Blue Cube
Intelligent Protection

De-mystifying GDPR

GDPR is one of the hottest topics in the business and security media alike. Advice on how to become GDPR compliant abounds and it is increasingly difficult to pinpoint where businesses need to focus their energy in the coming months.

Understanding GDPR and the subsequent actions you need to take is crucial for your business to become legally compliant but both you and your customers will benefit significantly if you seize this opportunity to bring overall improvement to your business processes and data security.

What is GDPR and how will it impact your business?

GDPR (General Data Protection Regulation) was agreed in the European Parliament on 14th April 2016 and will be enforced from 25th May 2018. The GDPR will harmonize data handling requirements across Europe and as it is a regulation rather than a directive it will eliminate national differences. It also serves to update data protection legislation to take account of technology advancements and plans for future innovation.

The regulation applies to any EU citizen data, personal or professional, irrespective of where that data is processed. This also means that post Brexit, most UK business will still need to comply.

GDPR is enforceable from 25th May 2018

Key changes brought in by the regulation impacting businesses and public bodies include:

- **Regulation concerning Data Controllers & Processors**
- **Rules concerning acquisition of consent**
- **Rights of individuals over their own data**
- **Role and working practices of Data Protection Officers (DPOs)**
- **Breach incident obligations**
- **Data breach fines**
- **Privacy by design**

We will examine these changes in more detail and look at actions your business should take to move towards GDPR compliance

Data Controllers and Processors

Data controllers and data processors will now be equally responsible for the protection of data and avoidance of breaches and therefore data processors must also comply with the regulation. A data controller cannot therefore outsource the risk to a third party such as a cloud service and is responsible for downstream control of data. It is important that you ensure your contracts with any data processors you use are clear on data protection responsibilities and they too are GDPR compliant. This is necessary even if the data processor is not headquartered in Europe.

Action!

- ✓ *Review contracts*
- ✓ *Review data held*
- ✓ *Review data lifecycle*
- ✓ *Review data protection*

Data Controllers and Processors are equally responsible For data protection

Consent

When a business is seeking consent to use an individual's data then the consent request must be clear and easy to understand. Implied consent will no longer be sufficient – unambiguous consent is required therefore pre- ticked boxes or other assumptions of consent will no longer be acceptable. It must also be clear the reason you are requesting consent and if you plan multiple uses of the data then each use case needs to be identified. You have an obligation to document when and how consent was given for future reference. Should you be processing data on children below 16 years of age you are also required to obtain parental/guardian consent, this age limit may be reduced by individual countries to a minimum of 13. You are not required to refresh all DPA consents in preparation for GDPR but must make sure you comply with the requirements – it is a good opportunity as you communicate with customers to refresh the consent.

Action!

- ✓ *Review transparency of consent gathering process*
- ✓ *Review clarity of data use*
- ✓ *Review data lifecycle*

Unambiguous consent of individuals is required

Rights of individuals

The Data Protection Act already gave individuals many rights, the key change in the GDPR is the "right of data portability" which combined with "right of access" and "right to be forgotten" (erasure) gives an individual a high level of transparency. An individual has the right to see all data held on them, the right to erasure (except in certain circumstances) and the right to be given their data in a commonly used machine-readable format at no cost (for data they provided to the controller for automated processing). An individual retains the right to rectify errors, restrict processing, object to data use and not to be subject to automated decision-making/profiling.

Controllers have a right to refuse to delete data under specific circumstances (compliance with legal obligations or public health, or rights of freedom of expression).

If a business receives a subject access request you have a reduced period of 1 month to comply.

Action!

- ✓ *Review data portability approach*
- ✓ *Review capability to respond to subject access requests*
- ✓ *Review process for data update*

Right to data portability – delivery in a month

DPO

There is no longer a requirement to register your data processing activity with a supervising authority, you are now required to maintain internal records this will simplify and improve the process of managing your data processing activities.

A DPO is mandatory where data processing is carried out by:

- A public authority or
- A company whose core activities require systematic monitoring of data subjects
- Companies processing data on a large scale (large scale not yet specified – considering 5000 records per year)
- If the business is processing 'Special categories' of data, e.g. health, religious and political beliefs, criminal convictions

Action!

