A NO NONSENSE GUIDE TO GDPR

THIS IS A PRINT FRIENDLY VERSION OF OUR GUIDE

thrings.com

@ThringsLaw

WHAT IS THE GDPR?

The General Data Protection Regulation (GDPR) is a piece of EU legislation which is automatically incorporated into UK law. It is intended to strengthen and bring greater harmonisation to data protection laws across the EU. It will come into effect, regardless of impending Brexit, and the UK Data Protection Bill is highly likely to ensure that the GDPR will remain in force in the UK even once Brexit takes place. The GDPR introduces new obligations and rights as well as increased enforcement powers. The new maxim for data protection is "privacy by design, privacy by default" and penalties for breach can be up to 4% of worldwide annual turnover or €20,000,000

WHEN DOES THE GDPR COME INTO FORCE?

It automatically becomes effective on 25 May 2018 and will replace the existing UK Data Protection Act 1998 (DPA). Although you will not need to comply with the GDPR until 25 May 2018, it is advisable to start planning and implementing the necessary changes to your business practices and procedures as early as possible.

DOES THE GDPR APPLY TO ME?

There will be very few businesses to whom it does not apply. If you hold personal data of any living individual then the GDPR will apply to you in one way or another and don't forget this includes personal data about your employees. Unlike the DPA, the GDPR directly applies to data processors as well as data controllers, and has a wider territorial ambit than the DPA. The GDPR not only applies to processing of data carried out by organisations operating in the EU but also to organisations outside the EU that offer goods or services to individuals in the EU, whether or not those goods or services are paid for.

DOES THE GDPR APPLY TO INFORMATION I HOLD?

Like the current DPA, the GDPR applies to "personal data". If you hold data which falls within the DPA then it will also fall within the GDPR. However, the GDPR definition of personal data is wider, partly to take account of changes in technology and the way organisations collect information. As well as details of staff, customers and contacts, the wider definition also includes a range of personal identifiers (such as IP addresses). The categories of "sensitive personal data" are broadly similar to those under the Data Protection Act but they now also specifically include genetic data and biometric data where it's processed to identify an individual. Criminal convictions are no longer classified as "sensitive personal data" but are now covered by their own specific safeguards.

WHAT RIGHTS DO INDIVIDUALS HAVE?

The rights of individuals (data subjects) have been extended. They include:

- The right to be provided with a privacy notice.
- Confirmation of whether you process personal data about that individual and the right to access that personal data (together with certain information about the processing in question).
- The right to rectification of the data.
- The right to erasure of the data in certain circumstances.
- The right to restrict certain processing of personal data.
- The right to portability of the personal data to the individual or another data controller.
- The right to object to certain processing.
- The right not to be subject to automated data processing.

HOW CAN I SHOW THAT I COMPLY WITH THE GDPR?

The GDPR does away with the requirement to register ("notify") with the Information Commissioner's Office (ICO) but imposes a new obligation of "accountability". This requires more than just establishing data protection policies and procedures - you will have to be able to demonstrate compliance e.g. by:

- Implementing internal data protection policies such as staff training, internal audits of processing activities, reviews of internal HR policies.
- Establishing a data protection compliance programme and privacy governance structure.
- Implement and maintain privacy controls on an ongoing basis by integrating data protection into your systems.
- Adopting ongoing privacy measures as part of your corporate policies and day to day activities (e.g. internal policies and procedures on handling personal data, obtaining valid consents, maintaining data quality, anonymising and pseudonymising data where appropriate, compliance with a personal data retention policy, and secure destruction of personal data.)

You should also take the opportunity to review the personal data you currently hold on clients and contacts, and also check the wording of your current policies, notices, contracts etc.

DO I HAVE TO CARRY OUT A DATA PRIVACY IMPACT ASSESSMENT (DPIA)?

Not necessarily. A DPIA is required where processing of personal data is likely to result in a high risk to the rights and freedoms of individuals. (That might occur when you introduce new systems or processes or when you make changes to your systems or processes, for example) A DPIA is required if you are involved in automated processing, large scale processing of sensitive data or large scale, systematic monitoring of a publicly accessible area. However, being able to demonstrate that you have considered the rights of individuals and the risks posed to them by your data processing will help you with your accountability obligation (see above).

DO I NEED A DATA PROTECTION OFFICER?

You only have to appoint a Data Protection Officer if you are a public authority, or carry out large scale systematic monitoring of individuals (e.g. online behaviour tracking) or carry out large scale processing of sensitive personal data or data which relates to criminal convictions and offences. However even if you are not required to appoint a DPO, you must ensure that your staff have the appropriate skills to comply with the GDPR and it may be prudent to appoint a member of staff with principle responsibility for GDPR compliance -again, this will assist with demonstrating accountability (see above).

DO I HAVE TO SIGN UP TO A CERTIFICATION SCHEME OR APPROVED CODE OF CONDUCT?

No, it is not a requirement. However if there is an approved code of conduct which is relevant to your processing of personal data, you may find it beneficial to work towards compliance with it.

WHAT HAPPENS IF I BREACH THE GDPR?

The GDPR imposes new obligations in the event of a breach of security which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. If the breach is likely to result in a risk to the rights and freedoms of individuals then you have to notify the ICO. If the breach is likely to result in a high risk to the rights and freedoms of individuals then you have to notify the individuals affected. Short deadlines (typically 72 hours) will apply and there is the possibility of a claim for compensation if an individual suffers damage as a result. Although there is also the risk of a serious fine for a breach of any obligation under the GDPR, the ICO has made it clear that its first resort will be to advisory and corrective action.

CAN I TRANSFER PERSONAL DATA ABROAD?

As with the DPA, there are restrictions on the transfer of personal data outside the EU. As with the DPA, you can only transfer personal data outside the EU where the organisation receiving it is covered by adequate safeguards and there are a variety of ways in which that can be done. However, the obligation is on you to demonstrate that those appropriate safeguards exist.

WHAT DO I NEED TO DO NEXT?

To an extent, the GDPR can be thought of as a refresh and a reboot of the existing law. However there are crucial differences to be aware of, in terms of both general approach and detailed application, which may not be immediately obvious even to experienced data protection managers.

For an appointment to discuss your business' specific position under the GDPR and its future data protection requirements, please call or email Thrings.

KEY CONTACTS

GRAEME FEARON

Partner | Intellectual Property
+44 (0)117 930 9557
+44 (0)7717 573 479
gfearon@thrings.com

MARY CHANT

Partner | Commercial
+44 (0)2380 930 321
+44 (0)7788 257 473
mchant@thrings.com