GDPR - How to be compliant with new data protection laws

What are the requirements?

From 25th May 2018, every UK business will need to comply with the new data protection laws as set out by the General Data Protection Regulation (GDPR). GDPR was approved at European parliament in 2016, allowing two years for organisations to comply with the new legislation.

GDPR will replace the current EU Data Protection Directive from 1995, bringing it up to date with how companies use Internet and cloud technology, making provision for the new, previously unforeseen ways companies are gathering and using personal data.

This new legislation is designed to protect and empower all EU citizens and UK citizens (post Brexit), offering improved control and transparency over how their personal information is held & used.

How could GDPR affect your organisation?

Broadly speaking, GDPR will affect every organisation that holds or uses personal data, including companies outside of Europe. So once the legislation comes into effect in May 2018, any kind of personal data, including IP addresses and other online identifiers, must be processed transparently and when required, deleted.

GDPR talks about both Data Subjects, Personal Data, Controllers and Processors in their guidelines. If you're unsure of the terminology, please read the GDPR & UK Data Protection Bill summary definitions.

You may fall into either category or both, but you'll still need to ensure you're compliant, and with the enforcement date looming, it's imperative that every organisation knows exactly what they need to do to avoid hefty fines.

Key Changes

The key changes GDPR will introduce are as follows:

1. Penalties for non-compliance are either 4% of a company's global revenue, or €20m.
2. If a data breach occurs, notification needs to occur within 72 hours. Failure to do so could lead to a €10m fine, or 2% of your annual worldwide revenue.
3. Clear and plain language must be used when requesting consent for the use of personal data, so any illegible T&C's full of confusing and obtuse language will need to be revised. You also can not offer pre-ticked boxes or ask to perform an action to opt-out. Instead, clear, affirmative consent needs to be obtained before using personal data.
4. Data controllers need to make it easy for data subjects to withdraw consent to use their data.
5. If requested, data controllers need to provide a data subject with a free of charge copy of their personal data in an electronic format.
6. Data must be saved in commonly used file formats like CSV, so they can be moved to other organisations (within one month) free of charge if a data subject requests it.
7. Data subjects can exert the right to be forgotten. This Data Erasure means that:
    a. Controllers must delete any data that's no longer being used for the purpose it was collected for;
    b. If a data subject revokes the right for that organisation to hold their data, all personal data must be deleted.
8. As a data controller, you can only hold and process data that is absolutely necessary for the completion of your duties.

Hall Farm, Sywell Aerodrome, Sywell, Northampton, NN6 0BN
t:01604 671177 www.document-genetics.co.uk

9. If you are a public authority, a company processing large amounts of sensitive data or you carry out large scale monitoring of individuals (for example, online behaviour tracking), you're required to appoint a Data Protection Officer.

Will Brexit Change Things for UK Organisations?

Although Brexit has made the implementation of GDPR less clear, in a recent 4D Survey, 69% of UK organisations voted to keep it even after we leave the European Union. Furthermore, organisations with customers in the European Union will still need to comply with GDPR regardless of the UK's status within the Union.

However, in August 2017, the UK government put forward their own Data Protection Bill, and it's very similar to GDPR, so, post-Brexit, UK data will still be protected in much the same way. The UK Data Protection Bill largely includes all GDPR European privacy laws but will be the UK view of GDPR when it enters the UK statute books post Brexit. See: GDPR & UK Data Protection Bill.

Getting ready for GDPR

The amount of work involved when preparing for GDPR will vary depending on a number of factors: how much you use marketing data and how you communicate with your prospects (e.g. email & telephone marketing to potential customers), and if you're already working in line with industry best practices for data protection.

Regardless of your businesses activity, if you use personal data you'll need to review the way you work and implement the necessary changes as soon as possible to ensure compliance; you may even need to seek expert advice (as we did here at Document Genetics) if you are unsure how to remain compliant.

In Conclusion

GDPR is the biggest shake up of data protection laws for over 20 years and fundamentally changes the way organisations can store and use data. Furthermore, it places the data subject's rights at the very centre of data protection regulations - Organisations no longer own personal data but, should instead, consider themselves as custodians of such data.

The challenge lies with defining the actions that need to be taken and bringing your organisation's processes and systems in line with GDPR before the 25th May 2018, so if you haven't started preparing to implement these new regulations across your business, start with the UK Information Commissioners Office who have produced an online GDPR checklists for data controllers and data processors and a 12 step guide to preparing for GDPR.

The use of technology alone will not ensure compliance, but Document and Records Management software (DMS / EDMS), such as infoRouter, can play a key role in the following areas within GDPR:

1. The right to be forgotten
2. The right of access
3. The right to data portability
4. Breach notification standards
5. Privacy by design

With this in mind, we have written a GDPR WhitePaper which considers the useful role of Document and Record Management Systems with regards to GDPR compliance.