MBA IT

Your IT solutions team

Outstanding · Trusted · Driven · Personal

CYBERCROWD

GDPR READINESS SERVICES

Service Brief

MBA IT Your IT solutions team
Outstanding · Trusted · Driven · Personal

CYBERCROWD

INTRODUCTION

The EU General Data Protection Regulation (GDPR) comes into force on 25th May 2018 and will profoundly reshape the way that organisations handle data governance. The regulation applies to all organisations within the EU and to any nonmember states that offer goods or services to EU data subjects. It extends and broadens the types of personal data that are protected and increases the rights of data subjects. Data controllers and data processors will have new and substantial obligations to meet, and will be expected to demonstrate accountability for protecting the privacy of personal data.

The penalties for non-compliance are potentially huge and are intended to be dissuasive. The data protection authorities will be entitled to fine organisations up to 4% of worldwide turnover or €20m (whichever is greater) for the most serious infringements. In addition, data subjects get a right to claim for compensation under GDPR, so organisations can expect to be subject to claims from affected individuals and groups. You need to be compliant by the date at which the law comes into force. Given this, it is important to understand your obligations and to start working towards compliance. Being ready by 25th May 2018 will be a major undertaking, but the risks of not being prepared are too big to ignore.

Our GDPR services can be split in two:

- Our GDPR Readiness Services help you make sense of the regulation in the context of your business. Our Readiness Check-Up provides a high-level assessment of your compliance preparations. The aim is to help you identify gaps and understand that the steps that you need to take.

- Our GDPR Consultancy Services are appropriate where a more granular assessment is required to help you understand your data protection maturity or where you require assistance to design, implement or manage a compliance and information governance framework.

GDPR READINESS CHECK-UP

Our GDPR Readiness Check-Up is a workshop and discussion based assessment of your GDPR readiness. The purpose is to help you demystify what GDPR is, what the implications are for your organisation and to advise on the practical steps that you should be taking now to prepare.

Areas that we discuss during the engagement include:

1. Understanding your status and obligations under GDPR
2. Understanding your data: where it is and how it is used
3. Having the required documentation in place
4. Applying appropriate technical and organisational measures
5. Securing third party relationships
6. Adherence to best practice certification schemes or approved codes of conduct

The service is delivered by gathering information from detailed questionnaires, through workshops and, in some cases, 1:1 interviews. It also includes a desk based review of your key data protection policies and documentation. The duration is 3 days of which one day is spent with you on-site and two days are delivered remotely. During the first day, we lead workshops and discussions with your stakeholders to brief them on GDPR and gather information. On the second day, we review your documentation and analyse the information gathered. The final day is used to put together our report and recommendations, to present it back to you and to discuss options and next steps.

Our report provides you with an overview of your GDPR readiness, and the practical and pragmatic steps that your organisation should take to mitigate the risks and demonstrate best practice in line with the Regulation.

For more information please contact us at
info@mba-it.com or 020 3815 6680

MBA IT Your IT solutions team
Outstanding · Trusted · Driven · Personal

CYBERCROWD

GDPR CONSULTANCY SERVICES

Where you require a more in-depth engagement, our consultants can work closely with your team to prepare you for GDPR and manage your ongoing obligations. This can be focussed on GDPR alone or be delivered as part of a wider information risk management and cyber resilience programme.

Example services include:

1. Detailed and tailored GDPR readiness reviews
2. Data and data flow mapping
3. Risk management and data protection impact assessments
4. Compliance and privacy governance framework design and implementation
5. Policy and procedure reviews and implementation
6. Reviewing and implementing technical measures and controls
7. Documentation creation and management
8. Ongoing outsourced maintenance and management

Every GDPR Consultancy engagement is delivered as a bespoke engagement according to your needs, desired outcome and available budget. The starting point is a scoping exercise during which we work together to define your desired outcome and put together an agreed statement of work.

FREQUENTLY ASKED QUESTIONS

What constitutes Personal Data?