- ✓ *Review requirement for DPO*
- ✓ *Review support & authority of DPO*
- ✓ *Review data recording/reporting*

The European Commission requires any enterprise over 250 employees to have a DPO. It is important that the governance of this role is clear and they have sufficient knowledge, authority and executive support to perform the role effectively – it can be an internal or external role.

Clarity on DPO requirements, role and responsibility

Breach Notifications

Mandatory actions following a data breach have changed. A breach must now be notified to a company's supervising authority within 72 hours furthermore the data subjects should be notified without undue delay ensuring that the data controller can't wait months and years to inform those affected by a breach. Breach notification to affected individuals may not be deemed necessary if it can be shown that access to the data was not possible (e.g. if it was encrypted)

Action!

- ✓ *Review security incident plan*
- ✓ *Review breach role & responsibilities*

Breach notification to DPA within 72 hours of breach

Breach Fines

Fines for companies who have suffered a breach have changed. There are now 2 tiers of fines that are applied according to the severity of a breach up to 4% of global annual TO or €20 million for major breaches and up to 2% or €10 million for data record breaches or failures to notify. While these are the maximum levels that can be levied, they won't apply in every case, that said, it is clear that fines will rise from the current levels. Fines will apply to both controller & processor as they are equally responsible.

Action!

- ✓ *Inform Board of breach fine changes*

Significant increase to breach fines

Privacy by Design

While privacy by design and privacy by default is not a new concept, GDPR makes it a legal obligation so it is no longer permissible to add privacy and security as an afterthought to a system or process. Data controllers & processors are required to build privacy into their processes and technology solutions from the outset.

Action!

- ✓ *Review & edit project plans to include privacy by design approach*
- ✓ *Review technology solutions*

Privacy by design becomes legal obligation

Implementation of GDPR in the UK

The UK's Data Protection Bill, will get its first reading in September 2017 (the second reading, when lawmakers debate legislation, is not currently scheduled). The Bill is designed to:

- Implement the GDPR and the new (UK) Directive which applies to law enforcement data processing
- Replace the Data Protection act of 1998
- Modernise data processing by law enforcement agencies covering both domestic & international data processing & transfer
- Update the powers and sanctions available to the Information Commissioner.

Action!

- ✓ *Check compliance with UK definition of personal data*
- ✓ *Check ability to comply with automated profiling opt-out*

The UK Bill will endure beyond Brexit and ensure ongoing compliance with GDPR as the UK continues to trade with Europe. GDPR allows for some national flexibility, the UK will take advantage of that to introduce some extensions and additions - the UK Bill will:

- Require social media companies to delete all of an individual's posts from before they were 18 should they request it.
- The definition of personal data will be extended to include IP addresses, website cookies and DNA all of which can be used to target individuals.

- Enable an individual to demand to be excluded from automated processing and profiling and to have the profiling done by a person (e.g. for insurance, mortgages etc.)

- The Data Protection Bill sets the maximum fine at £17 million and 4% of turnover translating it to UK currency.
- The powers of the Information Commissioner will be extended and strengthened to enable it to implement the new regime.
- There will also be two new criminal offences, which could have unlimited fines:
    - Re-identifying people from reconstruction of bits of anonymous data
    - Tampering with data that has been requested by an individual

Additional UK protections to be implemented

Summary

GDPR will harmonize the processing of data across Europe and will offer individuals far greater transparency and choice over how their data is used.

By clearly understanding the key changes that GDPR will bring and implementing a company wide action plan your business will achieve GDPR compliance by the deadline date of 25th May 2018. GDPR compliance will improve and enhance your process leading to better protection of your customers and improved customer service.

A number of key actions have been highlighted in this article. Blue Cube Security have prepared a detailed action plan that will help you further in prioritizing your actions and reviewing technology solutions to support GDPR compliance, contact us directly for further consultancy and assistance.

Blue Cube Security Ltd.
Fairway House
Portland Road
East Grinstead
RH19 4ET
enquiries@bluecubesecurity.com
+44 (0) 345 094 3070

Blue Cube
Intelligent Protectio