Employment Law Briefing

Volume 10 | Autumn 2015

Whistleblowing Hotlines: Top 10 Data Protection Issues

By Sarah Thompson

Whistleblowing can be a valuable tool for businesses, providing an early warning system against corporate malpractice and demonstrating a compliance culture. Hotlines are now established as an important tool in the whistleblowing process. Hotlines typically involve the personal data of both the reporter (e.g. name, location and the fact that he/she made the report) and the "wrongdoer" (e.g. name and allegation). Introducing hotlines therefore requires careful consideration as regulatory compliance steps must be taken prior to implementation to ensure adherence to data protection laws.

Whistleblowing hotlines are often rolled out on a global basis. Whilst EU data protection laws have been harmonised, to some extent, by the EU Data Protection Directive, Member States have interpreted the laws slightly differently and each country's data protection authority (DPA) takes a different approach to regulation and enforcement. It is therefore important for multinational corporations to understand that a "one size fits all" approach does not work when implementing whistleblowing hotlines in the EU, and they must instead navigate a patchwork of differing legal requirements.

Set out below are our top 10 issues that businesses should consider when implementing whistleblowing hotlines in the EU:

1. Notify the applicable DPA and, where necessary, obtain its prior authorisation.
2. Check whether Works Councils need to be informed and consulted prior to implementation.
3. Consider the type of concerns which may be reported via a hotline; more serious matters should be, while more trivial issues ought to be dealt with through normal reporting channels (e.g. line managers).
4. Think about anonymous reporting. Approaches to anonymous reporting differ from country to country; some prohibit it, while others require it to be available.
5. Implement data-processing contracts whenever any third-party service provider operates the hotline.
6. Put in place a mechanism for complying with EU data-transfer rules whenever personal data is transferred outside the European Economic Area, for instance, to an organisation's corporate headquarters.
7. Implement policies to provide employees with information about the hotline, how it should be used, handling complaints and any rights they may have in, and to, the data.
8. Train the employees responsible for processing hotline reports and consider entering into confidentiality agreements.
9. Adopt appropriate technical and organisational measures to keep secure any personal data that has been gathered through a hotline.
10. Place a time limit on the retention of data gathered through the hotline, which should be in line with regulatory recommendations and guidance papers.

McGuireWoods London LLP Employment Team Members:

Dan Peyton, Partner
+44 20 7632 1667
dpeyton@mcguirewoods.com

Sarah Thompson, Associate
+44 20 7632 1693
sthompson2@mcguirewoods.com

Andrea Ward, Senior Associate
+44 20 7632 1697
award@mcguirewoods.com

McGuireWoods London LLP
11 Pilgrim Street
London EC4V 6RN
United Kingdom
DX 249 London/Chancery Lane

SAVE THE DATE

European Data Protection and Security Conference

3 November 2015
London, United Kingdom

McGUIREWOODS

www.mcguirewoods.com

An Open Secret: Electronic Media and the Limits of Privacy

By Dan Peyton

Information technology and social media have transformed the workplace and the means by which people communicate with the rest of the world in a positive and exciting way. However, this immediate and accessible means of communication also brings with it significant risks, including in the employment context.

Employers are all too familiar with the risks arising from social media and email. These risks range from candidates sharing interview experiences on social media (whether that be sharing tests/exercises or criticisms of the process), to reports of management errors and even unlawful conduct within a business.

Most have now responded to the usual employment lawyers' mantra of "make sure you have a policy", including IT policies, disciplinary and compliance policies, and whistleblowing policies. Employees, on the other hand, often seem to consider IT policies as an inhibition on their personal freedoms, when in fact they are as exposed as their employers by the risks associated with an instantly accessible, global and basically unregulated form of communication.

Certainly, there are examples of cases where private and professional lives run perilously close to one another. In the case of *Game Retail v. Laws*, an employee opened a personal Twitter account in his own name. The account made no reference to his employer and the only connection with his employer was that a number of its employees were followers. He posted material on the account that was later described in Tribunal as being offensive to "dentists, caravan drivers, golfers, the Accident and Emergency Department, Newcastle supporters, the police and disabled people". His employment was terminated when his employer found out about the account. He brought a claim for unfair dismissal but was not successful.

In *Gosden v. Lifeline Project Ltd.*, an employee sent an email from his private email account to a colleague's private email account. After this email was forwarded and his employer discovered its offensive content, the employee was dismissed. He also lost his claim for unfair dismissal.

Employees need to understand, and employers have a role in helping them to understand, that there is no longer a clear and predictable division between private life and working life in this area. This is partly because it is now widely known, or should be, and should be foreseeable that ostensibly "private" communications will routinely become publicly accessible. Any employees who go online and post or email comments or views that are or could reasonably be taken as being offensive, risk draconian sanctions by their employers. Furthermore, these draconian sanctions are now more likely than ever to be upheld as fair by the Employment Tribunal.

