OnPoint Dechert LLP

October 2012 / Newsflash
A Legal Update from Dechert LLP

UK Information Commissioner issues guidance on deleting personal data and the use of cloud computing

The UK Data Protection Act 1998 ("DPA") imposes various restrictions on "data controllers", such as employers, when "processing" personal data relating to individuals. In particular, employers must comply with eight data protection principles when processing personal data about their employees. The Information Commissioner's Office ("ICO") has recently published guidance papers on two particular areas on which these principles impact: deletion of electronically stored data (including whether employers must disclose deleted or archived data in response to a Data Subject Access Request), and the use of cloud computing. This Dechert OnPoint summarises the advice provided by these guidance notes.

Deleting personal data

The DPA's fifth data protection principle requires data controllers not to keep data for longer than is necessary for the purposes for which it is processed. Complying with this principle is not always a simple task, particularly where personal data is stored electronically. Accordingly, the ICO has published guidance on "*Deleting personal data*" intended to:

- address the problem of organisations informing people that their personal data has been deleted when it has merely been archived and could be re-instated; and
- encourage organisations to put safeguards in place for information that has been deleted but is still in fact in an organisation's possession.

Keeping employees informed

The guidance acknowledges the advice contained in the ICO's "*Personal information online code of practice*", published in July 2010, that it is good practice to make it clear to people what will happen to their information when, for example, they close an account with an organisation, namely whether their data will be irretrievably deleted or simply deactivated or archived.

The guidance reaffirms this principle, stating that organisations should be "absolutely clear" with individuals who are the subject of personal data (so-called "data subjects") about what they mean when they say their data has been deleted and what actually happens to it once they have deleted it.

Information which has not been irretrievably deleted

In the guidance the ICO recognises that there is a significant difference between deleting information irretrievably, archiving it in a structured, retrievable manner and retaining it as random data "*in an un-emptied electronic wastebasket*". The ICO explains that it will adopt a "realistic" approach in recognising that deleting information is not always a straightforward matter and that it is possible for data protection compliance issues to be suspended if certain safeguards are in place.

Putting information "beyond use"

The guidance states that the ICO will not take action over compliance with the fifth data protection principle, nor will it require data controllers to grant individuals subject access to personal data, where the data concerned has been "put beyond use". The ICO will consider data to have been put beyond use where the employer holding it:

- is not able, or will not attempt, to use the personal data to inform any decision in respect of any individual or in a manner that affects the individual in any way;
- does not give any other organisation access to the personal data;
- surrounds the personal data with appropriate technical and organisational security; and
- commits to permanent deletion of the information if, or when, this becomes possible.

The guidance does note, however, that even where data has been put beyond use, as described above, employers may be obliged to provide it in response to a court order.

Guidance on cloud computing

Organisations are increasingly using cloud computing as an innovative, cheap and potentially more secure way to store and transfer electronic data. By its nature, cloud computing creates a variety of risks from a data protection perspective. Accordingly, the ICO has published its "*Guidance on the use of cloud computing*" to assist organisations in complying with the DPA when processing personal data "in the cloud".

What is cloud computing?

The guidance adopts a wide definition of cloud computing, describing it as "*access to computing resources, on demand, via a network.*" Services could be of an "infrastructure as a service (IaaS)" nature (such as additional "virtual" servers or additional remote data storage facilities) or could be "software as a service (SaaS)" (that is remote access to software; a common example being the well-known customer relationship management service provided by salesforce.com).

The guidance also defines three main parties involved in the use and delivery of cloud services, namely:

- Cloud providers – these are organisations that own and operate a cloud service.
- Cloud customers – there are organisations that commission a cloud service for a particular purpose.
- Cloud users – these are the end users of a cloud service such as, for example, members of the public or employees of the customer.

As always, it is the "data controller" who will have ultimate responsibility for compliance with the DPA. A data controller is the person who determines the purposes for which and the manner in which any personal data are to be processed. In a cloud computing scenario, the cloud customer will determine the purposes for which and the manner in which any personal data are being processed. Therefore, the cloud customer will be the data controller and thus the party with overall responsibility for DPA compliance.

Having said this, the guidance notes that the precise role of the cloud provider will have to be reviewed in each case in order to assess whether or not it is processing personal data and, if so, whether it is merely acting as a "data processor" on behalf of the controller, or whether it is a data controller in its own right. This can sometimes be a difficult assessment and although the guidance somewhat fudges a discussion of this topic (no doubt because of the difficulty), UK based cloud providers will no doubt take comfort from the assessment of the ICO as to what would normally be the case.

Whatever the position on cloud providers however, cloud customers will have to address their compliance obligations.

Considerations for data controllers

The guidance highlights various compliance requirements associated with the use of cloud computing. Although some will be familiar to cloud customers that have outsourced any type of data handling, others are unique to cloud and may not have been encountered previously. These include:

- Selecting which data to move to the cloud – Cloud customers may not need to move all of their data into the cloud and should consider which data they may not want to put in the cloud given that the processing of certain data will have a greater impact on individuals' privacy than the processing of

others.

- Obtaining a written contract with a cloud provider – The DPA requires data controllers to have written contracts with data processors. The existence of a written contract between a cloud provider and a cloud customer should mean the provider will not be able to change the terms of the data processing operations without the cloud customer's agreement. In particular, the guidance notes that cloud customers should take care if a cloud provider offers a "take it or leave it" set of terms and conditions without the need or opportunity for negotiation. Cloud customers should be aware of such arrangements as they may not – in the ICO's view - retain sufficient control over the data to comply with the DPA. However, most cloud services are precisely of a "take it or leave it" nature: the model is predicated on a consistency of service provision for multiple customers on the same or similar terms. The cost/pricing structures depend on this and only the largest of customers (with the largest of acquisitions) have the negotiating power to alter this.

