GDPR: Top Ten Facts Businesses Need to Think About Now

bto solicitors

The General Data Protection Regulation (GDPR) will have direct effect throughout Europe from 25 May 2018. The UK will still be in Europe at that time. The Government has confirmed that UK businesses will need to comply.

Post-Brexit there are unlikely to be many changes as the GDPR standards are likely to remain the same to allow the UK to do business with Europe.

What do businesses need to think about now:

1. ***Lawful Processing and Consent:*** It will become much more difficult to obtain valid consent under the GDPR but there are other lawful bases which have been ignored under the DPA. Businesses must identify what lawful basis it is relying on: is it necessary for you to gather the data for the performance of a contract; is it necessary for you to share the data because of a legitimate interest you have?

2. ***Transparency and Fair Processing:*** Any processing must also be done fairly which means telling individuals what you are doing with their data even if you do not require their consent. Under the GDPR you must provide the following information in a Privacy Notice when you collect their information: your identity; the purpose for processing; the legal basis for processing; the categories of personal data concerned; the recipients of personal data if any; and the safeguards in place if data is to be transferred to a country outwith the EU. Other information must also be made available such as the how long you will keep the data and a list of the rights each data subject has.

3. ***Data Protection by Design and Data Privacy Impact Assessments:*** For any new project if there is likely to be a high risk to the privacy rights of individuals then a DPIA should be carried out and in particular this refers to large scale processing of sensitive data; systematic monitoring of a public area and automated processing where the decisions have a legal or significant impact on individuals.

4. ***Accountability and Recording Data Processing:*** If you have over 250 employees or your processing is likely to result in a risk to the privacy rights of individuals then you must maintain a record of processing including the purpose of your processing; the categories of data you are processing; the recipients of data including if they are in a third country.

5. ***Data Protection Officer:*** Certain organisations will require to have a DPO to advise on GDPR compliance. This individual cannot be someone who makes decisions about data processing but should have access to the Board. The responsibility remains with the data controller; the organisation in control of the data. If you are a public authority; if your core activity is processing large amounts of sensitive personal data or if your core activity involves systematic monitoring, then you must have a DPO.

6. ***Data Subject's Rights:*** There are some enhanced and some new rights and organisations must have a system in place to deal with them. The timescales are tight for compliance. Subject access requests must be complied with in 30 days. In certain circumstances there is a right to be forgotten; a right to restrict processing and a right to object to processing. There are new rights concerning automated decision making and a right to move your data from one provider to another – data portability.

7. ***Children:*** If you are processing the data of children you must decide whether you need to have a system in place to confirm their age and to obtain parental /guardian consent if you are offering online services. Information provided to a child should be in an easily understood format. Under the GDPR a child is defined as under 16 however the UK may reduce that age to under 13.

8. ***Data Controllers and Data Processors:*** Both now have obligations to comply with the law and both can be investigated and fined. Any contract a data controller has with a processor must contain certain terms set out in the Regulation to ensure compliance and to ensure that the controller is aware of any sub-contractors.

9. ***Personal Data Breaches:*** A personal data breach must be reported to ICO without undue delay and within 72 hours of it being discovered unless there is likely to be no risk to the privacy rights of any individual. If there a high risk to the privacy rights of individuals then they must also be notified without undue delay.

10. ***ICO Powers:*** The ICO will have the power to impose significantly increased levels of fines up to a maximum of €20 million or 4% of global turnover, whichever is higher for processing breaches (not just personal data breaches), and €10 million or 2% global turnover for the more administrative breaches.

Guidance Updates from now until May 2018

European Guidance from the Art 29 Working Party (WP29)

The following Guidelines have been adopted by the WP29 following a consultation period which ended on 29 January 2017:

- Data Protection Officers
- The Right to Data Portability
- The Lead Supervisory Authorities

The Draft Guidelines in relation to Data Privacy Impact Assessments were out for consultation and closed on 23 May 2017. The WP29 has also indicated that it will produce Guidelines in relation to the following areas:

- Administrative fines
- Certification Profiling Consent
- Transparency
- Notification of personal data breaches
- Tools for international transfers

UK Guidance

The ICO's **Overview of the GDPR** provides more detail and contains its '12 Steps to Take Now' document. This is a living document which will be updated from time to time as further guidance is produced from Europe and the Government. There is also a **self-assessment tool** to assist you to prepare. The latest **Code of Practice on Privacy Notices** also included reference to the information that the GDPR will require to be included in notices come May 2018.

The ICO's **Draft Guidance on Consent** was issued in March 2017 and the final version is expected in June 2017 although it is understood that there were more than 300 responses and that this time scale may slip. This changes the requirements to obtain valid consent considerably and thought should now be given to this issue in particular.

Most recently the ICO produced **Draft Guidance on Data Profiling**. Responses were due by 28 April 2017 with final guidance to follow.

We are still waiting on the Government advising us and the ICO about what will happen with the Data Protection Act 1998 and the 50 areas set out in the GDPR where Member States can exercise discretion about how the GDPR will apply in each country. The Department for Culture Media and Sport issued a consultation paper asking for comment on each of these prior to the general Election in 2017. There is no additional information in the document. It simply identified the areas where there is discretion and asked for comment. The **ICO's Response** provides some insight into its thinking and is worth a read.

BTO Solicitors LLP also has its own **GDPR Website** which is updated regularly and can assist with any data protection queries you may have. Please contact :

Laura Irvine
Criminal Solicitor Advocate

E: lji@bto.co.uk
T: 0131 222 2939

Paul Motion
Solicitor Advocate Partner

E: prm@bto.co.uk
T: 0131 222 2939

@btodataprotect **www.bto.co.uk/gdpr**

SHARE this update with your contacts and colleagues.