trowers & hamlins

Flyer ——— Marchl 2016

Data protection
Gearing up for the General Data Protection Regulation: What you need to know —— March 2016

The law in relation to the processing of data is to be subject to a major overhaul as agreement has finally been reached in Europe on changes necessary to reflect the way we live and work in the 21st century. As the first step in this process, the ICO has issued a 12 step checklist of steps to take in preparing for the new regime.

The current state of play

The last four years have seen what seemed, to many, a painfully protracted debate in Europe concerning changes to the law on data protection.

Changes are long overdue, the original European Directive and its implementation in the UK by way of the Data Protection Act (DPA), dating back some 20 years, since when the manner in which data has been used in business has changed beyond all recognition.

Finally, agreement appears to have been reached on the wording of a new General Data Protection Regulation (GDPR), and its formal adoption is expected imminently.

Alongside these developments, concerns for business who transfer data overseas continue following the European Commission striking down the "Safe Harbour" regime enabling the transfer of data to the US, and in relation to which a new EU - US Privacy Shield is to be introduced. In addition to significant changes in the law, the Information Commissioner's Office continues to call for custodial sentences as well as fines for breaches of the law.

Although there will be a two year period before the GDPR becomes law, businesses should use that period to wisely to prepare themselves for the changes ahead. Many of the concepts and principles under the GDPR remain the same as those under the DPA, but there are significant changes.

Fines

The sanction which can be imposed for a breach of the law, and which is currently set at a maximum of £500,000 in the UK, is to be increased to the higher of 4% of an undertakings worldwide turnover or €20 million. It is intended that breaches will be grouped into different categories with maximum fine levels for each. Whether criminal sanctions can be enacted are matters to be left to member states, and indeed, section 77 of the Criminal Justice and Immigration Act 2008 makes unlawfully obtaining personal data punishable by up to two years in prison. This provision is not yet in force, but as mentioned above, it is the clearly stated wish of the Information Commissioner that custodial sentences should apply.

Source: Fotolia

Consent

The requirement to obtain consent before processing individuals' data is likely to be more onerous under the new legislation than at present. Consent must be unambiguous and given either through a statement or clear affirmative action. Consent must be "freely given, specific, informed and unambiguous" and must be a positive indication of agreement. It cannot be inferred from silence, pre-ticked boxes or inactivity. It cannot be buried in an agreement in which there is a significant imbalance of power, such an employment contract. If challenged by the ICO, it will up to an organisation to demonstrate that consent was given, underlining the importance of an effective audit trail.

Published by
Trowers & Hamlins

Trowers & Hamlins LLP
3 Bunhill Row
London
EC1Y 8YZ

t +44 (0)20 7423 8000
f +44 (0)20 7423 8001

www.trowers.com

It must be as easy to withdraw as to give consent, and data subjects must be made aware of this.

Privacy notices

Individual's rights in relation to data processing, in addition to the stricter consent obligations, are reflected in changes to the privacy notices which must be issued. There are specific obligations under the GDPR requiring businesses to explain the legal basis for processing data, data retention periods, the rights of individuals to complain about the way in which their data is handled and the right to be 'forgotten'. This information needs to be provided in clear language.

Accountability

There is to be an increased emphasis upon accountability, and the maintenance of records demonstrating the data that is held, where that data is derived from, who it is to be shared with, and that there are effective policies and procedures in place to protect this. The ICO will have the power to require evidence of compliance upon request, and although the anticipated provision that all organisations must have a formally appointed data protection officer have not been adopted, save for public bodies and those whose core activities consist of processing large scale data, the increased accountability will require the appointment of someone within an organisation to have overall responsibility for data matters.

For the first time, data processors, and not only data controllers, will be liable for fines and subject to claims by data subjects. This, in turn, is likely to result in an insistence by data processors on greater contractual protection in their arrangements with data controllers.

Breach notification

As for the requirement to notify a breach, this is at present limited to "significant" breaches. All breaches will need to be reported to the ICO once the GDPR is in place, unless the breach is unlikely to result in a risk to the data subject, which must be undertaken promptly and within 72 hours. This again underlines the importance of ensuring that there is coordinated responsibility within an organisation for data matters.

Subject access requests

There are also changes in relation to dealing with subject access requests. The general obligation to make a payment will be removed, although there will be additional grounds for refusing to comply with a request, and the possibility of charging a reasonable fee where a request is unfounded or excessive. The time period for dealing with a request, however, is to be reduced from 40 days to 30 days.

The Information Commissioner's Office has this month issued guidance identifying 12 steps which organisations can take, to ensure that they prepared for the new regime. These steps focus on the main changes proposed by the law, with an emphasis on preparing for the enhanced obligations on recordkeeping and seeking consent to processing.

Individuals' own rights are also enhanced, including a right to data reportability under which an organisation will be obliged to provide data electronically, and in a common format. The wording of privacy notices and the manner in which consent for processing is obtained will all need to be reviewed.

With an eye to this, the ICO is currently consulting on a privacy notices code of practice, in which it proposes a "blended approach" to present privacy information, including "just in time notices" – a notice appearing on screen at the point at which personal data is inputted, together with a breach message explaining that information will be used and an opt-out mechanism; video presentations and privacy dashboards - one place from which to manage what is happening to information.

Guidance has also been issued on conducting Privacy Impact Assessments to comply with the principles of the GDPR concerning data protection "by design and by default".

We would be delighted to help you prepare for these changes which will have a profound impact on the way in which data must be handled, if the risk of significant fines is to be avoided. We can review your existing policies and practices, data sharing agreements and where required advise you in detail of the ramifications of the new legislation.

For more information please contact

Richie Alder
Partner
t +44 (0)20 7423 8593
e ralder@trowers.com

Helen Cookson
Senior Associate
t +44 (0)161 838 2081
e hcookson@trowers.com

Cara Gillingham
Associate
t +44 (0)20 7423 8619
e cgillingham@trowers.com

Alex Razak
Solicitor
t +44 (0)20 7423 8082
e arazak@trowers.com