What Does GDPR Mean for Businesses

Effective from May 2018, the General Data Protection Regulation (GDPR) is the biggest shake up of data protection law in over 20 years.

The Regulation aims to put individuals back in control of their data, putting in place strict conditions over consent for data to be captured and stored. Organisations will also have to respond to requests from individuals and take the appropriate action "without undue delay". GDPR applies to all organisations worldwide who provide goods and services (paid or free of charge) to individuals within the EU or monitor the behaviour of those individuals. The GDPR applies to both data 'controllers' and 'processors'.

There are much tougher penalties under GDPR than previous data protection legislation. Organisations could face fines of up to 4% of annual worldwide turnover or €20 million – whichever is greater.

WHAT SHOULD ORGANISATIONS BE DOING TO PREPARE FOR GDPR?

Organisations need to look at issues such as whether existing technical systems efficiently retrieve and transfer individuals' data.

Security also needs to be robust enough to prevent disclosure of third party data to unauthorised recipients. Organisations need to assess whether practical changes to data processing systems are needed to meet new requirements and if existing privacy policies need to be updated to reflect the additional rights granted to individuals.

Employees who process personal data also need to be appropriately trained so that they can quickly recognise and respond to requests from data subjects to exercise their rights.

HOW GEMSERV'S GDPR SERVICES CAN HELP YOUR BUSINESS?

We take a pragmatic approach to help firms assess their readiness for the GDPR. We can undertake an assessment of GDPR compliance and help identify key areas of risk and non-compliance and then set out steps which will help organisations to:

- Understand risks to their personal data processing activities;
- Implement clear policies and procedures on use of data;
- Ensure consistency to harmonise data processing activities; and
- Demonstrate full compliance with GDPR to clients and partner organisations.

We have split our services into four focus areas to help you at every stage of your GDPR compliance readiness process.

GDPR HEALTH CHECK

A targeted and quick 'high-level' gap analysis assessment in order to help build a business case for further investment in GDPR compliance.

A Business Situation Review includes stakeholder interviews, assessment of data protection key principles and areas of risk and opportunity.

It also looks at data protection scope and strategic direction documentation including audit priorities and project planning. A data protection vision and action plan presentation is then developed.

DATA DISCOVERY

Providing total visibility of personal data processing activities and an assessment of existing controls in place to protect it.

A comprehensive inventory is compiled looking at type and location of data and purpose of process. It also looks at data retention periods, who has access to data, and security and breach mitigation measures.

Data Flow Mapping looks at the life-cycle across processing, security and compatibility, along with transfers and disclosures between business units and to third parties and service providers.

GDPR 'DEEP DIVE' ASSESSMENT

A detailed assessment showing where a business stands in relation to the GDPR. The assessment includes inventory and data flow analysis, along with review and drafting of data protection policies.

We also evaluate contractual documentation, along with data protection and confidentiality awareness training. The assessment also covers a review and update of contracts involving third parties.

Privacy Impact Assessments, re-designing consent mechanisms and a review of incident management procedures are also part of the assessment.

GDPR IMPROVEMENT PROGRAMME

A tailored and comprehensive GDPR Improvement Plan is then developed to ensure full compliance with GDPR. As GDPR compliance should not be treated as a one-off exercise, it is also important to embed the implementation actions within the organisation. This ensures not only that individuals' data continues to be protected but also reduces the risk of a data breach for organisations.

Gemserv can provide as much or as little support to implementation as is required by our clients, drawing on our strategy, risk, governance and compliance expertise. We are also able to support with ongoing independent evaluation and assessment of the ongoing maintenance of GDPR compliance.

This type of support to clients typically covers areas such as:

- Business transformation;
- Marketing;
- Legislation;
- Records management;
- Individual rights and transparency; and
- Physical and IT security.

As a consequence of our work in this area, we are also able to work closely with technology and infrastructure service providers to offer a turnkey service if required.

GEMSERV AND DATA PROTECTION

Gemserv's broad expertise across risk management, IT security and governance means we are uniquely placed to help organisations establish the processes and procedures in place to protect themselves.

Our extensive team of consultants provides a wide range of information assurance advice to both the public and private sector and work to CESG approved best practice standards and guidelines.

We take a pragmatic approach to help clients find intelligent and cost-effective solutions to their security challenges.

Our Third Party Information Assurance offering also provides a robust and independent assessment of current and future third party suppliers to protect against potential risks.

CONTACT US

To find out more about the GDPR or how we can help you, please contact one of our team on:

E: bd@gemserv.com
T: +44 (0)20 7090 1091
W: www.gemserv.com
@gemservinfosec

London Office

8 Fenchurch Place
London
EC3M 4AJ

Company Reg. No: 4419878