Selecting a cloud provider

The guidance sets out a number of key issues which cloud customers should consider when selecting a cloud provider. Again, these will be familiar to any entity which has undertaken an outsourcing involving personal data. These include:

- Rights of data subjects – the guidance clearly states that cloud customers must ensure that a move to a cloud service still allows data subjects to exercise their rights. This will include, for example, ensuring that data subjects can still submit data subject access requests to obtain details of their personal data and the right to object to their personal data being processed for certain purposes.

  Cloud customers will, therefore, have to carefully consider whether their proposed arrangements with a cloud provider will allow them to comply with these obligations.
- Assessing the security of a cloud provider – The DPA requires data controllers to take appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data. The data controller must, therefore, choose a processor providing sufficient guarantees about the technical and organisational security measures governing the data processing to be carried out and must take reasonable steps to ensure compliance with those measures.

  The guidance helpfully dispels a myth that has plagued a faster general take-up of cloud. It is not the case – confirms the guidance – that a physical inspection of the cloud provider is necessary as part of the security assessment. Instead, the guidance suggests that the most effective way for cloud providers to have their security assessed may be for an independent third party to conduct a detailed security audit, the results of which can be provided to multiple prospective cloud customers. Many cloud providers do in fact assert compliance with (or accreditation to) ISO 27000 series of standard. The guidance goes forward and expressly supports the introduction of an industry recognised standard or kitemark (designed for the cloud) which would allow cloud customers to compare services offered by cloud providers and be confident the assessment was sufficiently thorough.
- Encryption – Data which is "in transit" between endpoints should be secure and protected from interception through encryption. Furthermore, cloud customers should consider whether, given the nature of the personal data to be processed, data which is "at rest", i.e. when it is stored within the cloud service, will also need to be encrypted. This will be a particularly important consideration where sensitive personal data is being processed.

  For example, a cloud customer which is considering using a cloud computing system to back up its data should encrypt files before they are transmitted over a secure connection to the cloud provider. The cloud customer should keep the "key", which allows the data to be accessed, in its own possession preventing the cloud provider from viewing or processing the data other than to maintain it.
- Data retention and deletion – Cloud customers must ensure that cloud providers, who may have multiple copies of data stored in multiple locations, can delete all copies of personal data within a timescale that is in line with their own deletion schedule. Cloud customers should also ascertain what will happen to personal data if they decide to withdraw from the cloud service in the future and in this

respect would do well to bear in mind the guidance on "*Deleting Personal Data*" before entering into cloud computing arrangements with cloud providers.

- Further processing by the cloud provider – The cloud customer should ensure, through contractual arrangements, that the cloud provider can only process personal data for the lawful, specified purposes envisaged by the cloud provider. If the cloud provider is to process data for its own purposes such as, for example, its own advertising purposes, it must have the cloud customer's permission to do so and the cloud customer must have explained this further processing to (any) relevant cloud users.
- Using cloud services from outside the UK – The DPA requires that personal data is not transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for personal data belonging to data subjects. This raises difficult issues in the cloud computing context as cloud providers may well have a number of data centres located in various countries, some of which may be outside the EEA. Cloud customers will, therefore, need to ascertain from the cloud provider details of where the data is to be processed and what safeguards are in place in each different location. Furthermore, the cloud provider should be able to explain when data will be transferred to those locations. Many (if not all) of the major cloud providers are increasingly giving assurances in relation to the geographical locations of data (in particular, that the data will stay in particular regions (such as Europe). It is always an important conversation to be had.

  The ICO helpfully dispels another common concern of potential UK customers: access to data by foreign law enforcement agencies (the US "PATRIOT" Act is often mentioned in this context). The possibility of this happening is no reason – confirms the guidance – not to use a cloud service. Regulatory action would not be taken, for example, against the cloud customer if its US-provider disclosed data when legally compelled to do so by US authorities.
- Staff training – Cloud customers must introduce appropriate training and procedures to ensure that, when organisations switch to cloud computing, security is maintained.

  The guidance gives the example of a training organisation which has traditionally emailed course materials to students and student contact details (which contain personal data) to the course tutor. If the organisation were to switch to cloud-based file sharing, in order to avoid placing a heavy load on the email server, it might decide to upload course materials to the cloud but to continue emailing the student contact details to the tutor, given that they contain personal data. A new member of staff who was unfamiliar with the file sharing service might not be aware that the organisation had decided to continue to email the delegate list to the course tutor, and upload this information to the cloud, thereby making it publicly available.

Status of the guidance

Both sets of guidance provide helpful insights into these two tricky areas of data protection compliance. However, employers should note that, although the guidance notes are stated to be a guide to the ICO's general recommended approach, they come with the familiar proviso that individual cases will always be decided on the basis of their particular circumstances.

Copies of the guidance notes can be downloaded by clicking on the following links:

Deleting personal data

Guidance on the use of cloud computing

If you have questions or for more information, please contact:

Charles Wynn-Evans
London

Ed Holmes
London
Send an email

Renzo Marchini
London
Send an email


Send an email
T: +44 20 7184 7545


T: + 44 20 7184 7495


T: +44 20 7184 7563

For more information on Dechert's Data Privacy Group, please click here.

For more information on Dechert's Labor and Employment Group, please click here.