mti™
Managing Data Securely

steps to GDPR

+44 (0)1483 520 200 | ukinfo@mti.com | mti.com

Getting Ready for GDPR

The General Data Protection Regulation (GDPR) comes into force on 25 May 2018.

All organisations that process the personally identifiable information of EU residents will be required to abide by its provisions or face significant penalties.

GDPR makes provisions for considerably tougher penalties than the UK Data Protection Act. Organisations that breach the GDPR law provisions can expect fines of up to 4% of annual global turnover or €20 million (£17 million), whichever is greater.

€20 MILLION

Clearly fines of this scale can easily lead to business insolvency and, in some cases, bring businesses down.

Who does it affect?

UK organisations that do business in the EU with EU data subjects' personal data have to comply with the regulation even if you're not based in the EU.

Data breaches today are commonplace and typically increase in scale and severity with each passing month, leading to damaging headlines.

No organisation is bulletproof when it comes to data security so it's vital that they are all aware of their new obligations under GDPR.

The following Five Steps to GDPR highlight the key measures you need to take to ensure you are on the right road to full GDPR compliance.

1 Identify Your Data

The overarching aims of GDPR are to hand control of personal data back to citizens and hold responsible those organisations that breach this principle. This means that organisations that hold personally identifiable information must secure it.

What is defined as 'personal data'?

However, GDPR broadens the scope of what is defined as personally identifiable information. It considers any data that can be used to identify an individual to be personal data.

This includes, for the first time, things such as genetic, mental, cultural, economic or social information. Parental consent is also required for the processing of personal data of children under the age of 16 but is likely to be under 13 in many EU states.

Consequently, organisations need to take measures to reduce the amount of personally identifiable information they store, and ensure that they do not store any information for longer than necessary.

How can businesses do this?

This means identifying datasets that contain personal information. The difficulty for many organisations is that personally identifiable information is typically scattered across different systems.

For instance, HR systems may hold information on former employees, marketing systems will have data on campaign subscribers, CRM systems will have information on customer histories, finance will have information in its accounting systems, and data will probably also be held in the cloud if an organisation uses software-as-a-service.

What is the first step to GDPR compliance?

The first step then to GDPR compliance is to identify data owners within an organisation, whether it is marketing, sales, customer service or finance. By asking yourself who is processing personal data, who has access to data, and who is storing personal data, a system map can be established that shows precisely where personally identifiable information sits in your systems.

This will enable you to document what personal data is held, where it came from and who you share it with. This ensures that you take the correct steps to meet GDPR's accountability principle, which requires organisations to be able to show how they comply with the data protection principles.

2 Review Your Policies and Technology

GDPR requires that privacy is included in systems and processes by design. This means that software, systems and processes must consider and enable compliance with the principles of data protection.

What is the first question businesses should ask?

The important question to ask is whether existing data policies comply with GDPR. Many existing policies won't, so organisations will need to put procedures in place that enable GDPR's new transparency and individuals' rights provisions.

This means that if you don't have specific data policies in place then now is the time to produce them. GDPR enactment is not far away so it's essential to start planning your approach to compliance to gain 'buy in' from key people in your organisation.

For instance, in a large or complex organisation GDPR can have significant budgetary, IT, personnel, governance and communications implications. If, for example, there is no budgetary provision for GDPR within the IT budget, it will lead to problems when you review systems and processes and discover you need to make adjustments.

What if we already have data privacy processes in place?

Many organisations will already have systems in place that enable different levels of data confidentiality and access but are they sufficient to meet GDPR requirements? If not, a rethink is required on how data is accessed and how it is inputted, processed and outputted.

For instance, GDPR is clear that data controllers must demonstrate that consent is given before an organisation can change the use of the data from the purpose for which it was originally collected. This principle alone requires a review of existing systems and the need for an effective audit trail.

Another GDPR requirement is for organisations not to hold data for any longer than absolutely necessary. At the same time organisations must be able to delete data if a request is made by an individual.

Meeting these mandatory requirements requires systems that can accommodate and enable GDPR requirements. For instance, if a data deletion request is made, can an organisation easily meet this request with a few simple clicks or does it require each system to be approached individually?

If it's a small organisation that is anticipating very few data deletion requests such an approach might be passable. If it's a large commercial organisation that is expecting a hundred data deletion requests each month, it's clearly going to cause problems if systems don't facilitate data deletion. This is just one reason why a policy and technology review is absolutely essential.

+44 (0)1483 520 200 | ukinfo@mti.com | mti.com

3 Set Up Data Protection

Privacy impact assessments (PIAs)

GDPR includes mandatory privacy impact assessments (PIAs) requiring data controllers to conduct assessments in areas where privacy breach risks are high to minimise risks to data subjects.

Addressing these PIA issues will not only enable compliance with privacy impact assessments but also extend to the wider GDPR data protection requirements of protecting individual data.

We're flagging PIA's because they have considerable implications for many organisations. PIA's are only required in what are termed 'high-risk situations', for example where a new technology is being deployed or where a profiling operation is likely to significantly affect individuals.

