Briefing

October 2017

SHEPHERD+ WEDDERBURN

Who owns employees' emails?

Lessons to be learned from a failed interim injunction application



Neil Maclean
neil.maclean@shepwedd.com
Katie Russell
katie.russell@shepwedd.com
Elouisa Crichton
elouisa.crichton@shepwedd.com

A recent decision of the High Court, taken together with a ruling of the Grand Chamber of the European Court of Human Rights provides useful guidance for employers about the ownership of personal emails sent and received from company accounts, and the extent to which employers can access these emails.

In *Capita plc v Darch*, Capita raised High Court proceedings against ten former employees who had gone on to found a competitor firm. Capita sought a variety of interim injunctions to restrain the defendants on the basis that they (i) were threatening and intending to act in breach of their restrictive covenants; (ii) were misusing confidential information of Capita; and (iii) had secured an unfair advantage on behalf of a competitor. The judge refused to grant any of these orders.

The case provides useful guidance for employers about the ownership of personal emails sent and received from company accounts.

Do emails belong to employers?

Capita wanted the ex-employees to disclose all emails that had been sent from Capita accounts (whether by the ex-employees or other employees) to the defendants' personal accounts. The High Court did not accept that such emails or their contents were the property of Capita, as some or many of these would be related to employees' private affairs.

One of the defendants argued that if the order were to be granted he would have to disclose personal emails, for example photos of his holiday, which he had sent to colleagues from his Hotmail account and to which they had replied to from a Capita account. The court agreed with the defendant that such personal emails were not relevant and said that, in the circumstances, to grant the order would infringe the defendant's right to respect for private and family life that is guaranteed by article 8 of the European Convention of Human Rights.

The defendants also referred to the employee handbook's 'acceptable personal use' policy which states that "Capita believes that using the communication tools provided in the business for personal use is entirely acceptable, as long as that use is reasonable". Capita were not able to lead any evidence from their contractual documentation which said that they had the right to access all of the emails sent by Capita email accounts. The court stated that it is only to be expected that the employees would therefore use the Capita email accounts for personal use.

What is the effect of this decision?

This decision is in line with previous cases which have found that employees can use their work email accounts for (reasonable) personal use, particularly where this is set out in an employer's email communications policy. An

employer therefore does not have an automatic right to the contents of every email that an employee sends or receives. If employers are seeking to access employees' emails by way of court order, such an order should exclude emails of a personal or private nature.

Effect of *Barbalescu v Romania* – Employee Monitoring

The decision in Capita should be read together with a recent ruling of the highest court of appeal in Europe regarding the extent to which an employer can monitor employee communications. The Grand Chamber of the European Court of Human Rights ruled in a landmark decision that an employer that had read private messages sent from an employee's Yahoo Messenger account had breached Article 8 of the European Convention on Human Rights. You can read our previous briefing on the European Court of Human Rights decision here.

This case was raised in Romania in 2007 and the employer had imposed a blanket ban on personal email use at work so it is important to bear in mind that the facts of the case are very different to the reality of most workplaces in the UK today where, generally, employees are permitted to use their work computer, email and telephone etc. for reasonable personal use. However, Employers who wish to monitor the communications of employees should ensure that the right balance is struck between legitimately protecting business interests and workers privacy. The Grand Chamber set out the factors to be considered when assessing the monitoring of workplace communications. Employers should consider:

- Notifying employees about monitoring of communications - is this adequately covered in the acceptable use internet policy?
- The extent of monitoring - will communications be reviewed by managers to ensure compliance?
- The degree of intrusion into employee's privacy;
- Whether there are legitimate reasons to justify monitoring the communications and their content;
- Whether a less intrusive monitoring system is feasible;
- The consequences of monitoring for the employee, what will the employer use the results of the monitoring for;
- Whether the employee has been provided with adequate safeguards.

The Grand Chamber's decision does not protect employee privacy in the workplace in all circumstances. However, it does give employees a reasonable expectation of privacy when accessing a personal email account at work, even if this is against the employer's policy.

Impact of the General Data Protection Regulation

The General Data Protection Regulation (GDPR) will come into effect in the UK in May 2018 and will cause fundamental changes to the way that employers monitor employees and use personal data.

Employers will need to justify the processing of employees personal data by demonstrating that they have a legal basis for doing so. It is no longer likely to be possible to rely on employee consent to processing. Processing of any employee data, including the monitoring of emails, must be proportionate, transparent, and carried out in the least intrusive manner.

Measures should be put in place to protect the balance between the employers legal basis and the employees right to privacy. This could include avoiding monitoring employee's personal communications. The Article 29 Working Party (an advisory body with a representative from the data protection authority of each EU Member State) suggested in June 2017 that as a matter of good practice employers could offer employees access to alternative unmonitored communication systems (for example free WiFi or access to tablets in the canteen) to allow employees to exercise their legitimate right to use work facilities for reasonable private use.

Employers should also look to review their email retention and deletion policies to ensure that they are compliant with the GDPR principles of data minimisation and storage limitation. The penalties for a breach of GDPR are significant and could result in a fine of up to €20 million or 4% of gross annual turnover, whichever is higher. Employees will also have the right to claim compensation any damage they suffer as a result of a breach of GDPR.

If you are interested in learning more about what employers need to do to prepare for and comply with the GDPR then please read our guide.

SHEPHERD+WEDDERBURN

Key contacts

Neil Maclean
Partner
T +44 (0)131 473 5181
M +44 (0)782 541 3316
E neil.maclean@shepwedd.com

Katie Russell
Partner
T +44 (0)131 473 5266
M +44 (0)787 269 9897
E katie.russell@shepwedd.com

Elouisa Crichton
Associate
T +44 (0)141 566 7249
M +44 (0)770 214 1289
E elouisa.crichton@shepwedd.com