What the business should consider

Becoming GDPR compliant

March 2018

Sabre Associates

GDPR – impact and implications

Every organisation within the UK and Europe will need to be compliant with the new data regulations by 25th May 2018, yet estimates show that less than half of organisations consider themselves fully prepared.

It is a startling thought when you consider that in less than 20 weeks, the General Data Protection Regulation (GDPR) is coming into force. This update on the 1998 Data Protection Act is a robust piece of legislation that covers 11 chapters, 99 articles and 173 recitals.

The important thing to note is that GDPR can neither be ignored nor simply assigned to an administrator. Achieving and maintaining GDPR compliance is a business challenge and should not be seen as just an IT or data protection challenge. It is about the way an individual organisation approaches its data protection obligations, and that post 25th May this must be by adopting an approach that is ***privacy by design and default***.

There is a compelling business reason why GDPR should be seen as a business issue; the financial implications are far more onerous than before. The potential financial penalties for non-compliance are fairly substantial, up to €20m or 4% of annual turnover, whichever is larger. This means that making sure your business is compliant with the new regulations around data collection, collation and storage is essential.

Sabre Associates

What does this mean for your firm?

The wide variance in companies within the UK means that there is no 'one-size-fits-all' approach. Each organisation needs to have a tailored approach that takes into account their data approach and practices.

To be able to carry this out it is recommended that five key steps are undertaken; these are:

- ❑ Assess your current approach and practice – identify how GDPR will impact what you are currently doing.
- ❑ Develop and design – identify how to address areas of non-compliance and build into an implementation plan.
- ❑ Capture your new processes – show how the technical and operational measures have been put in place.
- ❑ Embed the culture – adopt the new GDPR compliant ways of working across the company.
- ❑ Monitor the performance – regularly measure how the company is working to ensure GDPR compliance.

What does GDPR cover

The special category data is broadly similar to the concept of sensitive personal data under the 1998 Act. However it now includes:

- Genetic data
- Some biometric data
- Personal data relating to criminal offences and convictions are now included under Article 10. However special category data includes:
- Race
- Politics
- Trade union membership
- Health
- Sex life
- Ethnic origin
- Religion
- Genetics
- Biometrics (where used for ID purposes)
- Sexual orientation

Who needs to be involved

The new GDPR regulations are not simply how you use IT to collect and record data. Far from it; it includes any data, whether electronic or printed, across the organisation and is seen as the responsibility of everyone. This means the assessment of the data held by the organisation (in the first of the five steps) needs to include every department who handles data.

Typically the main areas involved are:

- Marketing: where information is collected and held on targets, clients and prospects from across all the traditional and digital marketing channels.
- HR: where employment related information is held for current employees, past employees and potential employees.
- Payroll: Where personal financial information is held on employees.
- Finance: Where personal information is held on individual customers.

However this is not exhaustive, there are other areas which may collect and record information such as customer service, operations and research.

One of the main changes is that each company needs to have a Data Protection Officer appointed as the point of contact for data queries and ensuring data compliance.

Where potential breaches may occur

It is important that the company demonstrates it has introduced compliant processes and that security systems are in place to keep the data safe from external interrogation or interference, however often a breach is from either a disgruntled or past employee. Building in safeguards to protect the company from this is paramount.

Sabre Associates

What you have to consider

It is still legal to collect and hold personal data, if there is a valid reason to do so; in fact companies are legally obliged to hold certain information for at least six years. From 25th May any data provided must be informed, unambiguous and freely given. This also means that any new purpose of using data requires additional explicit, informed, and unambiguous consent, and that consent can be revoked at any time.

Information collected from an individual must be:

- Freely given with consent
- Informed
- Unambiguous
- Held for a reason
- Only used for the purpose stated on collection
- Removed when no longer removed

Some of the key changes are around marketing and business development. From 25th May the organisation's marketing will need to ensure that any information collected or held has:

- Lawful, fair, and transparent processing
- Explicit limited purpose
- Full consent
- Minimising data
- Data accuracy
- Limiting storage
- Integrity and confidentiality
- Accountability

In addition marketing will need to ensure the company has a compliant privacy notice, aligned requests for data with a legitimate interest and opt-in messages when requesting information.

What you have to consider

HR will need to ensure that employees (whether current, past or potential) are both held and destroyed at the appropriate time. For example CVs sent in should not be kept ad infinitum; HR will need to provide clarification of data held to support references and suitable timeframes; and demonstrate how printed documents such as copies of driving licences are securely held.

The GDPR changes signal a significant shift in the current data protection act and is a fairly complex area. However it is a move towards best practice approaches and procedures which ensure that data around an individual is treated with respect and value.

For those organisations not dealing directly with end customers passengers it will be a relatively straight-forward exercise to review how current data is held, processed and destroyed. It will be those directly involved with interactions and transactions for customers and the general public who will find becoming GDPR compliant a larger exercise in identifying and securing the personal data they hold on individuals.

Regardless of whether your organisation is B2B or B2C though every business within the UK has a requirement to be compliant with the new GDPR regulations by 25th May 2018.

The outcome should be that you have privacy by design and default in all of your data transactions.

Sabre Business Associates

207 Regent Street
London
W18 3HH

0207 138 1067 | info@sabreassociates.co.uk | www.sabreassociates.co.uk

Sabre Associates