GDPR: ARE YOU READY? WHAT TO KNOW AND PLAN FOR

ONI, YOUR GDPR READY PARTNER

ONI plc is a leading UK IT Services Provider for whom Information Security and Data Protection has always been a top priority. ONI is already certified under ISO27001:2013, Information Security Management and is now on track to become the first UK company to achieve accreditation from Alcumus ISOQAR Limited under the new standard, **BS10012:2017**, Data Protection which reflects the requirements of the General Data Protection Regulations (GDPR).

ONI is on track to achieving full alignment with the requirements of the Regulations well before the implementation date for GDPR on 25 May 2018.

Fully supported by ONI's board, the project has progressed significantly towards its compliance. Richard Smith, ONI Finance Director, has also been formally appointed as ONI's Data Protection Officer (DPO).

Under the guidance of ONI's DPO, a firm of consultants and a firm of lawyers specialising in data protection and information security matters have also joined the project team to provide ongoing guidance and legal assistance.

ONI's GDPR project includes the following elements:

- Privacy Impact Assessment
- GDPR questionnaire
- Data Transfer Matrix
- Risk Assessment
- Overall Data Protection Policy
- Data Retention policy
- Data Protection operating procedures
- Breach response procedure
- Communications Plan
- Training and awareness for all ONI staff

About BS10012:2017:

This new standard replaces the previous British Standard of 2009 to accommodate the new GDPR changes taking effect in 2018. These new changes include:

- New definition of personal and sensitive data;
- Restrictions on profiling using personal data;
- New administrative requirements for data privacy officers;
- Pseudonymous data specifically covered;
- Abolishing of notification/registration requirement;
- New stricter require for consent for processing;
- Changes to subject access and other rights for data subjects;
- Enhanced right to erasure and new right to profitability;
- Security breach notification requirement;
- Privacy by design and privacy impact assessment requirements;
- Extension of the law to cover data processors;
- Removal of the safe Harbour ground for data transfers to the U.S.

YOU, SHADOW IT AND GDPR

The growth of shadow IT over recent years has plagued IT departments seeking to find a balance between business application control and end user experience. The changes that GDPR and the Data Protection Bill bring in will require much tighter governance over this runaway issue. Fortunately, actions and processes through IT can bring this issue under control.

Most organisations underestimate the level of Shadow IT in their business. Unlike BYOD before it, both hardware and software are now being used to overcome business and efficiency challenges.

The growth of low-cost and freely available cloud-enabled applications has naturally accelerated this issue exponentially, where every user has access to potential IT workaround solutions through their own devices.

This short term benefit, whilst good for the user, is a huge security risk for the business. The introduction of GDPR regulation means that taking back control is now paramount.

IT departments must be able to identify, control and secure Shadow IT solutions to avoid risk and legislative penalties.

What are the worst Shadow IT offenders? With literally millions of apps and services available to users, it is not an easy task to name them all, even if it were practical. However, research has shown that there are five commons types of applications and services that IT administrators should be aware of:

Business productivity apps - these can often be quite innocent, including anything from Microsoft Office and Google apps to other SaaS platforms that may be in use on desktops, but not on tablets and other smart devices.

File-sharing, storage and back-up - a very popular Shadow IT area, applications such as Evernote, Dropbox, Box and Google Docs to name four are regularly used.

Social Media - Facebook, Twitter, LinkedIn and Instagram are typical examples of services that have entered enterprise IT without business authorisation.

Communications - WhatsApp, Skype, Facebook Messenger, Slack and so on, all help undermine IT's communications and security stance.

USB drives - portable storage continues to be a huge issue when it comes to data leaks and security breaches.

To fix the issue, you first have to know what the issue is and then set out a strategy to overcome it.

Steps to tackle Shadow IT:

- Gain visibility of shadow IT services
- Understand & assess your current risk
- Educate your departments and users
- Introduce and enforce new IT policies
- Apply data loss & misuse procedures
- Monitor ongoing IT activity

WHAT'S CHANGING WITH GDPR?

The aim of GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established. Although the key principles of data privacy still hold true to the previous directive, many changes have been proposed to regulatory policies. The key points of GDPR as well as information on the impacts it will have on business can be found below.

EUGDPR.ORG

The General Data Protection Regulation (GDPR) will replace the out of date Data Protection Act 1995 on 25 May 2018 (before BREXIT occurs).

The act itself will have a significant impact on business & government bodies within and outside the European Union. Even after Brexit, GDPR will apply to any UK organisation that:

- Has an 'establishment' in the EU
- Sells to customers in the EU or 'monitors' their behaviour

Expanded territorial reach

More companies will be subject to GDPR which is not the case now.

Consent

Consent of personal data must be freely given, specific, informed and unambiguous.

Accountability and privacy by default

Increased emphasis on the accountability for data controllers to demonstrate data compliance.

Notification of a data breach

Notification to the Data Protection Authorities has changed.

