# Making it personnel — unlawful practices by HR departments

***Referenced in terms of UK data protection law, Stephanie Pritchett, Principal at Pritchetts, examines the common data protection compliance traps that human resources departments fall into, and how to navigate around them***

HR (or human resources) departments will use personal data about employees regularly throughout each working day and, of course, should always ensure that they comply with the Data Protection Act 1998 ('DPA') when doing so. They will no doubt have been told repeatedly about the potential for fines from the UK Information Commissioner's Office ('ICO') of up to £500,000, and may even be aware that these are set to increase to up to 2% of an organisation's worldwide turnover under the proposed new European Regulation.

But such warnings are not always enough to prompt individuals to take action towards compliance. Despite doomsday forecasts of colossal financial penalties, disastrous PR and other sanctions commonly imposed for non-compliance, mistakes (some of which are well-intentioned) and misunderstandings in relation to data protection practices in the HR environment are still commonplace.

Some of the most common errors, along with some practical ideas to avoid them, are included below. These can also serve as a useful compliance checklist for those dealing with often complex organisational HR issues.

## A fine (blue) line: Acceding to police requests for staff data, without making the appropriate checks

There is a common misunderstanding that section 29 of the DPA allows (or even requires) any information that has been requested by the police about employees or others to be immediately handed over by the organisation for the purposes of the prevention or detection of crime.

In reality, section 29(3) works only as an exemption under the DPA which allows an organisation to consider whether it may, in the particular circumstances of the request, be able to claim an exemption from one or more of the 'non-disclosure provisions'.

The 'non-disclosure provisions' under the DPA are:

- the First Data Protection Principle (requiring fair and lawful processing) except that compliance with the fair processing conditions (under Schedules 2 & 3 of the DPA) must still be achieved;
- the Second, Third, Fourth and Fifth Data Protection Principles;
- section 10 — the right to prevent processing likely to cause damage or distress; and
- sections 14(1) to (3) — the right to rectification, blocking, erasure and destruction.

Section 29(3) is relevant where organisations are asked for information for any of the following 'crime and taxation purposes':

- the prevention or detection of crime;
- the apprehension or prosecution of offenders; and
- the assessment or collection of any tax or duty or of any imposition of a similar nature, and where the application of the non-disclosure provisions in relation to the particular disclosure would be 'likely to prejudice' any of the crime and taxation purposes.

Even if the information has been requested for one of the 'crime and taxation purposes' and application of the 'non-disclosure provisions' would prejudice those reasons, then the exemption will only apply to the extent to which compliance with one or more of those parts of the DPA would be inconsistent with the particular disclosure in question. The exemption is not a 'blanket' exemption from all of the non-disclosure obligations.

The 'non-disclosure provisions' operate to enable personal data to be disclosed under the DPA in circumstances in which it is in the public interest. However, the organisation will need to make a careful assessment to consider whether this is actually the case when dealing with the request at hand. When carrying out any such assessment, the individual dealing with the police

(Continued on page 4)

(Continued from page 3)

request for information must consider, for each of the non-disclosure provisions set out above, which (if any) would be inconsistent with the disclosure request in question and the extent of the inconsistency. Only those provisions can then be disregarded if they would be 'likely to prejudice' one or more of the crime and taxation purposes and even then, only to the extent to which prejudice would be likely to result.

Unfortunately no clarification is provided in the DPA as to what is meant by 'likely to prejudice'. However, ICO guidance states that:

- for the exemptions to apply, there would have to be a substantial chance (rather than a mere risk) that complying with the provision would noticeably damage one or more of the crime and taxation purposes;
- the exemption should not operate in a 'blanket' way to justify denying subject access rights to whole categories of data where in fact those purposes would not be likely to be prejudiced in the case of all data subjects;
- the data controller is responsible for making a judgment about whether or not prejudice is likely in relation to each individual case;
- decisions should be made at a senior level within the organisation and should be documented in case of future challenge.

Making such an assessment is not always an easy task, with the result that some organisations choose not to disclose information on receipt of a request from the police, and instead await a court order requiring disclosure.

There are no easy and straightforward answers to whether a request should be complied with or not, without considering the particular facts relating to each police request. What is abundantly clear though is that employee information should not be readily handed over without a careful assessment and, ideally, a written record of this assessment. Organisations should carry out careful staff training, particularly to those tasked with handling any such police requests. Having a clear policy in place to ensure all staff are aware of how to handle them is also essential. It is also usual to ask the police to confirm any request on an Association of Chief Police Officers S29(3) form. Finally, organisations may also wish to provide template forms to record its assessment process.