The definition of Personal Data is very wide and covers any information which can be used to identify a natural person. This might include their name, contact details, location data, online identifiers (such as an IP address and mobile device IDs), photographs and more.

The definition covers direct identification and indirect identification, such as two different data sets that you hold which might not identify an individual on their own but which can be used together to identify a data subject.

What constitutes Processing?

Again, the definition of Data Processing is widely drafted. The GDPR defines it as "any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means". It then goes on to provide a list of example operations, but in short - if you do anything with personal data (including deleting it) then you are processing it.

What's the difference between a Data Controller and a Data Processor?

A Data Controller is a person or body which alone or jointly "determines the purposes and means of the processing of personal data" whereas a Data Processor "processes personal data on behalf of a controller". The key distinction is around determining the 'purpose and means of processing'. If these decisions rest with you, then you are a Data Controller. Both Data Controller and Data Processors have significant obligations under GDPR.

We're Cyber Essentials / Cyber Essentials Plus, does that make us compliant?

No, but it is an indication that you consider information security technical controls to be important. Whilst having appropriate technical measures in place to protect Personal Data is a requirement of GDPR, the controls set out in Cyber Essentials cover the basics and should be considered a good starting point. GDPR requires more than technical controls, it necessitates a framework covering people, process and technology.

For more information please contact us at
info@mba-it.com or **020 3815 6680**

MBA IT Your IT solutions team
Outstanding · Trusted · Driven · Personal

CYBERCROWD

We're ISO27001 certified. Does that make us compliant?

Not on its own, but an ISO27001 certified Information Security Management System does provide you with a strong, risk based starting point to demonstrate that you are applying appropriate technical and organisational measures and controls to protect personal data. In the event of a breach of GDPR, your adherence to an approved 'code of conduct' or certification such as ISO27001 will also be taken into account when the value of any fine is set. All the same, GDPR extends beyond Information Security so it's important that you take this into account when preparing for compliance.

Can you certify us as compliant?

No, GDPR isn't a "pass/fail" standard. It requires organisations to take a "risk based" approach to data protection whereby they implement protective measures corresponding to the level of risk associated with their data processing activities.

Who needs to be involved when we buy your GDPR Readiness Services?

You should ideally involve the owners of personal data that you process across your business. This will typically include the following functions: IT, HR, Finance, Legal and Marketing. Depending on the nature and size or your organisation, you may need to involve multiple stakeholders to understand your data and start mapping its flows.

How does Brexit affect GDPR?

The UK Government is committed to GDPR notwithstanding the Referendum result. Even if the UK was not bound by the regulation, any organisation processing the personal data of data subjects in a member state would still be affected.

Can you help us improve our information and cyber security as well?

Yes. Our Security Posture Review focusses on your cyber resilience maturity, covering strategy, people, process and technology. It provides a detailed analysis of your current security posture against best practice together with detailed recommendations. Our Cyber Threat Review provides a detailed assessment of your security vulnerabilities. It includes a firewall security assessment, external vulnerability scan, internal vulnerability scan, privileged account audit, optional security monitoring of your network for 48 hours and more. We can also provide security consultancy services tailored to your requirements.

Can you provide your GDPR services on a rolling basis?

Yes. We can work with you on an agreed programme of work to be delivered as a virtual member of your team over an extended period of time. We can also provide a Data Protection Officer service, whereby a suitably qualified practitioner acts your DPO for the purposes of GDPR and supports your business for an agreed number of days each month over a year. This can include a high activity period at the outset reducing to maintenance activity thereafter.

For more information please contact us at
info@mba-it.com or **020 3815 6680**

We'd love to hear from you!
Please get in touch using the details below:

Canonbury Business Centre, 190A
New North Road, London N1 7BJ
info@mba-it.com
020 3815 6680
www.mba-it.com

MBA IT

Your IT solutions team
Outstanding · Trusted · Driven · Personal