SEDDONS

On your side

GDPR: Are You Ready?

What is GDPR?

On 25 May 2018 the General Data Protection Regulations, or "GDPR", will replace the Data Protection Act 1998 ("DPA"). Under the GDPR, individuals will have increased rights of access and control in respect of their personal data. and the regulator (the Information Commissioner's Office "ICO") will have greater powers. This includes the ability to levy fines of up to 4% of a business' annual turnover, in the event of breaches of data protection.

Why the change?

In order to better understand GDPR we need to place these changes into context.

Over the last decade we have seen major advances in technology with smart phones and smart meters etc – the "fourth industrial revolution". These advancements have radically increased the ease with which data may be collected, transmitted, stored, manipulated and, most importantly, disseminated. People are now more aware of how this technology can potentially compromise their right to privacy.

It is not just Europe that has introduced stronger privacy laws. The number of jurisdictions with data protection or privacy legislation has increased significantly during the last decade and the list continues to grow.

The thinking behind the GDPR is that by empowering individuals "data subjects", requiring organisations "data controllers" to justify how they process data and giving regulators increased punitive powers, the imbalance of power between individuals and businesses created by the advances in technology can be better contained.

And Brexit?

Any business outside the EU that sells goods and/or services to people in the EU or monitors the behaviour of EU citizens will be subject to GDPR. The UK Government will implement data protection laws which mirror the EU's. The Data Protection bill puts the GDPR onto the UK statute book so it will remain regardless of Brexit.

What changes does GDPR bring?

For data controllers

We start with the major conceptual change and then highlight several specific changes.

With the DPA, in order to lawfully process personal data, data controllers have to register with the regulator – the Information Commissioner's Office (ICO). Data controllers have to then abide by the seven principles of data protection. Seddons, for example, as a law firm is registered to process the personal data of its clients and employees etc.

GDPR retains the seven principles, which are broadly unchanged. However, the GDPR asks data controllers to record how data is processed and ultimately, if required, to justify its procedures to the ICO. The GDPR requires this to be recorded but it is best practice to go beyond recording this and to audit it. This

requirement to internally record the data replaces the need to register with the ICO before processing personal data. The ICO will expect each data controller to explain how it processes personal data and how that processing meets the principles.

The specific changes include:

1. Data controllers have to inform the ICO of any breach within 72 hours;
2. Any specific change to working practices will require a Privacy Impact Assessment;
3. Any outsourcing of data to a data processor (e.g. to a payroll company) must be documented with certain clauses being mandatory;
4. In order to show that an individual has "consented" it will not be enough to say that because the individual has not objected, that consent is a given. Consent under GDPR will require a positive action.

For individuals

The rights of individuals are greatly enhanced – they have the right to:

1. Access their data (subject access request (SAR));
2. Control how their data is processed – this includes the right to be forgotten, have data rectified or ensuring that the data controller restricts the processing of data;
3. Compel a data controller to move the data to another controller.

The headline points are that the £10 fee will go and the controller has less time in which to respond (a month rather than the current 40 days).

The bigger point is that these increased rights are worthless without the increased powers of the ICO to ensure that data controllers respond to these requests.

For the ICO

As is widely reported in the media, the ICO has the power to fine up to 4% of a data controller's turnover or €20million, whichever is greater.

Why is the Data Audit crucial?

In addition to positioning the data controller to deal quickly and proactively with any approach from the ICO, the data audit is an opportunity for a business to "spring clean" its procedures. Given that the processing of data is at the heart of how most businesses operate, by auditing this process the data controller will learn how its operations currently work and can be improved. The data audit should be seen as an opportunity, and not a meaningless administrative task.

Turning to the GDPR angle:

1. Having the audit available will enable the data controller to deal quickly and proactively with the ICO. By contrast a data controller without this information will be on the backfoot with its dealings with the ICO. If a data controller has merely recorded the processing of data but not analysed this, the ICO may well highlight and punish breaches that an audit would have rectified.
2. The audit enables the data controller to risk assess how it processes data, by way of an example – if data is being transferred outside the EU, what emails are encrypted? How long is data archived? How are redundant IT equipment/ devices disposed of? And have the data subjects consented to the processing

of their data?

3. We expect there to be a plethora of SARs following GDPR. If the data controllers have not documented where the data is the workload caused by a SAR will be unnecessarily labour intensive and challenge the one month turnaround requirement.

So our conclusion is that although the statutory requirement is to record, it is difficult to see how a data controller can show compliance with the principles if it has not audited and risk assessed the information.

Apart from the Data Audit what should be done between now and May?

The ICO expects each data controller to have a programme of staff training. Whereas breaches of some laws only involve management, breaches of data protection can be done by anyone. If no one knows what a data breach is then the breach cannot be reported or rectified.

The ICO expects each data controller to prepare a set of bespoke policies setting out how it processes data, and what happens if there is a breach.

The ICO expects each data controller to have a privacy notice which sets out how and why it processes personal data.

Every data controller must report breaches. Therefore the ICO will expect to see what breaches were not reported and the procedure behind the decision not to report.

Penalties

Under the GDPR, major breaches by data controllers can attract a fine of up to a maximum of 4% of their annual turnover or €20million, whichever is greater. Even minor breaches can carry fines of up to €10million or 2% of annual global turnover. A minor breach can be a failure to maintain training records or up to date procedures.

There is a lot of speculation as to how rigorously the ICO will enforce the GDPR. We understand the ICO has already identified a “hit list” of certain organisations which it will approach next summer. The ICO will have greater resources in terms of budgets and manpower and will be able to investigate complaints in more detail.

From our dealings with the ICO we suspect that the ICO will take a holistic approach. The role of a regulator is to pre-emptively deal with likely future risk. So regulators will expect to see training records, procedures, a breach register etc. If there is a “one off” breach – including unencrypted emails sent to the wrong person, documents left on a train etc, then the “firewall” of good procedures will mean that the ICO will be more understanding. By contrast, if there is a minor breach that shows bigger problems - a SAR is not completed in time but the ICO discover that there are no procedures, no record of data processing etc, then that controller is more likely to be fined than the controller whose breach was more serious but a “one off” incident despite the procedures.

SEDDONS

Helen Crossland

+44 (0)20 7725 8034
Helen.Crossland@seddons.co.uk

Helen is head of our Employment team. She has extensive experience of all aspects of contentious and non-contentious employment law including Employment Tribunal and High Court claims, exiting employees, TUPE issues, enforcing post-termination and confidentiality restrictions, and drafting bespoke employment documentation.

Helen acts for businesses of all sizes, including start-ups, SME's, charities and not for profits, and international organisations. She has a stunning track record of successfully defending claims and securing costs for her clients and her advice commonly results in claims being averted or withdrawn.

Alexander Egerton

+44 (0)20 7725 8030
Alexander.Egerton@seddons.co.uk

Alexander is a partner in our Corporate department. He advises a number of businesses on all commercial issues. Many of his clients are in the technology and media sector.

His work in the corporate team involves working with clients through each stage of a business's 'life' from choice of structure, share incentives, raising finance, putting a legal infrastructure (regulatory requirements, contracts etc.) in place and ultimately in working to ensure that there is a viable exit strategy in place.

Published: 21.09.2017
Updated: 09.02.2018

5 Portman Square
London
W1H 6NT

www.seddons.co.uk