Employee data surgery

Ann Bevitt and **Harriett Swan** answer questions that deserve attention in any organisation that processes employee data.

With the General Data Protection Regulation ("GDPR") poised to bring about the most significant changes to data protection law and practice in the EU since 1995 and the recent invalidation of the US-EU Safe Harbour scheme followed by the imminent introduction of the EU-US Privacy Shield, there is currently an enormous focus on data protection in the EU. Given the wide scope of data that they process and their often disparate processing practices, employers in particular should be proactively reviewing the procedures they currently have in place in order to ensure that they are dealing with employee data appropriately and are in the best position possible to take the necessary steps to comply with the more stringent requirements of the GDPR. The following Q&A addresses some common issues and concerns regarding the processing of employee data.

Consent

Is consent the best approach to processing employee data? Consent to process employees' personal data is often used as a default legal basis for processing. However, it is not always required and/or there may be other legal bases which may be more appropriate. For example, the processing may be required by the employment contract. This would apply to the processing of data for the purposes of providing employees with their contractual entitlements such as benefits and holiday. Alternatively, the employer may be under a legal duty to process the information, such as absence information processed for the purposes of paying Statutory Sick Pay. Finally, the processing may be necessary for the employer's legitimate interests and the benefits to be gained from processing justify the privacy intrusion. When considering whether this basis is available, the Information Commissioner's Office ("ICO") Employment Practices Code (the "Code") and Supplementary Guidance advises employers to carry out an impact assessment which involves:

1. identifying the purpose(s) for collecting the information and any likely adverse impact of doing so;
2. considering any possible alternatives;
3. taking any obligations that would arise from collecting and holding the information into account; and
4. finally, judging whether the employer's proposed actions are therefore justified.

Where employers process employees' sensitive personal data, they will also have to satisfy one of the conditions for processing such data set out in Schedule 3 of the Data Protection Act 1998 (the "DP Act"). In these circumstances, the options are more limited and in particular there is no legitimate interest condition for processing. Employers may be able to process employees' sensitive personal data without consent if the processing is necessary to comply with a legal obligation, such as health and safety legislation, checking employees' entitlement to work in the UK or considering reasonable adjustments to accommodate for employees with disabilities. However, consent may sometimes be the only option available to employers to legitimize the processing of sensitive personal data. To be valid under the DP Act, consent for the processing of sensitive personal data must be explicit.

> There are limitations as to how far consent can be relied upon for the processing of employees' personal data.

While the ability to obtain consent is useful, there are limitations as to how far consent can be relied upon for the processing of both employees' personal data and sensitive personal data. In particular, employees must be fully informed about the processing, must freely give their consent and can withdraw it at any time. Further, looking forward, under the GDPR it will be even harder for employers to rely on employees' consent.

Employee Records

An employee is of the view that their appraisal record is incorrect, but the manager in question rejects the request to correct the information. What is the correct way to handle this situation? The employer should refer to the company's appraisal and grievance procedures and policies. The Advisory, Conciliation and Arbitration Service ("ACAS") guidance on appraisals states that employers should set up a procedure for employees to:

1. in the first instance, be given the opportunity to sign the completed form and express their views on the appraisal they have received; and
2. if necessary, appeal against their assessment, in order to preserve the credibility of the appraisal scheme.

Appeals should be made to a more senior manager than the appraiser. If it is subsequently agreed that the appraisal record is inaccurate, this will need to be updated in order to comply with the DP Act. One of the data protection principles under the DP Act is that "personal data should be accurate and, where necessary, kept up to date". Employers should be aware that where a record is inaccurate, the employee has a right to apply to the court for an order to rectify, block, erase or destroy the inaccurate information.

Who should have access to employee appraisals? On the grounds that those who delegate work and monitor performance are best placed to appraise performance, in most organisations employees are appraised by their immediate managers. In some organisations, senior managers may have the

opportunity to check and comment on appraisal forms as part of the process. In addition, HR usually has overall control of the appraisal process. In any case, only employees with proper authorisations and the necessary training should have access to employee appraisals, and those who do have access should be made aware that data protection rules apply and personal information must be handled with appropriate care and respect. For example, it may be deemed inappropriate to share an employee appraisal with someone junior to the employee being appraised.

Monitoring Employees

Do companies need to inform the ICO if using employee monitoring technology? Employers need to register their processing with the ICO if they process data other than for the three basic purposes (staff administration; advertising, marketing or public relations; accounts or records). By using employee monitoring technology, such as CCTV, employers will be required to register as a data controller with the ICO and pay a fee of £35 annually: failure to do so is a criminal offence. There is no additional requirement to inform the ICO about new monitoring practices if an employer is already registered as a data controller with the ICO.

While it is easy to understand that employers may be concerned about how and when employees spend their time online or otherwise, they do not have free rein on employee surveillance. If employees are monitored by collecting or using information about them, the DP Act will apply. While there is no general prohibition on monitoring employees under the DP Act, the courts have been willing to find that Article 8 (right to privacy) of the European Convention of Human Rights may be breached when telephone calls, emails and internet use are monitored. Employers should ensure clear rules and policies are in place so that employees are aware when they may be monitored. Doing this can, in certain circumstances, displace the expectation of privacy.

Company management suspect theft but cannot be sure whether the culprit is someone from inside the company. The company wants to investigate covertly by hiring a private investigator. Does the company have to inform employees? As mentioned above, while there is no general prohibition on monitoring employees under the DP Act, employees should be made aware of monitoring practices unless more covert action is justified. Before seeking to monitor employees, employers should carefully consider why the monitoring is needed. Employers should question whether the monitoring is justified by the benefit of solving the problem, and in doing so, alternative approaches should also be considered.

