Legal Update

How to protect data in times of change? A review of the EU Commission's and ICO's response to updating the law on data protection

Kate Shires

is a trainee solicitor in the Bristows Commercial IP & IT team. She has particular experience in the area of data protection.

ABSTRACT Data protection law faces a challenging and difficult road ahead, and while the current law still has valid core principles, there is a need for it to evolve and adapt to global changes, in particular those driven by the Internet. The fast pace of technological innovation has triggered a review of data protection law both at an EU and UK level. This article explores these broad changes, as well as considering the implications any review may have on individuals with regard to their personal data. The article also considers the new enforcement powers of the Information Commissioner and the growing role of the ICO in administering data protection law in the United Kingdom.

Journal of Database Marketing & Customer Strategy Management (2011) 18, 65–68. doi:10.1057/dbm.2011.1

Keywords: data protection; commission communication; ICO consultation; ICO fines

Data protection is constantly evolving. The EU Commission during a recent review of the EC Directive on data protection (95/46/EC) has confirmed that while the Directive does still contain valid core principles, rapid technological developments and globalisation have brought new challenges to protecting personal data.

The fast pace of technological innovation coupled with the changes in EU law has also triggered a shift for UK data protection. A recent consultation on the existing framework of the UK law has requested a drive to a more sophisticated application of

data protection, backed up by a stronger regulatory attitude.

This article will consider the broad changes developing at both a European and UK level, as well as considering the wider implications these changes may bring for individuals with regard to their personal data, and the new enforcement powers of the Information Commissioner in the United Kingdom.

THE EUROPEAN APPROACH TO PERSONAL DATA

The EU Commission's review considers the application of data protection law 15 years

Correspondence:

Kate Shires
Bristows, 100 Victoria
Embankment, London,
EC4Y 0DH, UK
E-mail: Kate.Shires@Bristows
.com

since the inception of the EU's original Directive on data protection. The review considers how best to continue protecting the fundamental right to data protection within an increasingly interconnected world, yet also how to allow the free flow of information as required within the EU internal market. The Commission review is arranged around a series of principles, the most important of which are transparency, control, free flow of data and enforcement.

Transparency of data processing is fundamental for individuals; the use of the internet has led to increasingly elaborate and less easily detectable ways of collecting personal data. This can lead to the erosion of data protection rights where individuals can lose control and become unaware of how their data is being used. To rectify this, the Commission has suggested that there will be specific obligations for data controllers on both the type of information to be provided by individuals in the first place and the modalities for providing it, with a particular focus on the protection of children. The suggestions by the Commission could also lead to the compulsory use of standard EU privacy notices, ensuring a harmonised approach to data protection.

It is thought that individuals also ought to have greater control over their own data, particularly with respect to social media. The Commission promotes everybody's 'right to be forgotten' by stopping data processing and allowing data to be deleted if it is no longer needed for a legitimate purpose. This idea is complemented by the right to 'data portability', which gives individuals an explicit right to withdraw their own data if they feel a specific need to.

These rights are balanced against the need for data to flow freely within the internal market. The Commission supports further harmonisation of data protection law at an EU level, potentially simplifying the notification system and creating a uniform EU-wide registration form, which would

allow the standardisation of personal data collection and also a standardised approach as to how it can be shared and utilised across the EU and other adequately regulated countries. In tandem with this, there is an aim to clarify the applicable law for multinationals operating across several member states. The Commission wants to ensure that data protection obligations are followed regardless of where the data are processed. This means internal mechanisms for data protection need to be strengthened through, for instance, effective policies, the appointment of independent Data Protection Officers, obligations to carry out data protection impact assessments, the use of privacy-enhancing technologies and 'privacy by design' principles requiring companies to roll out products and services with privacy functions already embedded within them.

These increased obligations on the part of data controllers are to be combined with stronger law enforcement. The Commission hopes to promote the role of Data Protection Authorities at a national level to ensure coordinated protection for all free-flowing data across the whole of the EU.

HOW WILL THE UNITED KINGDOM RESPOND TO THESE CHANGES?

In response to the Commission's communication, the Ministry of Justice (MoJ) launched its own consultation in October 2010 on the UK's existing data protection law. The ICO provided an open response to the MoJ's consultation, giving a useful insight into the regulator's views on UK data protection law.

Like the Commission's opinion, the ICO considers that the core principles of UK data protection law should be maintained; any major revision would cause confusion and undermine its effectiveness. While the ICO believes that the current regime is broadly fine, there are areas where the ICO would like to see change.

In line with the Commission, the ICO believes in a more flexible approach to international data transfers with an emphasis placed on the mutual recognition for decisions across EU data protection authorities. The ICO also requests a shift to authorise 'methods of transfer' of data, that is, a broader approach to the actual mechanism safeguarding the transfer of data, over and above the current, more cumbersome authorisation of each individual data transfer.