> ***"Organisations should carry out careful staff training, particularly to those tasked with handling any such police requests and having a clear policy in place to ensure all staff are aware of how to handle them."***

Requests for information received by employers from other third party organisations (such as HMRC, public sector organisations) or individuals (such as private investigators or others) are not considered in any depth in this article. Needless to say, in all such situations, employers should comply with the DPA, and also the relevant ICO guidance. Such guidance includes the ICO's Employment Practices Code and Supplementary Guidance ('EP Code'), the Data Sharing Code of Practice, the Good Practice Note: 'When can I disclose information to a private investigator?', and the technical guidance notes on 'Dealing with subject access requests involving other people's information' and 'Freedom of information: Access to information about public authorities' employees'.

(Copies of each of these documents are available to subscribers by sending an email to docs@pdpjournals.com)

## One flu over the cuckoo's nest: making staff details (including details of sickness and reasons for absence from work) available to too many people within the organisation

Personal data on staff members should only be disclosed to others within the organisation in compliance with the DPA. Going back to basics, it is always a good idea to consider the Eight Principles before making any disclosure of staff data internally.

Under the First Principle, organisations must provide relevant staff members whose data are being disclosed with fair processing information, advising them with whom their data may be shared internally and the purposes for this. Before making the disclosure, organisations must additionally consider whether they can show that the disclosure is necessary for one or more of the reasons set out under the fair processing conditions in Schedule 2 of the DPA. Given that sickness information often contains physical or mental health data — i.e. 'sensitive personal data' — about the individual, organisations should consider whether a fair processing condition under Schedule 3 of the DPA can be claimed in respect of such data. Even where staff are told that a disclosure is planned and compliance with the Schedule 2 & 3 conditions can be demonstrated, organisations should ask whether they believe the disclosure is generally fair. If not, alarm bells should be ringing and a more careful impact assessment undertaken.

Under the Second Principle, organisations should consider for what reasons the information were initially collected from members of staff and ensure that subsequent processing is compatible with these reasons. If the planned disclosure to other members of staff is not consistent with those reasons, there may be a breach of the Second Principle.

Under the Third Principle, organisations must consider whether the collection of information from staff members is adequate, relevant and not excessive to the initial reasons for collection. Would the onward disclo-

sure to the intended recipients be adequate, relevant and not excessive? Unless this can be clearly established, the disclosure cannot be made without risk of breaching the Third Principle.

The EP Code recommends that sickness and injury records which contain specific information about an employee's illness or injury should be kept separately from absence records, which merely record that an employee was not present at work referring generically to 'illness' or 'injury. This helps to ensure that only those that have a legitimate need to know the actual details of the sickness are informed.

Under the Fourth Principle, organisations must ensure that the information that has been collected about the staff member is accurate. If this is in question, further checks should be made and, where necessary, evidence collected, before onward disclosures are made.

Under the Fifth Principle, organisations must consider how long the information in question has been held for. Is it appropriate that the organisation still has sickness records and is now planning to use and disclose them?

Under the Sixth Principle, are individual staff members' rights under the DPA being complied with when making the disclosure. For example, if the staff member makes a subject access request, are we happy to divulge all the disclosures of his/her data that we have made internally? Or, if the individual has, for example, asked us not to disclose their sickness data to particular people on the basis that it will cause them damage or distress, can we respect that request, or have we made a careful assessment as to why we need to disclose it regardless?

Under the Seventh Principle, when disclosing data to others, have we done so in a secure way to prevent unauthorised or unlawful processing? Have we done so in line with our staff security policies? Have we ensured that only those with a need and right to know the information are given it and that it will not be further disclosed without careful compliance checks (for example, limited access rights)?

Any intended disclosure of the data to anyone outside of the European Economic Area (even another part of the organisational group) will need to be carefully assessed to ensure compliance with the Eighth Principle.

More generally, organisations need to consider whether the internal disclosure has been made in line with recommendations made in the EP Code. Consider the situation in which an organisation is also required to share sickness records externally. For example, HR departments often need to obtain advice from GPs or external Occupational Health Providers and consultants (who may or may not be treating the employee and be covered by the Access to Medical Reports Act), and which involves disclosing sensitive personal data to third parties. Any such sharing of information externally must also be made in compliance with the DPA. The EP Code states that employee health information should only be disclosed to third parties where there is a legal obligation to do so, where it is necessary in connection with legal proceedings or where the employee has given their specific consent.

