

UK Update

ICO publishes guidance on “BYOD”

The ICO has published [guidance](#) which highlights the dangers of allowing your employees to use their own devices (known as “bring your own device” or “BYOD”) for work emails and other work related uses.

According to a recent [survey](#), commissioned by the ICO and carried out by YouGov, 47% of UK adults now use their personal smartphone, laptop or tablet computer for work purposes, but less than 30% of these users are provided with guidance on how their personal devices should be used in this capacity (and in particular how to look after the personal data accessed and stored on their personal devices).

As highlighted by the ICO guidance, an employer has significantly less control over BYODs than it would have over a traditional corporately owned and provided device, leading to risks over the security of the data stored and otherwise processed by BYODs. The Data Protection Act 1998 requires that the data controller must take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data, and against its accidental loss or destruction or damage. Employers allowing BYODs will be exposed to investigations and ultimately enforcement action and fines from the ICO if nothing is done to protect personal data and comply with their obligations under the Act.

Although there are certainly benefits in allowing employees the flexibility of BYODs, employers need to take action to avoid these risks. In particular, the guidance shows that employers need to give serious thought to whether their current data protection or e-communications policies provide sufficient protection.

Key recommendations

- Being clear on the types of personal data that can be processed on personal devices
- Registering personal devices with remote locate and wipe facilities so the confidentiality of personal data can be maintained in the event of loss or theft
- Being clear with staff about which types of personal data may be processed on personal devices
- Using strong passwords to secure personal devices and ensuring that access to a personal device is locked or personal data automatically deleted if an incorrect password is input too many times
- Enabling encryption to store data on personal devices securely
- Being extremely wary about using public cloud-based sharing and public backup services, which the employer has not fully assessed.

The ICO admits that the cost of introducing the suggested controls may be “quite significant” and might be greater than the initial savings expected through having a BYOD policy, but suggests that the sum will be insignificant if you consider the reputational damage caused by a data breach.

As regards updating your data protection policies to take account of any BYOD practice, the ICO recommends following guidance in the ICO Employment Practices Code. The guidance explains that employees have a legitimate expectation that they can keep personal lives private and that an employer who wishes to monitor an employee's data use should be clear in the policy about the purpose for doing so and the benefits such monitoring is likely to bring, and should make sure that employees understand this.

If this article raises any questions in relation to the current policies that you have in place in relation to BYOD, please refer these to **Heidi Watson** who would be happy to provide you with further guidance.

Further information

If you would like further information on any issue raised in this update please contact:

Heidi Watson

E: heidi.watson@clydeco.com

Ruth Bonino

E: ruth.bonino@clydeco.com

Clyde & Co LLP
The St Botolph Building
138 Houndsditch
London EC3A 7AR

T: +44 (0)20 7876 5000

F: +44 (0)20 7876 5111

Further advice should be taken before relying on the contents of this summary.

Clyde & Co LLP accepts no responsibility for loss occasioned to any person acting or refraining from acting as a result of material contained in this summary.

No part of this summary may be used, reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, reading or otherwise without the prior permission of Clyde & Co LLP.

Clyde & Co LLP is a limited liability partnership registered in England and Wales. Authorised and regulated by the Solicitors Regulation Authority.

© Clyde & Co LLP 2013