All employees being monitored should be made aware of the practices and the reasons for implementing them, and clear signage should be used where monitoring is taking place. Covert monitoring can very rarely be justified, and to do so, an employer must have grounds for believing that informing employees about any required monitoring would make it difficult to prevent or detect the wrongdoing. When covert monitoring is used, it should only be in relation to a specific investigation, and should be stopped as soon as that investigation comes to an end.

Can employers carry out drug testing in the workplace, and if so, how should they ensure their employees' privacy is respected? Before carrying out drug testing in the workplace, employers need to be sure that the intrusion involved is justified by the purpose they are trying to achieve. For example, random testing of blood-alcohol levels of train drivers may be justifiable on safety grounds, however testing office workers in the same way is unlikely to be. The Code advises employers to conduct an impact assessment when determining whether the collection of information through testing is justified and also provides helpful guidelines in relation to carrying out testing which will assist employers to respect individuals' right to privacy. The underlying message is that drug or alcohol testing is usually justifiable for health and safety reasons only. These guidelines include using the least intrusive forms of testing that will bring the intended benefits to the business, ensuring random testing is genuinely random, and telling employees what drugs they are being tested for.

As well as following these guidelines, employers should ensure data stored about employees' health are kept particularly secure. This could be achieved by introducing password protections on any soft copy files, and/or keeping hard copies in a sealed envelope in a locked environment. It would also be appropriate to limit access to only one or two employees for whom it is necessary to provide it.

Data Transfers

Following the recent invalidating of the US-EU Safe Harbour scheme in 2015, what is the best option for legitimising transfers of employee data to the US? Companies must ensure that they compensate for the lack of data protection in a country outside the EU by using appropriate safeguards. Following the recent decision by the European Court of Justice declaring the Safe Harbor framework invalid, and until the EU-US Privacy Shield is formally adopted, companies should make sure that standard contractual clauses or alternatives are in place to legitimise transfers of personal data to the United States, where necessary. Alternatively, companies can rely on employees' consent, but should note the limitations on consent referred to above.

Looking forward, under the GDPR standard contractual clauses, contractual clauses authorised by a supervisory authority and Binding Corporate Rules are all still considered to be adequate safeguards. In some situations, the GDPR also provides that companies may be able to rely on a 'legitimate interest' justification when transferring data outside the EU.

Employer Rights

Can an employer demand to see prescribed medication details? Employers should be very clear about why such data are being collected and comfortable that any requirement to provide such details is justified by the benefits that will result. A key consideration here is being transparent with employees and making proportionate requests for information.

As a general rule, employers should seek to limit the amount of medical information they collect on their employees as much as possible. For

example, they should consider using a health questionnaire as opposed to conducting medical testing. They should also only collect health information from those employees from whom it is really required and should ensure that health information is kept particularly secure and separate, as outlined above.

If an employee is off work due to illness, does an employer have the right to demand access to passwords to the employee's computer? Although employers don't have a free rein on monitoring employees, and employees are not considered to leave their right to privacy at the office door, it may be reasonable for an employer to request passwords from an absent employee in order to meet business needs while they are away. Ultimately, the computer and the information on it are company property. As above, in relation to requesting medical information or carrying out drug testing, a key consideration is proportionality. Employers should consider:

1. who is the most appropriate employee to access the absentee's computer;
2. limiting who is given access;
3. the purpose for access and whether any alternative approaches are available to the employer; and
4. only accessing the computer for as long as is necessary to achieve the purpose.

Employee Rights

Do employees have a right of access to personal information stored by an employer? The DP Act covers computer records and some manual records kept in structured form. Employees (prospective, past and current) may request from an employer what information is kept about him/her, and the employer may make a charge of up to £10 for responding to each request. Employers are entitled to protect third parties, and to withhold information that might prejudice their business, but the general principles of the DP Act are that employees should have access to personal information held by the employer.

It is useful to note that while there is no general exemption from an employee's right of access to information about him/her simply because the information is confidential, there is a special exemption from the right of access to a confidential reference when in the hands of the organisation that gave it. This exemption does not apply once the reference is in the hands of the person or organisation to whom it has been given. As above, the recipient may still be entitled to take steps to withhold information that reveals the identity of any other individuals named within the reference, for example, the author.

AUTHORS

Ann Bevitt, Partner,Cooley (UK) LLP, and Harriett Swan, trainee, Cooley (UK) LLP. Emails: abevitt@cooley.com and hswan@cooley.com

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data Protection Act 1998, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

PL&B's United Kingdom Report will help you to:

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access
You will be sent the PDF version of the new issue on the day of publication. You will also be able to access the issue via the website. You may choose to receive one printed copy of each Report.

3. E-Mail Updates
E-mail updates keep you regularly informed of the latest developments in Data Protection, Freedom of Information and related laws.

4. Back Issues
Access all the *PL&B UK Report* back issues since the year 2000.

5. Events Documentation
Access UK events documentation such as Roundtables with the UK Information Commissioner and *PL&B Annual International Conferences*, in July, Cambridge.

6. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

"I particularly like the short and concise nature of the *Privacy Laws & Business Reports*. I never leave home without a copy, and value the printed copies, as I like to read them whilst on my daily train journey into work. **Steve Wright, Chief Privacy Officer, Unilever**"

Subscription Fees

Single User Access
UK Edition **£400 + VAT***
International Edition **£500 + VAT***
UK & International Combined Edition **£800 + VAT***
* VAT only applies to UK based subscribers

Multi User Access
Discounts for 2-4 or 5-25 users – see website for details.

Subscription Discounts
Special charity and academic rate:
50% discount on all prices. Use HPSUB when subscribing.
Number of years:
2 (10% discount) or 3 (15% discount) year subscriptions.

International Postage (outside UK):
Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30
Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the International Report.
www.privacylaws.com/int