## Bigging up brother: conducting overly-intrusive monitoring of staff

The key issue is this: if monitoring of staff is over-the-top to the point that it is illegal, then it may not be possible to lawfully use the evidence obtained during that monitoring for internal disciplinary and Employment Tribunal proceedings. Clearly, this may rather defeat the point.

Carrying out lawful monitoring of employees, particularly of email, internet and telephone use, is a legal minefield. Suffice to say that lawful monitoring requires compliance not only with the DPA and the ICO's guidance, but also the Human Rights Act 1998, Regulation of Investigatory Powers Act 2000 and Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699). (Discussion of these other regimes is beyond the scope of this article).

Considering compliance from the perspective of the DPA, all Eight Principles of the DPA are 'in play'. The key principles to consider are:

**First Principle:** Has detailed fair processing information been provided to employees about the employer's monitoring activities? Is that information in line with the ICO's recommendations in the EP Code? Note that the EP Code imposes a positive obligation on employers to be proactive in communicating information about the monitoring being carried out. So, for example, organisations cannot get away with simply posting the policy on the intranet and then hoping employees read it. Employers should instead ensure that: (1) training is provided on the monitoring from employees' induction stage onwards; and (2) using IT systems to set reminders before workers access the systems. Even where information has been provided, the employer will still need to show compliance with the processing conditions set out in Schedule 2 (and Schedule 3 where sensitive personal data are processed) before the monitoring is carried out.

**Second Principle:** To ensure that personal data are only obtained during monitoring for specified lawful purposes and not processed in a manner incompatible with those purposes, the employer would need to show that it has provided staff with detailed information about:

- the methods by which it monitors its employees;
- the information it collects; and
- how any information collected may be processed.

Employers should then only use the information collected through monitoring for the purposes for which the monitoring was undertaken, unless that information reveals an activity that no employer could reasonably be expected to ignore. The EP Code suggests that such activity would be criminal activity, gross misconduct or health and safety breaches that jeopardise others.

**Third Principle:** Is the monitoring carried out, and the personal data collected during the process, adequate, relevant and not excessive for

(Continued on page 6)

(Continued from page 5)

the purposes for which the processing is taking place? Where an organisation wishes to investigate potential misconduct by an employee, it is important that it does so in a way that is proportionate to the matter being investigated, in compliance with the DPA and Part 3 of the EP Code (monitoring at work). The EP Code states, for example, that accessing the personal and private emails of all members of a department in order to track down a culprit is unlikely to be justified, even if employees have been told that their personal emails might be accessed.

**Sixth Principle:** Is the monitoring of personal data being carried out in accordance with the rights of the data subjects under the DPA? For example, employees have the right to request access to the results and records of monitoring that has been carried out.

**Seventh Principle:** Is the monitoring being carried out subject to appropriate technical and organisational measures to protect against unauthorised or unlawful processing and accidental loss, destruction or damage? The EP Code states that staff with access to information obtained through monitoring should be limited, and should have received appropriate training, and that data obtained through monitoring should be secure.

**Eighth Principle:** This Principle may be relevant where an employer must share the results of monitoring with an overseas parent employer, or monitoring is actually conducted by an overseas parent.

Some other key points made by the EP Code in relation to lawful monitoring are:

- an impact assessment as set out in the EP Code should be carried out prior to any monitoring to help ensure the proportionality test has been met. Monitoring should also not be carried out just because a third party customer requires it — organisations should satisfy themselves that the monitoring is justified in all the circumstances; and
- if the results of monitoring might have an adverse impact on a worker (because, for example, it reveals evidence of a disciplinary offence), organisations should always ensure that the worker has an opportunity to make representations. This is because equipment or system malfunctions might sometimes produce misleading or inaccurate results, and information can be misinterpreted or even deliberately falsified. Allowing a worker to make representations is, of course, in line with good employment practice and in any event reflects an employer's obligations under unfair dismissal legislation.

## Clouding your judgment: outsourcing staff data functions without undertaking the relevant due diligence and putting compliance mechanisms in place

The basic position is that the DPA applies where a data controller has *control* of, rather than *possession* of, personal data. This means that data controllers remain responsible under the DPA for any processing carried out by their sub-contracted data processors. Data processors themselves have no obligations under the DPA unless they are also acting as a data controller.