In a different context we are accustomed to ostensibly private conduct being treated as work-related because of the impact of such conduct on the workplace. For example, in *Gimson v. Display by Design*, an employee was held to have been fairly dismissed for punching a colleague on their way home after a Christmas party. It was held that this was a fair dismissal because there was a sufficient connection to work and the event would have material impact on relations within the workplace.

If I make an inappropriate comment to a friend in the pub at the weekend, no one would suggest that I should lose my job. However, there is a qualitative difference between a comment to a friend in a pub and posting on Twitter or even sending an email. This is why employees can, even acting in their private capacity, through the use of such readily and widely accessible media, cause substantial reputational damage to a business by virtue of their actions. Furthermore, there should now be an expectation that any such comments or emails are likely to come into the public domain and that people who post material that is or may be offensive do so at their own risk. Not only that, but there should also be an expectation that evidence of such material will likely remain accessible and visible for a long time. When such stories attract press attention or go "viral", the general public may not know that Joe Bloggs is an employee of New Co, but its clients, suppliers and other employees do, and that may be enough to result in dismissal.

Of course, the case law does not go this far. But employees should be aware of the practical risks they take in sharing on social media, or by email, any conduct, comments or thoughts that may cause offence and damage not only to their own reputations, but also the reputations of those associated with them, including their employer.

Therefore, the message is that policies are necessary, but they are not sufficient. Employees need training. They need to be made aware of the risks to their own reputations and careers if they do not act in accordance with the policies that they may see currently as an interference with their privacy.

Transferring Data Outside Europe – A Quick Guide

By Sarah Thompson

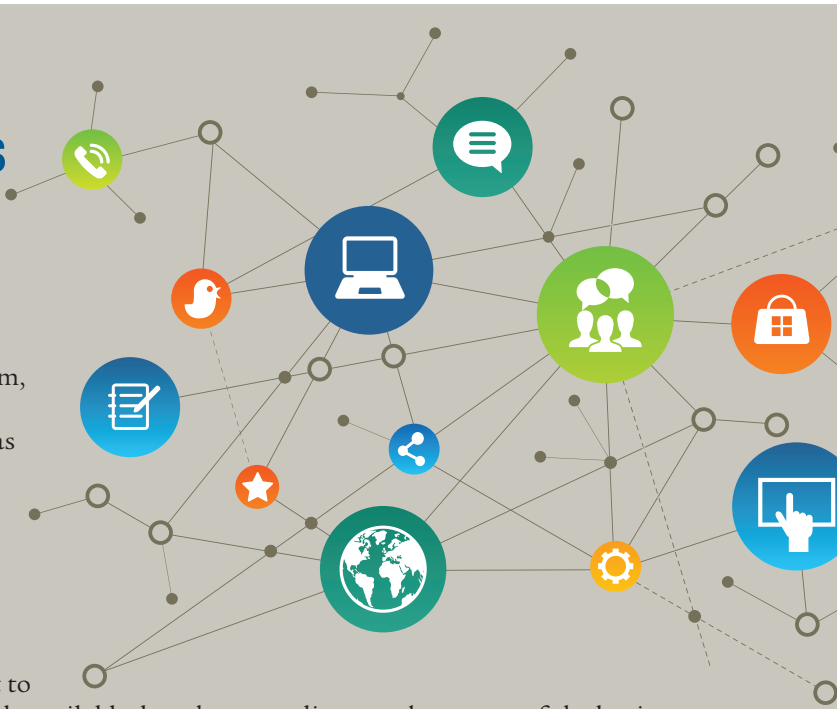
The ongoing globalisation of business, and ever more accessible technology, allows personal data to be transferred anywhere in the world. Data protection laws allow such transfers to be made within the European Economic Area (EEA). However, transfers to countries outside the EEA are prohibited unless sufficient safeguards are put in place to protect the rights of the individuals to whom the data relates (data subjects).

The following highlights the ways in which personal data can be transferred outside the EEA:

1. It is transferred to a country approved by the European Commission as having an "adequate level of protection" (e.g., Australia and Canada).
2. It is transferred to a U.S. company registered under the U.S. "safe harbor" programme. The safe harbor scheme is currently under negotiation at the EU level following the Snowden revelations about mass surveillance of EU citizens' personal data held by U.S. cloud computing providers. A decision of the European Court of Justice on the validity of the safe harbour framework is also expected soon.
3. It is transferred pursuant to "Model Clauses" that have been approved by the European Commission. There are different types of clauses depending on whether the transfer is to a data controller or a data processor.
4. It is transferred between group companies who have implemented "Binding Corporate Rules" that have been approved by the Information Commissioner's Office.
5. The data subject has provided valid (freely given and informed) consent to that transfer.
6. The transfer is necessary for the performance of a contract with the data subject, for public interest reasons or for legal proceedings.

