SEDDONS

On your side

GDPR: Where are we now?

GDPR's Third Birthday

On 25 May 2018, the General Data Protection Regulations, or "GDPR", replaced the Data Protection Act 1998 ("DPA"). Three years later, the GDPR may no longer attract much press coverage, but we consider that GDPR compliance has to remain on every business' in-tray. We have already seen the UK Privacy Regulator, the ICO, use its powers to levy substantial fines. As many businesses have to become predominantly online following the coronavirus pandemic, the volume of personal data will only increase. However, the GDPR is not about "Project Fear" and fines - we see GDPR compliance as adding value to any business.

Following Brexit, the UK has "cut and pasted" the GDPR into UK law – the UK GDPR. We conclude this article by identifying two changes that Brexit has imposed on UK businesses that handle the personal data of EU citizens.

What is the GDPR and How do you Comply?

In order to better understand the GDPR, we need to look at recent changes to technology and how we all use that technology.

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. Under the GDPR, individuals have increased rights of access and control in respect of their personal data. The regulator, the ICO, has greater powers. This includes the ability to levy fines of up to 4% of a business' annual turnover.

The view was taken that the 1995 EU Directive could not properly regulate this new world of big tech and smart technology – hence the GDPR.

Why Comply - the GDPR Dividend

At its most basic, the GDPR is a risk assessment process asking data controllers to record how and why data is processed; how secure are the systems and for how long is the data retained? The GDPR requires these data flows to be recorded, but it is best practice to go beyond just recording, and also to audit. The audit process will help a business identify weaknesses in its procedures. Even without the GDPR, the audit is an invaluable management exercise. Given that the processing of data is at the heart of how most businesses operate, by auditing data flows, the data controller will learn how its operations currently work and where there is room for improvement. The data audit should be seen as an opportunity, and not a meaningless administrative task.

Beyond the risk assessment, there are specific action points that the GDPR entails.

The GDPR Action Points

- Data controllers have to inform the ICO of any breach within 72 hours.
- Most changes to working practices will require a Privacy Impact Assessment.
- Any outsourcing of data to a data processor (e.g. to a payroll company) must be documented with certain clauses being mandatory.
- To show that an individual has "consented" to their data being processed, a positive action will be required. It will not be enough to say that because the individual has not objected, that consent has been given.
- The Privacy Policy has to be made accessible, and is a mission statement as to how personal data is processed. It will also explain to data subjects the rights they have under the GDPR and how to exercise them.
- A data controller has a month in which to deal with any requests lodged by a data subject regarding their data, and needs to do so free of charge. This will typically be an access request which will involve trawling through files and emails to identify that person's data. If there is a data audit, dealing with an access request becomes easier.
- Staff training?

The Impact of Brexit

Although the UK privacy regime remains largely unaltered, the landscape has changed for UK businesses that work with EU consumers.

Brexit Change Part One – the EU Representative

Any UK company that processes a certain volume of personal data of EU citizens, or data that is high risk, will have to consider appointing a representative in the EU. The representative will deal with the EU citizens regarding access requests, and the EU regulators in place of the UK company. If a company that should appoint a representative fails to do so, the potential fine is up to 2% of turnover.

If the appointment is considered a tick box exercise with price being the sole determinant, then this may cause problems. The representative must have an understanding of the data that the UK company processes. If the two parties cannot work together, both parties expose themselves.

The best advice is to look at this appointment for what it is. The representative is an extension of the UK company's brand, and deals with the UK company's customers with no oversight from the UK company.

Any UK company considering appointing a representative should look carefully at the bona fides of the representative and document the following:

- What documented due diligence was conducted prior to appointment?
- Does the representative have the experience of dealing with its local regulator?
- Is there insurance cover?
- Is there a contract in place that allows the UK company to recover losses if there is a problem?

Brexit Change Part Two – EU to UK Data Transfers

If personal data is transferred from the EU to the UK, then the EU company may conduct due diligence on the UK company. The EU has strict rules regarding transferring data outside of the EU. In order to reduce disruption and maintain the business relationship, the UK company will have to respond quickly, and should take the following actions:

- The UK company should self-audit. It can then pre-empt any request from the EU company by disclosing its own internal due diligence first.
- If the UK company is familiar with the standard contractual clauses or other safeguards, it will be able to agree these quickly.
- The GDPR has other safeguards allowing on data transfers outside the EU. One of these may be more applicable. If the UK company identifies one, it can pre-empt the approach by the EU company.

A proactive approach can only enhance the business relationship.

Our Team

This note touches on a lot of issues. If you have any queries, please contact a member of our team.

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.

Alexander is our Privacy Compliance Officer, responsible for ensuring that we are GDPR compliant. He is also an active member of the IAPP – the International Association of Privacy Professionals.

George de Stacpoole

+44 (0)20 7725 2032
george.destacpoole@seddons.co.uk

George is an Associate in the Corporate Department. He advises on a full range of corporate transactions including private mergers and acquisitions, equity fundraisings and shareholder arrangements, joint ventures, share buybacks, corporate re-organisations and general corporate advisory for small to medium sized companies. George also acts for a number of entrepreneurs, assisting them with early stage fundraisings, corporate advisory, and other legal issues affecting start-up companies, including compliance with the GDPR regime.

Richard Raban-Williams

+44 (0)20 7725 8061
richard.raban-williams@seddons.co.uk

Richard is an Associate in our Dispute Resolution team. He has an interest in privacy law and assists the Corporate Department when GDPR issues become contentious. Richard is also involved in the provision of UK GDPR Representatives services to our clients who are not based in the UK but process the personal data of UK citizens.

SEDDONS

About Us

Seddons is a top 200 law practice based in London's West End, with a strong reputation for both commercial and private client work. We advise our UK and international clients on personal and commercial disputes, real estate law, family law, estate planning, corporate law, employment law, and more. Seddons achieves the best possible outcome, with the professional and interpersonal skills needed for sensitive matters, complex technical work and cross-practice issues. Working alongside other professionals to protect clients' financial and emotional interests. Our clients are from varied backgrounds, with an emphasis on business owners and professionals, and regularly act for high-profile clients, understanding the importance of preserving confidentiality and reputation with utmost discretion.

Contact Us

To discuss how we can help with any legal matters, or should you have any questions, please contact us on **020 7725 8000.**

Seddons

5 Portman Square
London
W1H 6NT

www.seddons.co.uk

020 7725 8000

5 Portman Square
London
W1H 6NT

www.seddons.co.uk