Sanctions

Fines – up to 4% of annual worldwide turnover or 20 million euros is possible.

Role of data processors

Direct obligations to implement technical and organisation measures to ensure data protection.

One stop shop

This legislation will be applicable in all EU states.

Removal of notification requirement

Notifying or seeking approval from a Data Protection Authority is changing.

Right to be forgotten

One of the most useful changes for the average person managing their data protection risks.

The General Data Protection Regulation (GDPR) is the biggest change in data protection laws for over 20 years. Taking effect on **May 25th, 2018**, it will give back control of personal data to EU citizens.

HOW SHOULD YOU PLAN FOR GDPR?

Be prepared. As with any successful implementation, planning and preparation are key. The Information Commissioner's Office (ICO) has set out 12 practical steps to help you prepare for the GDPR:

Awareness
Raise awareness among management and staff of the new rules and their impact on the organisation and individual.

Information you hold
Perform data audits to review and document the personal data held and its location and source.

Communicating privacy information
Review your current privacy policies and put a plan in place for making any necessary changes in time for GDPR implementation.

Individuals' rights
Check that your procedures ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

Subject access requests
Update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

Legal basis for processing personal data
Look at the types of data processing you carry out and identify your legal basis for carrying it out and document it.

Consent
Review how you are seeking, obtaining and recording consent and whether you need to make any changes to these processes.

Children
Start thinking about putting systems in place to verify individuals' ages and to gather parental or guardian consent for your data processing activity.

Data breaches
Make sure you have the right procedures in place to detect, report and investigate any personal data breaches.

Data Protection by Design and Data Protection Impact Assessments
Familiarise yourself with the guidance the ICO has produced on Privacy Impact Assessments and determine how and when to implement them in your organisation.

Data Protection Officers
Appoint a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

International
If your organisation operates internationally, you should determine which data protection supervisory authority you will come under.

74% of UK SMEs had a data security breach in 2016

GDPR'S IMPACT ON THE INDIVIDUAL

GDPR's aim is to put individuals back in control of their data which means businesses will need to look at every aspect of how they collect, manage and protect data.

GDPR provides the following 8 rights for individuals:

The right to be informed

This encompasses your obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency on how you use personal data.

The right of access

Individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data;
- and other supplementary information – this largely corresponds to the information that should be provided in a privacy notice

The right to rectification

Individuals are entitled to have their personal data rectified if it is inaccurate or incomplete.

If you have shared the personal data in question to 3rd parties, you must also tell them of the rectification where possible. You must also tell the individuals about the 3rd parties to whom the data has been shared where appropriate.

The right to be forgotten

This enables an individual to request the deletion or removal of personal data where there is no requirement for its continued processing.

The right to restrict processing

Individuals already have a right to 'block' or suppress processing of personal data. Now, if processing is restricted, you are permitted to store the personal data, but not further process it.

The right to data portability

This allows individuals to obtain and reuse their personal data for their own purposes across different services. They can move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/ historical research and statistics.

Rights in relation to automated decision making and profiling

This provides safeguards for individuals against the risk that a potentially damaging decision is automated or taken without human intervention.

GDPR AND YOUR ORGANISATION

Whilst GDPR follows a similar approach to existing data protection legislation, there are some material changes. The new data protection regulation puts the consumer in the driver's seat, and the role of complying with this regulation falls upon businesses and organisations.

GDPR applies to all businesses and organisations established in the European Union, regardless of whether the data processing takes place in the EU or not. Furthermore, non-EU established businesses will also be subject to GDPR if they offer goods and/or services to citizens within the EU.

All businesses and companies that work with personal data should appoint a 'data protection officer' or 'data controller' to be in charge of and manage GDPR compliance.

Whilst high profile fines have grabbed the headlines, they can be enforced if businesses do not comply with GDPR. These penalties could result in fines of up to 4% of annual global revenue or 20 million Euros, whichever is greater.

The GDPR isn't just an IT issue. It has wide-reaching implications, including the way companies handle customer services, marketing and sales activities.

6% of UK businesses see GDPR as their number one priority

Source: Sophos. December 2017

FALSE FACTS

We're a non-EU-based company so the GDPR doesn't apply to us.

Since the UK is leaving the EU, we don't need to worry about GDPR compliance.

Personal data that is already in our database isn't subject to the GDPR.

My data is stored with my cloud service provider so it's their responsibility to remain compliant with GDPR, not mine.

Our company uses pseudonymization and encryption to protect personal data, so that should be enough for GDPR purposes.

01582 429 999
www.oni.co.uk
marketing@oni.co.uk
16-24 Crawley Green Road, Luton, Bedfordshire LU2 0QX

Established in 1992, ONI plc is a leading provider of IT services and solutions.
We deliver unique blend of on-site, hybrid and Cloud computing systems, from our Tier 3+ UK data centres.
Our workforce holds over 400 accreditations from vendors such as Cisco, VMware, NetApp, Veeam, Gamma, BT and Microsoft.