Aon Risk Solutions
National | Public Sector

Ten questions and answers about GDPR

Welcome to the February 2018 edition of Aon Inperspective

The Public Sector Bulletin

Staying in front of insurance related issues and trends affecting the public sector can be challenging. Aon Inperspective – the Public Sector Bulletin contains insight and news articles written exclusively by public sector experts and is designed to keep our clients and future clients ahead of the risk curve.

Bill Sulman
AC11 AIRM
Public Sector Client Director

The General Data Protection Regulation (GDPR) comes into effect on 25 May 2018. Public sector technology specialists PublicTechnology (https://www.publictechnology.net/) highlight 10 of the key questions and answers following its recent GDPR summit.

Q1 Will Brexit render GDPR irrelevant?

It's tempting to think that our scheduled exit from the EU makes the regulation a legislative lame duck but, with the Data Protection Bill, the government is effectively signing GDPR into UK law, and introducing some additional measures to boot.

Q2 What's happening with the Data Protection Bill?

It's successfully completed its House of Lords stages and was presented to the House of Commons for its first reading on 18 January 2018. There was no debate at this stage so it now continues through the remaining four stages in the House of Commons before attaining Royal Assent and becoming law.

Q3 Whom should you appoint as a data protection officer?

An individual's experience is more important than letters after their name according to Jonathan Bamford, head of parliamentary and government affairs at the Information Commissioner's Office (ICO). He also explains that, although they are required to report directly to an organisation's board, this does not have to mean a direct reporting line. Monthly or six weekly reports are sufficient. Bamford also stresses the importance of having a team and sufficient resources to support a data protection officer.

AON
Empower Results®

Q4 How will data subjects react to the introduction of GDPR?

Under GDPR, citizens have a number of additional rights in respect of access to information on what data is held on them and how it is processed. These include the right to obtain information on how long data is stored; whether they have the right to request erasure or otherwise object to their data being processed; justification for automated processing procedures; and additional information on data sources.

Paul Woods, head of library services operations at the Government Legal Department, says public sector organisations will see an initial rush of requests for information as people look to exercise their new rights, but does not expect this to be unmanageable. He adds: "We have to be able to demonstrate a willingness to be transparent about how we process people's data."

Q5 What should be your legal basis for processing people's data?

Under GDPR there are six ways to establish a legal basis for data processing, of which five are applicable to the public sector. Obtaining a data subject's consent may appear to be the easiest and cleanest option but Bamford warns against this. "You need to be careful because consent is a very high standard. It has to be very specifically given, evidenced in some way and it is capable of being withdrawn. If you need to process people's data irrespective of whether they say you can, you cannot rely on consent as a legal basis."

Other options include demonstrating that data processing is necessary for the purposes of the fulfilment or creation of contract between the data processor and the subject; proving that processing data is necessary for the purposes of complying with another legal obligation; and demonstrating that it is done to protect an interest which is essential for the life of the data subject or that of another person.

However, the option that is likely to be used most often within the public sector is to prove that processing is required to perform a task that is in the public interest, or forms part of 'the exercise of official authority vested in the controller'.

Q6 Who is ultimately accountable?

Data controllers are organisations or people with responsibility for defining how and why data is processed while processors simply carry out such processing on behalf of controllers. Public sector bodies are invariably controllers, while the technology firms that provide their data processing tools and services are processors.

Controllers are ultimately responsible for the legality of data processing but GDPR tips the balance a little, with processors potentially also bearing responsibilities.

The ICO currently advises that contracts between public bodies and their commercial data processing partners do not 'relieve the processor of its own direct responsibilities under GDPR, and reflect any indemnity that has been agreed'.

It is also working towards creating a code of conduct to help all parties understand their obligations and liabilities and create contracts accordingly.

In light of the changes, incumbent contracts may need to be revisited.

Q7 What does GDPR mean for public bodies sharing data with each other?

The question of liability becomes even thornier when the two parties sharing data are both public sector entities. Although data is typically shared under the protection of a non-legally binding memorandum of understanding agreement, it is unlikely that this will be sufficient under GDPR. No guidance has been issued but we expect a more formal contract will be required where data is shared.

Q8 What should public bodies do when they suffer a breach?

Where a data breach occurs that is likely to result in a risk to people's rights and freedoms, this must be reported to the ICO within 72 hours of becoming aware of it.

The ICO's Bamford cautioned against delaying to allow time to assemble a detailed report and plan of action. "Report as soon as you're able," he says. "We need to know that something has gone wrong and you're dealing with it."

Q9 How much could non-compliance cost?

Fines for contraventions have attracted the most attention and not surprisingly so as penalties are significant under GDPR. While the maximum fine under the Data Protection Act is £500,000, GDPR raises this maximum to 2% of global turnover or €10m for lesser incidents and 4% of turnover or €20m for more serious breaches.

Putting this into context, GDPR would have increased TalkTalk's record £400,000 fine into one for £59m.

Q10 What happens if there's a breach on 24 May?

Although GDPR comes into effect on 25 May, there is a possibility that a number of incidents will straddle both pieces of legislation. As an example, Bamford was asked which piece of legislation would apply if a breach occurred on 24 May and was reported two days later on 26 May. Although he didn't have a definitive answer, he pointed out that the law should not be seen merely as a document but as a living entity. "We want to get organisations on the front foot and incentivise them to do the right thing," he says. "It's about ensuring public trust and confidence in how data is used."

Thanks to PublicTechnology for enabling us to reproduce this informative Q&A session.

Contact Bill Sulman at bill.sulman@aon.co.uk to find out how Aon can support your GDPR preparations.