MACFARLANES

DATA PRIVACY: SUBJECT ACCESS - THE INFORMATION COMMISSIONER'S DRAFT CODE OF PRACTICE

DATA PROTECTION

THE POWER OF KNOWLEDGE

Knowledge is power: whilst attributed to Sir Francis Bacon in 1597, the same is true when it comes to workplace disputes in the 21st Century. If you want to know if your pay is unequal, if you have been unfairly dismissed or retaliated against, the evidence is likely to be stored on information systems controlled by the employer.

Employees have a number of ways of obtaining this information from their employer. If they present a claim, the Employment Tribunal will in due course order disclosure as part of its standard case management directions. If an employee feels that they might have been discriminated against, they can obtain information as part of the questionnaire procedure under the Equality Act 2010 although this is in the process of being repealed and does not necessarily require disclosure of documents and nor does it apply to disputes where there is no suspected discrimination.

A common tactic on the part of aggrieved employees is to submit a subject access request at an early stage in a workplace dispute: perhaps upon being selected for redundancy, as part of a grievance or when receiving a negative appraisal. The advantage of making a subject access request for the employee is that information can be obtained at an early stage before a formal claim is issued, and this allows the employee to formulate his or her complaint.

BIG EMPLOYMENT DATA

In the age of "big data", where it is less expensive to retain data than to selectively destroy it, responding to a subject access request in a fully legally compliant manner can be a surprisingly expensive and time-consuming business.

What personal data might an employer hold on its employees? Most obviously personal data is likely to be contained in an individual's personnel file, performance appraisals and HR database. In these cases, it is usually relatively easy to provide extracts. However, personal data is also likely to be held in emails and documents in the hands of co-workers and managers; this is likely to be intermingled with all kinds of other information that the employer may or may not wish to provide to the employee.

WHY ARE SUBJECT ACCESS REQUESTS SO EXPENSIVE TO DEAL WITH?

Once an employer is satisfied that it has received a valid subject access request, it must identify where personal data is likely to be located - which devices, systems or custodians - search those systems using key word searches, such as for the employee's name, and then review the results before providing copies to the data subject.

The purpose of the review is partly to consider if an exception applies, but more importantly to check that none of the documents also contain information which is commercially sensitive. It is also important to check that none of the materials are legally privileged or contain personal data relating to other data subjects. Unfortunately this part of the review cannot be automated and can be particularly laborious.

IS THE CODE HELPFUL?

It is important to emphasise at the outset that the Code will not have the force of law. That said, employers who comply with the Code are unlikely to be in breach of the DPA. The Code is likely to drive good practice.

The Code (like the DPA itself) is focused on large consumer and/or governmental organisations which process large volumes of data in a standardised format and so is less relevant to data controllers who merely process data as employers. Nonetheless, the Code does provide some practical guidance:

- The Code provides a number of best practice recommendations such as providing staff training, adopting a subject access request policy, responding to subject access requests on a centralised basis and appointing data protection "champions".
- The Code does not require data controllers to suspend their routine document destruction policies and suggests that no enforcement action would be taken if data were deleted after the request was received by the data controller (unless data was deleted or amended deliberately).
- The Code acknowledges that staff may be permitted to process personal data at home on personal devices. It reminds data controllers that they should have a policy to appropriately restrict the circumstances in which employees may hold data on personal devices or email accounts. The Code confirms that it does not require data controllers to instruct staff to search their private emails or personal devices unless there is a good reason to believe that they are holding relevant personal data.

- The Code states that if there is evidence that archived systems differ from live systems then data controllers should search archived resources. However if there is no evidence that the archived systems contain different information then the Code expressly states that the ICO will not take enforcement action.
- Data controllers do not need to seek to recreate deleted data using sophisticated techniques where data is deleted in line with normal data retention policies.

HELP FROM AN UNLIKELY SOURCE

Whereas the ICO's guidance has tended to take a more expansive interpretation of the DPA the courts have tended to interpret it in a more limited way. When reading the draft Code it should be borne in mind that:

- the Courts have held that information must have biographical significance for the data subject for it to be "personal data" (*Durant v Financial Services Authority* [2003]) and so all information returned from a search against an individual's name will not automatically be their "personal data" (*Ezsias v Welsh Ministers* [2007]);
- the Courts are unlikely to exercise their powers to order disclosure or award compensation where the data controller has conducted a reasonable and proportionate search (*Ezsias and Elliott v Lloyds TSB* [2012]); and
- the Courts are unlikely to exercise their powers to enforce the DPA where the sole purpose of the subject access request is to further litigation.

WHAT SHOULD YOU DO NOW?

The Code includes a number of best practice recommendations set out above. You may wish to consider if these are helpful or appropriate in view of the size of your business, the types of personal data processed and your attitude to risk.

However there is one particular recommendation that we are commending to our clients. That is the suggestion that data controllers maintain "information asset registers" or, in other words, a list of systems, devices and locations where personal data controlled by the organisation may reside. This is sometimes also referred to as a "data map" and is an important first step in any data privacy compliance programme. Having this to hand will not only make the process of responding to subject access requests more efficient but also assist with other data privacy issues – such as responding to data security breaches, renewing ICO notifications, compliance audits and responding to new legislation.

Macfarlanes' lawyers frequently advise clients on their obligations in relation to compliance with subject access requests both in a contentious and non-contentious context. We can also co-ordinate the review process including a review for legal privilege.

CONTACT DETAILS

If you would like further information or specific advice please contact:

RUPERT CASEY
DD: +44 (0)20 7849 2256
rupert.casey@macfarlanes.com

DANIEL POLLARD
DD: +44 (0)20 7849 2200
daniel.pollard@macfarlanes.com

MARCH 2013

MACFARLANES LLP
20 CURSITOR STREET LONDON EC4A 1LT
T: +44 (0)20 7831 9222 F: +44 (0)20 7831 9607 DX 138 Chancery Lane www.macfarlanes.com