Client Alert | Data, Privacy & Cyber Security / Employment, Compensation & Benefits

How employers can stop departing employees taking client lists with them

June 2016

Authors: Stephen Ravenscroft, Tim Hickman

When an employee departs for a role with a competitor, there is often a risk that the employee might take confidential client details with them, with potentially damaging consequences for the employer. However, a recent court decision has confirmed that data protection law may provide employers with strong protection against this risk.

The UK Information Commissioner's Office (the "**ICO**") recently announced that it has brought an enforcement action against an individual named Mark Lloyd. Mr Lloyd departed from a role with his former employer, a waste management company, and joined a competing company. He took with him a list of 957 clients. The list included a significant amount of information about those clients, including their purchase histories and other commercial data.

In the past, employers have used a number of methods to safeguard against departing employees from taking customer lists and other confidential information with them. These measures include practical steps (such as locking down databases of customer details and preventing large-scale exports of the data) and legal measures (such as claims brought against former employees for breach of confidentiality obligations[1] or infringement of database rights[2]). However, data protection law may offer an equally strong deterrent.

In Mr Lloyd's case, his former employer alleged that Mr Lloyd had infringed Section 55 of the Data Protection Act 1998. Under section 55, it is a criminal offence for any person to knowingly or recklessly obtain or disclose personal data without the permission of the data controller. It was clear that the client list taken by Mr Lloyd contained a significant amount of personal data, and that Mr Lloyd had taken the list (and the personal data it contained) without the permission of the data controller (his former employer).

Mr Lloyd pleaded guilty to an offence under Section 55 of the Data Protection Act. He was fined £300, and ordered to pay £405.98 costs and a £30 victim surcharge. The amount of the fine is not particularly high, but the fact that Mr Lloyd was found guilty of a criminal offence is enough to make many departing employees think twice before taking customer lists (or other personal data) with them when they leave.

1 See, for example, *Eurocell PLC v Crohill* [2016] EWHC 959 (QB)

2 See, for example, *Intercity Telecom Ltd v Solanki* [2015] EWHC B3

How should employers protect themselves?

While Section 55 of the Data Protection Act may provide employers with a strong mechanism to discourage departing employees from taking client lists with them, that mechanism does not enforce itself. It is essential for employers to be vigilant, and to consider taking the following steps:

- **Appropriate IT security measures** – One of the best ways to ensure that employees cannot take information that does not belong to them is to ensure that such information is appropriately protected, and cannot be accessed or copied without proper authorisation. Typically, employers achieve this aim by implementing appropriate IT security measures, to protect their information assets. This would include removing or restricting a departing employee's access to the employer's IT systems once notice of termination has been given by either party.

- **Employee training** – A significant factor in ensuring that employees understand their responsibilities is the provision of appropriate training with respect to their, and their employer's, data protection compliance obligations. In particular, this training should highlight the fact that if employees obtain or disclose client lists (or other personal data) without the employer's permission, they may face criminal prosecution.

- **Enforcement** – It is vital to ensure that employees understand that these risks are not purely hypothetical, and that the employer will take action to protect its information assets. The appropriate enforcement action may depend on the circumstances, but if personal data are taken by an employee without permission, the employer should at least carry out an investigation. If the investigation reveals that the employee has committed an offence under Section 55 of the Data Protection Act, then the employer should consider whether further action is appropriate.

  In most cases, it will not be possible for an employer to bring a private prosecution against a former employee in relation to a breach of Section 55.[3] However, if an employer believes that such a breach has occurred, the employer can report the breach to the ICO, which has the power to investigate and prosecute the relevant former employee, as it did in the case of Mr Lloyd.

In addition to the steps set out above, it is important for employers to stay up-to-date with legal developments in this area, and ensure that they understand their rights and responsibilities. Data protection law in the EU will undergo radical changes over the next two years, and the impact of these changes on Section 55, and other employment-related issues, remains to be seen.

White & Case LLP
5 Old Broad Street
London EC2N 1DW
United Kingdom

T +44 20 7532 1000

[3] Under section 60(1)(a) of the Data Protection Act 1998, proceedings in respect of offences (such as an offence under section 55) can only be brought by the ICO or by, or with the consent of, the Director of Public Prosecutions.