



Preventing data security breaches

November 2009

It was recently reported that employees of T-Mobile have been selling details of customers' contracts to competitors. The details included telephone numbers and contract expiry dates.

Customer lists are always a valuable asset for a business and in this case T-Mobile's competitors were allegedly willing to pay large sums of money for them.

In related news, a study by security supplier Cyber-Ark in London and New York has shown that 41% of finance sector workers have taken sensitive data to new jobs. The study of 600 workers in Canary Wharf and Wall Street also revealed that a total of 85% of people admitted they know it is illegal to download corporate information from their employer, but this wouldn't stop them from taking it, and 57% of respondents said it has become a lot easier to take sensitive information from work.

So how can businesses take steps to prevent similar things happening to them?

- 80% of data security incidents involve staff so vetting staff when they are employed and regular training on data protection is vital. A clear and consistent procedure to adhere to when vetting staff will go some way to minimising the risk and will also provide evidence that you are taking a proactive approach should the ICO need to assess your internal processes.
- Basic security measures should be taken: passwords should be secure and changed regularly; confidential waste should be shredded; information held on portable devices should be encrypted; documents containing personal data should have restricted viewing, editing and printing rights; and USB and other memory ports on computers should be disabled.
- Sensitive personal data relating to race, religion or political beliefs should only be collected if necessary and should only be accessible by vetted and trained personnel. Regular training should be provided for all employees and more specialised training may be required for individuals who have particular data security roles.

- Organisations should have a policy of running regular data inventories to understand how data is collected, stored, used, maintained and disposed of.
- Data access and monitoring technologies should be implemented to monitor the movement of personal data throughout the organisation.
- Organisations should undertake regular auditing of their data protection training, security and management policies.

With the ICO set to gain new powers to fine organisations from next April, ensuring that personal data is kept secure has never been more important. As well as the negative publicity and fines that may follow, theft and loss of customer data has a significant impact on consumer confidence.

If you would like any further advice on the matters raised above, or any other data protection concerns, please do not hesitate to contact us.

Technology, Media and Telecommunications contacts:



Andrew Dunlop
Partner
 +44 (0) 117 902 2786
 andrew.dunlop@burgessalmon.com



Martin Cuell
Senior Associate
 +44 (0) 117 902 6673
 martin.cuell@burgessalmon.com

Disclaimer: This information sheet gives general information only and is not intended to be an exhaustive statement of the law. Although we have taken care over the information, you should not rely on it as legal advice. We do not accept any liability to anyone who does rely on its content.

© Burgess Salmon LLP 2009. All rights reserved. Extracts may be reproduced with our prior consent, provided that the source is acknowledged.

Data Protection: Your details are processed and kept securely in accordance with the Data Protection Act 1998. We may use your personal information to send information to you about our products and services, newsletters and legal updates; to invite you to our training seminars and other events; and for analysis including generation of marketing reports. To help us keep our database up to date, please let us know if your contact details change or if you do not want to receive any further marketing material by contacting marketing@burgessalmon.com.

Burgess Salmon LLP, Narrow Quay House, Narrow Quay, Bristol BS1 4AH
 Tel: +44 (0) 117 939 2000 Fax: +44 (0) 117 902 4400
 Chancery Exchange, 10 Furnival Street, London EC4A 1AB
 Tel: +44 (0) 20 7685 1200 Fax: +44 (0) 20 7685 1266
 www.burgess-salmon.com



Burgess Salmon LLP is a Limited Liability Partnership registered in England and Wales (LLP number OC307212) and is regulated by the Solicitors Regulation Authority. A list of members, all of whom are solicitors, may be inspected at our registered office: Narrow Quay House, Narrow Quay, Bristol BS1 4AH.