Gallagher

Insurance | Risk Management | Consulting

THE GDPR AND WHAT IT MEANS FOR YOUR ORGANISATION.

The General Data Protection Regulation (or GDPR) is one of the biggest shake-ups to data protection legislation in history, so it's no wonder that it's a hot topic for many organisations. With such dramatic changes on the horizon, now is the time to make sure your organisation is prepared for this overhaul to data security and privacy law. In this bulletin Arthur J. Gallagher break down what the GDPR is, what you need to do to comply and what the penalties for non-compliance are.

What is the GDPR?

The existing Data Protection Directive was introduced in 1995 – before widespread use of the internet changed our environment irrevocably. Designed to ensure that data legislation across the EU reflects the myriad new ways that data is used, the GDPR aims to enforce stronger data security amongst organisations that handle personal data, and enhance privacy rights of individuals that entrust those organisations with that data, giving people more say over how their data is handled. While it came into force on 25 May 2016, the GDPR will apply to all EU member states from 25 May 2018, which is the final date for organisations to comply. The UK Government has indicated its commitment to the GDPR after Brexit and has already introduced the new Data Protection Bill, which will implement the GDPR in full.

What does it involve?

The changes brought in by the GDPR are wide-reaching, but here are the key points of the updated legislation.

1. Processing of personal data is only permitted where a legal basis for processing applies, such as where it is necessary for the performance of a contract. Specific rules apply to the collection of "special category data" (previously known as "sensitive personal data"), which will require the explicit consent of individuals. Organisations will need to keep a record of the relevant consent or legal basis relied upon. Consent is becoming more onerous, and organisations will no longer be able to hide consent in terms and conditions or complex jargon or use pre-ticked 'opt-out' check boxes. The individual will also be able to withdraw consent to processing at any time.

2. The definition of what qualifies as personal data now expressly includes IP addresses and location data.

3. Individuals will have the right to request that organisations erase their data, restrict how their data is used and to have their data transported to another controller if they choose to do so. Data controllers must take action within a month of the request.

4. GDPR doesn't just apply to organisations based within the EU, it also applies to any company offering goods or services to, or monitoring the behaviour of, data subjects in the EU.

5. While there has always been a requirement to take appropriate measures to keep personal data secure, the GDPR now expressly recognises pseudonymisation and encryption of personal data as good practice.

6. Organisations will be required to maintain records of their data processing activities including, for example, purpose of the processing, a description of the categories of data subjects and categories of personal data, details of any transfers to third parties or outside the EU, and contact details of the data controller. Data should not be held for longer than is necessary for the purpose of the processing.

7. Data protection impact assessments will be required for all data collection which is likely to result in a high risk to the rights of individuals, for example, where new technologies are being used to carry out large scale profiling.

8. It will be mandatory to report all data breaches to the Information Commissioner's Office within 72 hours of becoming aware of the breach occurring, unless the breach is unlikely to result in a risk to individuals. It may also be necessary to notify the individuals involved if the breach is likely to result in a high risk to them.

9. All organisations processing large amounts of data or sensitive personal data will be required to employ an independent Data Protection Office to monitor compliance.

10. Data subjects have the right to view the data held on them, and your organisation should provide it within one month. If information is incorrect, it must be rectified without undue delay.

What should you be doing to comply?

The legal and technical changes required by your organisation could be very significant and will require co-operation from all departments. Compliance cannot be achieved without the help of legal and IT security support, but everyone needs to understand what is required of them – especially concerning how data is handled. You will need to audit your current data protection measures, document all existing information held and ensure all data collection measures are compliant with the above. This also applies for any third-party companies your organisation currently uses who are not compliant with the new law.

If you do not have one already, you should also ensure that your organisation has a data breach plan in place, that individuals involved in the plan know their roles, and that the plan is practiced regularly, to ensure that you can react to a breach and notify the ICO within 72 hours. It is worth considering implementing a security alert system to spot data breaches as quickly as possible, in order to prevent further damage.

If your organisation processes large quantities of personal and/or sensitive personal data, you should also consider appointing a Data Protection Officer who will be responsible for how your organisation handles data – this role can be filled internally (though they must be independent of other roles) or by an external company.

What are the penalties of non-compliance?

The fines for inadequately protecting data are severe – the most serious infringements attract fines of up to €20 million or 4% of your annual global turnover, whichever is greater. This is regardless of who is responsible for the breach - even if it is a malicious attacker or third party, your organisation will be responsible for the fine and any resulting reputational damage.

For less serious infringements a tiered system of fines would apply. For example, failure to notify in the event of a breach would result in a fine of up to €10 million or 2% of global annual turnover. This could be significantly greater than the current maximum fine in the UK of £500,000 under the Data Protection Act 1998.

Our conclusions

The way data is transmitted has changed unrecognisably in the last two decades and an overhaul to existing legislation is well overdue. You need to be working to engage senior leaders in your organisation to ensure that changes are implemented across the board. Conducting a thorough review of your existing data collection and protection policies can be time consuming, which is why many organisations are choosing to outsource the task. There is technology available which can help you to meet the requirements around data deletion and portability, and where your budget allows, you should utilise this.

We can work with your organisation to develop processes surrounding data protection which will ensure you are prepared for the introduction of the GDPR. We can also help you to prevent data security breaches with our Cyber and Crisis Resilience products which have been designed with the requirements of the GDPR in mind.

Regardless of how you choose to approach it, the sooner you begin the process the more time you will have to ensure you comply. The GDPR aims to ensure that data protection and privacy are no longer just an afterthought and are included in all of your systems and processes. Organisations need to show that they value an individual's privacy, and reflect this in how they handle the data they collect.

WOULD YOU LIKE TO TALK?:

Walbrook Office
The Walbrook Building
25 Walbrook
London
EC4N 8AW

T: +44 (0) 808 178 1947
E:ukenquiries@ajg.com

www.ajginternational.com

About Arthur J. Gallagher

Founded in 1927, Arthur J. Gallagher & Co. has become one of the largest insurance broking and risk management companies in the world1. With extraordinary reach internationally, our parent group employs over 24,000 people and provides services in more than 150 countries. Outside the US we are known as Arthur J. Gallagher and wherever there is an issue of risk, we're there for our clients. We are dedicated to working together to create solutions that drive value and competitive advantage for our clients.

For more information, visit us at **www.ajginternational.com**

1 http://www.businessinsurance.com/article/20170703/NEWS06/912314229/Business-Insurance-broker-rankings-2017-Arthur-J-Gallagher-Co