In this age of mobility many organisations are engaged in deploying new technologies and as such it's an important issue. Before organisations can begin projects involving personal information, they need to conduct a privacy risk assessment to ensure they are in compliance as projects progress.

Why privacy by design so important?

It's always good practice to adopt privacy by design but because GDPR now makes it a legal requirement you need to consider issues and ask questions around data encryption, data segmentation and access authentication.

For instance, do existing systems encrypt personal identifiable data? If not, at what point in the system will data be encrypted? Will it be encrypted during transit or in situ? Asking these questions also leads to the management of encryption keys. For instance, how will they be secured?

In some cases, GDPR compliance may be applied to a segment of data and not a full dataset. In this case, the data segments need to be identified and protected appropriately.

Issues around authenticating access also need to be addressed. For instance, do you know who is accessing personal identifiable information and what rights, if any, they have over the data?

By identifying the relevant data sets governed by GDPR, access and authentication can then be designed to ensure compliance with privacy impact assessments and wider GDPR data protection requirements.

+44 (0)1483 520 200 | ukinfo@mti.com | mti.com

4 Create a Data Breach Plan & Test It

The important next step is the creation of a data breach plan to ensure that you have the right procedures in place to detect, report and investigate a personal data breach.

If a data breach occurs that is likely to result in some form of damage to an individual, such as identity theft or a breach of confidentiality, the Information Commissioner's Office (ICO) needs to be notified.

However, not every breach requires you to notify the ICO. That said, if you fail to report a breach when required you could be fined as well as receiving a fine for the breach itself.

Breaches need to be reported within 72 hours of discovery. As a result, organisations need to have the technologies and processes in place that will enable them to detect and respond to a data breach. This may require a change to internal security policies.

How to create a data breach plan

To create a data breach plan you need wide engagement within the organisation and the sponsorship of executive management. This ensures that everybody is 'on board' and aware of the importance of GDPR.

When the plan is created it needs to be tested simulating a real-world breach. This will test the effectiveness of the plan, highlight vulnerabilities and allow you to introduce remedies where required.

It's also important to test your detection technology. This is one foundation upon which your compliance is built and it needs to be able to detect all breaches as soon as possible, and especially before the impact of a breach becomes damaging.

Breach detection technologies are essential for GDPR compliance. For instance within the context of an external hack, cyber crooks have moved on from sending generic malware to carefully plotting attacks using zero-day exploits, advanced persistent threats or social engineering.

The initial intrusion in a breach scenario typically takes minutes to a few hours. The real damage, however, occurs after hackers get around the first line of defence, making after-the-fact breach-detection efforts so critical.

Traditional breach detection technologies such as intrusion detection systems and security information and event management technologies generally fall short in the face of new threats.

If your breach detection technology can cut through network noise and highlight relevant, actionable security alerts, it is doing its job. A data breach plan that is rigorously tested will enable you to establish whether your detection technology can do this and as a result meet compliance requirements.

+44 (0)1483 520 200 | ukinfo@mti.com | mti.com

5 Implement Training and Reviews

Organisational awareness is key

The success of GDPR compliance will ultimately be determined by organisational awareness. Decision makers and key people, typically director level, within the organisation need to be aware that the law is changing and failure to comply can potentially have seriously damaging financial and reputational consequences.

This will focus minds and help stakeholders understand the importance of GDPR compliance. It will help them appreciate the gravity of GDPR and help you in identifying areas that could cause compliance problems.

It will also help to avoid a situation in which GDPR compliance is left until the last minute, which would likely create significant difficulties. Further, it will raise awareness that GDPR could have significant resource implications.

One of the requirements for GDPR is that public authorities appoint a data protection officer if they are processing personal information. The act actually states that this also applies to other entities, when 'core activities' require 'regular and systematic monitoring of data subjects on a large scale' or consist of 'processing on a large scale of special categories of data'.

This may or may not apply to your organisation, but even if it doesn't it makes sense to appoint someone to a similar role to ensure personal data processes, activities and systems conform to GDPR.

A further critical step is to train all staff on GDPR-based policies and why they are so important. It's a fact that data protection policies are most often breached by people within the business. As such GDPR-based policies shouldn't be reduced to a few paragraphs in a staff handbook, rather formal staff training is required to ensure that your plan is well understood and is consequently robust.

Appoint annual policy and technology reviews

It's also important to conduct an annual policy and technology reviews. In short, the data breach plan and compliance steps need to be tested each year to ensure there is no policy 'slippage'.

Finally, ensure that you conduct annual penetration tests to identify potential breach points. Penetration tests will uncover points of vulnerability that you may not have thought of, whether its technology or people flaws.

It's important to understand that the threat landscape is dynamic and always evolving. There's no such thing as a static threat landscape so penetration testing is one of the most critical steps you can take to ensure your GDPR compliance is rigorous and robust.

+44 (0)1483 520 200 | ukinfo@mti.com | mti.com

Contact MTI Today

Managing Data Securely

MTI - Global Solutions and Services Provider

Datacentre - Managed Services - Security

to find out more, please visit www.mti.com

Call us on +44 (0)1483 520 200

Email us at ukinfo@mti.com

MTI Technology Limited, Riverview House, Catteshall Lane, Godalming GU7 1XE