Therefore, where an employer outsources staff data functions (for example, payroll, headhunting, or data back-up) to a third party that is to process personal data on behalf of that employer, the DPA requires the employer:

- to carry out due diligence checks to ensure that the third party data processor has adequate security measures in place (both in terms of physical security and technological security) to protect the data and take reasonable steps to ensure compliance with those measures (for example, ensuring that all relevant workers at the data processor are reliable and adequately trained in data security measures);
- to enter into a written contract with the third party which requires the data processor to act only on the instructions of the employer, and to comply with data security obligations equivalent to those specified in the Seventh Data Protection Principle. Ideally, in that contract the employer would also insist that it has audit rights to check that relevant security measures are being appropriately implemented, and that it retains the right to approve any onward subcontracting relationships (as the employer will be responsible for compliance with the DPA all the way down the contractual chain). The employer should also consider adding specific terms as appropriate in each particular outsourcing, in order to transfer as much responsibility as possible to the data processor. This will assist the data controller in complying with its obligations under the DPA; and
- to ensure that it complies with the Eighth Principle under the DPA where it outsources those functions internationally, either directly or as part of a contractual chain. An example of this might be where an organisation outsources payroll to a UK provider, who in turn subcontracts some of the data processing internationally, say to a data back-up provider based in the USA.

In the workplace environment, it is important to remember that the rules apply to data processors which belong to the same corporate group as the employer data controller in the same way that they do to unconnected third party data processors. The data are still moving out of the company, and this movement must be properly regulated.

## Spinning a record: inappropriate handling of SARs

Employees have a right under the DPA to make a subject access request ('SAR') to gain access to data held about them by their employer, provided that they make the request in writing and pay a fee of up to £10. Employers should be aware that em-

ployees often exercise this right as a tactic to determine if the employer has complied with the DPA when processing their personal data, or to gain access to information that they may not know about — often in the middle of a grievance or disciplinary procedure.

Therefore, appropriate handling of SARS — both how to deal with them and what should be provided when handling particular requests — is an issue regularly faced by HR departments. One example is whether a HR manager can disclose witness statements identifying third parties without redaction or permission.

Appropriate handling of SARS is a subject that has been dealt with in numerous articles published in this journal and will not be repeated here, other than to say that the EP Code recommends putting a system in place so that SARs are always recognised, and handled by appropriately trained staff.

## Life's a breach: inappropriate handling of data protection or data security breach events and onward reporting

Gone are the days when we could bury our head in the sand when faced with a data protection breach or remain blissfully unaware that they were even taking place.

On investigation, the ICO will expect organisations to demonstrate awareness of the day-to-day breaches faced by the organisation, ideally evidenced by a centrally maintained internal data protection breach register. The idea behind this is that the breach register will help the organisation pinpoint areas where there may be compliance gaps, where a change in policy or training is required, or where a report needs to be made to the ICO.

Although there is currently no mandatory security breach notification in the UK, the ICO recommends that organisations consider voluntarily informing it of breach incidents, and states that any penalties to be applied may be lower where voluntary notification to the ICO has been made. Should an organisation decide to 'self-report', the ICO has made available an online form for organisations to use when reporting the data breach. Employers should ensure that staff are trained in breach handling and that a policy is made available setting out how the employer requires employees to handle a data protection or security breach incident internally. These should be drafted in line with the ICO's Data Security Breach Management Guidance (copy available at www.pdpjournals.com/docs/88086).

## How long has this been going on: inappropriate data retention

When an employer considers how long employee personal data should be retained for, it must consider compliance with the Fifth Data Protection Principle — that information is not held for longer than is necessary for its particular use.

Although the ICO's Employment Practices Code recognises that the retention period will be based on the business need of the employer, what is clear is that large amounts of employee data should not be kept simply because "it might come in handy one day", or on the off-chance that someone may bring a claim against the organisation.

As the DPA does not set out any specific data retention periods or guidance, employers need to create their own employee data retention policies after they have undertaken a risk analysis to determine what the appropriate legislative and regulatory requirements for retention are, as well as any appropriate statutory limitation periods (for example, three to six months for employment tribunal claims and six years for county court claims) and best practice requirements.

See pages 10—12, Volume 11, Issue 3, of *Privacy & Data Protection,* for a more detailed discussion of the requirements for retaining and destroying data.

## Final thoughts

HR teams have a great deal of responsibility vis-à-vis the information they hold about employees, and some would argue that they face a substantial challenge in carrying out their modern business functions in full compliance with the DPA.

While more 'form filling' is never welcomed in the HR environment, often the use of template forms can formalise many of the assessments staff have to make day to day. Having clear, comprehensible staff policies backed up by bespoke training on particular issues is always an essential foundation.

**Stephanie Pritchett**
Pritchetts
stephanie@pritchettslaw.com