The ICO also requests a move away from an 'all or nothing' approach to the application of the data protection principles; for example, it suggests that while IP address logs may be personal in some circumstances and ought to be kept secure, it may be impossible for organisations to provide individuals with full access to their IP address information or indeed to obtain their consent for its processing. The new framework then, according to the ICO, should be realistic about advances in technology and the rights and choices that individuals can actually have or want.

The ICO seeks for a drive towards a more sophisticated application of data protection law; for instance, there are calls to replace the 'outdated' concepts of data controller and data processor with a new 'accountability' principle under which all organisations are responsible for their own aspects of processing. This goes hand in hand with express 'privacy by design' obligations mentioned in the Commission communication to encourage privacy compliance to be built into new online systems ensuring greater protection and awareness from the beginning of a data collecting process.

There is also an aim to remove the category of 'sensitive data' from the existing legislation as it is seen as somewhat arbitrary classification; instead, the ICO are hoping to replace the category with a new risk-based regime applicable to all personal data, based on both its nature and use. For example, financial or geo-locational data might

require greater protection in some contexts, whereas health data, which is currently always considered 'sensitive', may not in others.

The ICO also believes that there ought to be an obligation on the data controllers to alert the subjects themselves to any breach involving personal data, and particularly in relation to 'serious breaches' where there is a potential for financial loss or danger. The ICO hopes to gain greater powers for enforcement against serious breaches; for instance, custodial sentences against breaches by individuals who disclose personal data without the consent of the data controller.

The ability to reinvent current data protection law as considered by both the Commission communication and the MoJ consultation provides a good opportunity to improve the application of the existing data protection regime. Clearly, the flipside to any flexibility that the ICO and Commission have called for is the potential for increased uncertainty and a greater need to self-regulate. It seems then, with this in mind, that both National and European level guidance, as well as enforcement, will be key.

THE BEGINNINGS OF A STRONGER UK ENFORCEMENT MODEL?

It is hoped that this improved approach to data protection will be backed by stronger enforcement powers for the ICO, ensuring that data protection is taken seriously. For a long time, the United Kingdom has stood out among European jurisdictions as having a low-key approach to the enforcement of data protection law; the Spanish Data Protection Authority for example, issued a total of €16.4 million of fines during 2009. Up until recently, this lack of financial enforcement has made it harder to argue the business case for improvements to data protection compliance, unless of course the organisation falls under the powers of the Financial Services Authority who can issue significant fines for data losses.

In April this year, however, the Information Commissioner acquired a new power to issue fines for serious breaches of the Data Protection Act, with a maximum fine of £500 000. The ICO may fine any data controller where there has been a serious breach of data protection principles, which are likely to cause substantial damage or distress and which are either deliberate or reckless and where no reasonable steps were taken to prevent the breaches.

These new powers were left unused by the ICO for the first 6 months following their enactment much to the growing disquiet of privacy activists. Finally, however, on 24 November 2010, the ICO announced that it had served two organisations with the first monetary penalties for serious breaches of the Data Protection Act.

The first penalty of £100 000 was issued to Hertfordshire County Council for two serious incidents in which council employees faxed highly sensitive personal information to the wrong recipients. The first incident involved a court case for child sexual abuse. Within two weeks, the council had sent another misdirected fax, this time details of care proceedings of three children and information relating to previous convictions, domestic violence records and care professionals' opinions, to the wrong recipient.

The Information Commissioner commented that the Council's procedures failed twice in situations where access to the data could have caused substantial damage and distress, saying 'it is difficult to imagine information more sensitive than that relating to a child sex abuse case'. It was also significant that the Council did not take sufficient steps after the first breach to reduce the chances of another.

The second organisation, A4E, an employment services company, also received a monetary penalty of £60 000 on 24 November 2010. This fine was for the loss of an unencrypted laptop that contained personal information relating to 24 000

people who had used community legal advice centres in Hull and Leicester. A4E issued an unencrypted laptop to an employee for the purposes of working at home. The laptop was then stolen from the employee's house with the full names, dates of birth, postcodes, employment status, income level, information about alleged criminal activity and whether an individual had been a victim of violence.

In short, the laptop contained significant volumes of data and the sort of information that could assist identity theft. This information was actually never seen by the thief because of an unsuccessful attempt to access the data shortly after the laptop was stolen. However, the Commissioner commented on the fact that thousands of people's privacy could have been compromised, and that A4E had not taken the reasonable steps to avoid the loss of data through encryption or other methods, despite knowing the amount and type of data on the laptop.

Currently, the ICO will serve penalty notices of differing sizes dependent on a series of criterion; for instance, the circumstances of the breach, the type of data lost, the duration of breach and the number of people affected. Actions to remedy or prevent the loss in the first instance are also viewed favourably.

If the Commission's communication and the ICO response to the MoJ consultation are taken into consideration, it seems likely that data controllers' obligations to protect data from the outset will become far more important. It also seems that there will be evolution of data protection law towards a more flexible and therefore far-reaching solution to the fast pace of technological and communications development. The responses, at both the UK and EU level, give a hopeful note that data protection law will endeavour to become more applicable to the increasingly globalised world of data; surely this can only aid the difficult task ahead.