An introduction to the General Data Protection Regulation

Twenty years is a long time given the fundamental changes to the way in which we seek, store and share information. The Data Protection Act 1998 will therefore shortly be replaced with the General Data Protection Regulation (GDPR). This is intended to strengthen the rights of data subjects in this digital age by introducing enhanced obligations upon organisations processing personal data.

The GDPR is directly applicable European legislation which will be brought into force in May 2018. The Government also intends to incorporate the contents of the GDPR into a new Data Protection Act which will continue to apply after our exit from the European Union. There is no intention to dilute the terms of the GDPR.

What difference will the GDPR make to my organisation?

The Information Commissioner's Office (ICO) has demonstrated repeatedly that it will take enforcement action against organisations which take an irresponsible approach to handling personal data. Alongside the range of other enforcement action it is able to take, the ICO will soon be able to impose a maximum fine of 20 million euros or 4% of your organisations annual turnover. The Information Commissioner has reassured data processors that issuing fines will continue to be a last resort under the new regime, whilst at the same time emphasising that enforcement measures such as warnings, reprimands and corrective orders can deliver a significant blow to your organisation's reputation.

If irresponsible data handling can damage your organisation, the converse is also true. Data is an asset and ensuring that you have got proper data handling systems in place means that your organisation can profit from this asset, whether by minimising storage costs, enhancing your ability to learn from the data you hold or maintaining a trusting relationship with your customers.

What are the changes which will affect my organisation?

Whilst the existing data protection principles remain essentially unchanged, certain practical aspects of the legislation have been strengthened. Guidance on topics such as consent, notification of breaches and international transferred will be issued by both the ICO and the Article 29 Working Party in the months ahead of the GDPR coming into force. However, none of the changes required can be implemented overnight and so it is important to commence the process of review and change now. Some of the key changes are:

The new principle of accountability

Organisations must now be able to demonstrate compliance with the GDPR's principles. In the event of a data protection breach, this will be a critical element of your organisation's notification to the ICO. This will involve a review of your organisation's data handling practices and procedures, followed by the implementation of practical measures to ensure that personal data is handled by every member of your organisation in compliance with those principles. This will involve assessing risk, integrating privacy measures into your day to day data handling processes, implementing policies, training staff, undertaking audits, recording breaches and maintaining up to date records every step of the way.

New requirements for Data Protection Officers

Data Protection Officers (DPOs) will now be required by organisations which are: public authorities, or involved in regular and systematic monitoring or the large scale processing of sensitive data. This statutory role has clearly defined responsibilities. The individual is required to remain independent to the organisation which employs them and owes specific obligations to the ICO. Careful consideration needs to be given to whether a DPO should be appointed or whether an equivalent post can be created to ensure compliance without the associated statutory obligations.

More detailed information notices

The ICO has long promoted the use of plain, concise and prominent information notices. The GDPR requires significant amounts of further detail to be included such as the precise nature of legitimate interests you rely upon to process personal data, retention periods, the source of data and details concerning how an individual can exercise their rights under the GDPR. Consideration will need to be given to the drafting of your organisations notices, along with the way in which these are made available to individuals whose data you are processing. More fundamentally, your organisation will need to assess and clarify the bases upon which you are legitimately able to process personal data.

Stricter requirements for consent

Currently, obtaining the consent of an individual generally provides an organisation with a sound legal basis upon which it can process that data. Under the GDPR, consent remains one possible condition enabling processing but it must be freely given, specific, informed and able to be withdrawn. Once withdrawn, if there is no other basis upon which an organisation may process the data, the organisation will have no option but to erase the relevant data. The ICO has specifically stated that organisations should take care not to rely on consent where there are other conditions which apply, including where it has a “legitimate interest” in processing.

A new right to data portability

Alongside the existing rights to access and rectify data, there is a new right available to individuals to port data from one organisation to another. This right is only available to individuals in strictly prescribed circumstances – where data in electronic form which was either provided by the individual or which the individual agreed you could collect where the processing is based upon the individual’s consent or contractual necessity. However, within these circumstances, upon request, you will be required to post all the relevant data to another organisation in an electronic and structured format within one month.

A new right to data erasure

An individual’s right to have their personal data erased by an organisation is more commonly referred to as the “right to be forgotten.” This will be available in various circumstances such as when personal data is no longer necessary for the purpose for which it was obtained, consent has been withdrawn or there is no legal basis for processing. The consequences of a request for erasure are complex. Not only must you erase the data from your own systems but you will need to communicate this to any organisation with whom the data has been shared and if the data has been made public, take reasonable steps to inform relevant organisations.

New notification obligations in the event of a data protection breach

Data protection breaches are unfortunately almost inevitable and therefore, it is critical to be prepared to deal with them quickly and effectively. In the event of any breach of the principles of the GDPR, where the rights of individuals have been affected, an organisation must notify the ICO within 72 hours. It must also notify any individual affected without undue delay, depending on the necessity of mitigating immediate risk to the security of the data concerned. A breach is broadly defined. It not only includes situations where data is stolen or lost but also where it is destroyed or altered. Whether an action was accidental or intentional is immaterial. Your organisation must be able to identify a breach, implement security measures in response, mitigate the loss or risk to individuals affected, notify all relevant regulators and to deal with the impact upon your organisation.

And returning to the importance of the principle of accountability, if the ICO enquires into the breach, you must be in a position to demonstrate that the breach occurred despite the systems and procedures in place, not because of them.

Under the GDPR, responsible data handling will be central to your organisation's governance. Should you need assistance in getting ready for GDPR compliance in May 2018, you are welcome to contact our data protection team. In the meantime, if you want to be kept up to date with practical guidance and legal developments over the coming months, please sign up to events@kingsleynapley.co.uk.

Our data protection team

For advice on data protection issues for employers, please contact one of our lawyers listed below, who will be able to draw on the expertise of relevant contacts in our cross practice data protection team as required.

Richard Fox
Partner, Head of Employment
T +44 (0)20 7814 1285
E rfox@kingsleynapley.co.uk

Adam Lambert
Partner, Employment
T +44 (0)20 7566 5272
E alambert@kingsleynapley.co.uk

Kirsty Churm
Senior Associate, Employment
T +44 (0)20 7814 1223
E kchurm@kingsleynapley.co.uk

Adam Chapman
Partner, Head of Public Law
T +44 (0)20 7566 5271
E achapman@kingsleynapley.co.uk

Emily Carter
Partner, Public Law
T +44 (0)20 7814 1255
E ecarter@kingsleynapley.co.uk

Andrew Solomon
Senior Associate, Corporate & Commercial
T +44 (0)20 7369 3794
E asolomon@kingsleynapley.co.uk