal Data must at all times be:

- processed lawfully, fairly and in a transparent manner, including, where necessary, with the appropriate consent or because it is necessary for the performance of a contract ('lawfulness, fairness and transparency')
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation')
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed ('data minimisation')
- accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay ('accuracy')
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed ('storage limitation')
- processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing ('integrity and confidentiality'). The organisation must comply with all relevant information security and data management policies.

EXPECTED ORGANISATIONAL MEASURES

The organisation must ensure that it complies with the law and regulation relevant to data subjects' rights and can be expected to demonstrate that it has measures of the following nature:

- Documented what personal data it processes and where. This can be done with a personal data inventory or a register of personal data
- Documented how long it is allowed to retain personal data in a retention schedule
- Embedded privacy requirements in the design of new data processing activity
- Assigned roles and responsibilities for the processing of personal data
- Implemented an incident management process catering for personal data breaches in line with local legal requirements and capable of meeting applicable notification deadlines
- Published transparent and easily accessible information about how personal data is processed across the organisation. This applies to the processing of both customer data and employee data
- Where necessary, documented a process to remove, anonymise or pseudonymise data to a level where personal data would not be retrievable
- Documented processes to respond to data subject requests particularly in cases of:
  - right of access in order to confirm whether or not personal data concerning the individual is being processed, and, where that is the case, access to details of the personal data held
  - right to rectification in case of inaccurate personal data being processed
  - right to erasure (right to be forgotten) when the organisation no longer has legitimate grounds to process the personal data
  - right to restriction where a data subject has a legitimate reason to request a suspension of the processing of the individuals personal data
  - right to portability where there is a valid request to transmit personal data in a structured, commonly used and machine-readable format
  - right to object where it is permitted by law, for example, where there is automated decision making including profiling or when data subjects decide to withdraw their consent for activities such as marketing.

An organisation should have processes in place to ensure that all transfers of personal data to third parties and to foreign countries are documented, covered by contracts and compliant with local laws.

Outbound transfers from Europe must be completed in compliance with the GDPR and must rely on the following:

- the transfer is necessary for the performance of the contract between the data subject and the data controller

and

- the receiving country is on the official EU list of adequate countries

or

- the European Commission's standard data protection clauses are in place between the sending and the receiving entity

or

- the data subject has specifically consented to the transfer.

Relationships with third parties can create a dual legal responsibility under the GDPR. Where your organisation are the owner of the customer relationship, and you determine the means and purposes of the data being held, then you will be the 'Data Controller'. Where you enter into a contract with a third party to process or store data on your behalf this creates a party that will be known as the 'Data Processor'. Both will have obligations under the GDPR. Simply asking a third party to process the data does not absolve your organisation from these legal obligations.

Under the GDPR, you must appoint a Data Protection Officer if you are a public authority; carry out large scale systematic monitoring of individuals; or carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

Regardless of whether the GDPR obliges you to appoint a Data Protection Officer, you must ensure that your organisation has sufficient staff and skills to deliver your obligations under the GDPR.

Your Data Protection Officer must:

- inform and advise the organisation of its obligations under data protection laws and manage the associated compliance framework
- have expert knowledge in Data Protection and operate and influence at a sufficient level of seniority, reporting to the highest level of management in the organisation
- act with independence within the organisation such that the organisation does not prescribe how the DPO performs its role
- monitor compliance with the GDPR
- oversee the completion of data protection impact assessments
- cooperate with and act as the organisations' key contact for its Data Protection supervisory authority
- maintain relevant Data Protection documentation (e.g. the supporting materials).

DATA BREACH GUIDANCE

WHAT IS A DATA BREACH?

The definition of a personal data breach in the GDPR is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

A data breach can take many different forms. Some examples include:

- external hacking of your organisation's systems
- loss or theft of data servers containing personal data
- transfer of personal data to an unauthorised third party, either accidentally or maliciously
- personal data being shared (e.g. with a supplier or partner) where this has no legal basis and hasn't been disclosed to the individual on a privacy notice
- loss or theft of servers, laptops, USB sticks and other hardware or paper files containing personal data
- documentation containing personal data being posted or emailed to the wrong address
- personal data being shared on social media channels
- inappropriate access of personal data due to a lack of appropriate internal controls.

WHAT SHOULD YOU DO IF YOU SUSPECT A DATA BREACH?

There must be clear processes in your organisation with defined roles and responsibilities to manage incidents and breaches. Any member of staff who identifies a potential data breach must follow the process immediately. Data breaches must be handled by a trained incident management team.

HOW DOES THE GDPR CHANGE WHAT AN ORGANISATION NEEDS TO DO IN THE CASE OF A DATA BREACH?

The GDPR states that every data breach that is likely to result in a risk to the rights and freedoms of individuals must be notified to the supervisory authority as soon as possible, and **no later than 72 hours after it was identified.**

It is the responsibility of the Data Protection Officer to assess whether a reported incident meets the definition of a data breach and notify the relevant authorities. This is based on a legal assessment of the impact to the individual(s) concerned, and is not related to the technology involved

DO WE HAVE TO TELL OUR CUSTOMERS ABOUT A DATA BREACH?

Only where a breach is likely to result in a high risk to the rights and freedoms of individuals, does an organisation need to notify those concerned directly. The threshold for notifying individuals is higher than for notifying the relevant supervisory authority (a risk to the rights and freedoms).

It is imperative to the success of your business, that you take a multi-faceted approach to your IT risk management, staff training, data management, and disaster and business recovery planning.

In a digital world, can you afford not to insure your virtual risks too?

Speak to your Insurance broker to explore our Cyber Risks insurance product.

UKC05130