Shutting the Stable Door – Protecting Business Assets in an Age of Social Media

By Dan Peyton



It used to be so simple. Business contacts and useful client information were kept on an employer's IT system, belonged to the employer, and could not be copied or taken away when the employee left. When information was taken, we would all trundle off to court to seek forthwith delivery up orders and springboard injunctions.

But what if contact information is not stored on the employer's IT systems? Many of us are now actively encouraged, even trained, to make and keep contacts on networks like LinkedIn and other social media using accounts personal to the user. It may seem less important to protect client or contact information that is readily publicly available, but these are clients and contacts of the business.

Of course, employers should have, and should seek to enforce, up-to-date social media policies which make it clear that any contacts added during the course of employment should be deleted on termination of employment and not reinstated for a period after employment has ended. However, it is not entirely clear whether such precautions will be enforceable post-termination. Nor does this deal with the practical issue that, even if an employee deletes his or her contacts, there is nothing to stop those contacts easily from reconnecting. This is the whole point of many social/business networks.

So employers may also have to rely more heavily on post-termination restrictive covenants, such as non-solicitation and non-dealing covenants, which may protect client connections even where information is publicly available (see for example, *East England Schools v. Palmer and Sugarman Group Limited* [2013] EWHC 4138 (QB)). Whilst it is true that general announcements regarding an employee's new position may not themselves amount to solicitation, departed employees will need to be careful that there is no solicitation once approached by former clients. An enforceable non-dealing provision will also be vital in limiting the damage, a restriction often omitted from contracts.

Data Protection for Employers – the Basics

By Sarah Thompson

Data Protection is primarily governed by the Data Protection Act 1998 (the Act). The Act is concerned with respecting the rights of individuals when their personal data is processed. Personal data means information about individuals who can be identified from that information – such as names, addresses and National Insurance numbers – and also includes the employer's opinions and intentions with respect to employees. Sensitive data is also covered and subject to more robust legal requirements. Sensitive data includes information about an individual's racial or ethnic origins, political opinions, religious or other beliefs, trade union membership, health and criminal proceedings or convictions. Generally speaking, personal data does not include day-to-day business correspondence to, from or copying the employee, where normal work activities are being carried out.

An employer will be processing (collecting, retaining, recording, deleting, etc.) personal data throughout an employment relationship for a number of reasons, including to recruit, to monitor performance, and for health and safety reasons. From time to time, as part of routine checks or a specific investigation, an employer may also monitor or check an employee's telephone, emails and Internet usage, which will inevitably result in accessing or using personal data. There are strict legal requirements regarding such monitoring.

The Act requires employers to comply with eight principles when processing personal data. These principles include the requirement that data must be collected and used fairly and lawfully, be accurate, be up to date, be kept for no longer than necessary, be protected by appropriate security measures, and not be transferred outside the European Economic Area, unless certain protective measures are first put in place.

Employees' Rights

Employees have the right to request a copy of the personal data their employer holds about them. This includes information about grievance and disciplinary issues, and information obtained through monitoring. Arrangements should be in place to deal with requests, as a 40-day time limit is required by the Act. There are some exemptions to providing such data, such as, when giving information would make it more difficult to detect a crime and where the information concerns a third party. For example, if an employee has been accused of harassment, the employer may need to protect the identity of the person making the accusation.

Employees can object to their employer holding or using personal data about them if it causes distress or harm, and in such instances, the employer should delete that information or stop using it in the way complained about, unless the employer has a compelling reason not to delete or stop using it. If an employee considers that there has been a breach of the Act in respect of personal data about that employee, the employee should first raise the matter internally with the person responsible for dealing with it. However, employees also have the right to apply to the Information Commissioner's Office (ICO), who will determine whether there has been a breach by the employer. The ICO can serve enforcement notices, requiring employers to comply with the data protection principles and information notices, requiring employers to provide certain information within a specified time. If the employer fails to comply with either of the notices, it will be guilty of a criminal offence with a maximum fine of £5,000. If employees suffer damage because their employer fails to comply with its data protection obligations, they can also issue court proceedings whereby unlimited damages could be awarded. Where data is inaccurate, the court also has powers to order its rectification, blocking, erasure or destruction.

Employers' Obligations

Set out below are some of the key requirements employers need to observe when processing employee data:

1. Employees must be notified of the employer's processing activities, typically through a privacy policy, covering the conditions under which personal data will be processed (for example, monitoring of email/Internet/telephone should be explicitly stated), ensuring that everyone is aware of their individual responsibilities and the employer's expectations regarding privacy.
2. Records should be kept secure, e.g. manual files kept in locked filing cabinets and computer records password protected.
3. Data should be accessed only by appropriate, authorised staff members who have been adequately trained.
4. Records should be kept up to date, with employees asked to check and update them periodically.
5. Data must not be irrelevant or excessive, and should be deleted once there is no longer a business or legal requirement to keep it.
6. Data needs to be discarded securely, e.g. by using confidential shredding.