Making it personnel: unlawful practices by HR departments

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 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 Acts 1988 and 2003 ('the Acts') when doing so. They will no doubt be aware that fines of up to 2% of a company's worldwide turnover are proposed for non-compliance with data protection laws under the proposed European Regulation.

But it's not always enough: despite these doomsday warnings of colossal financial penalties, disastrous PR and other sanctions commonly imposed for non-compliance, we still often come across common mistakes (some of which are well-intentioned) and misunderstandings in relation to data protection practices in the HR environment.

Some of the most common mistakes and misunderstandings are discussed below, along with some practical ideas as to help. Hopefully these will also serve as a useful compliance checklist for those dealing with complex organisational HR issues.

A fine (blue) line: acceding to requests from An Garda Síochána for staff data, without making the appropriate checks

There is a common misunderstanding that Section 8(b) of the Acts allows (or even requires) any information that has been requested by An Garda Síochána 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 8(b) works only as an exemption under the Acts which allows an organisation to consider whether it may, in the particular circumstances of the request, be able to claim an exemption from:

- any restrictions in the Acts (thought to mean the need to comply with the fair processing conditions under the Acts);
- the requirement to obtain and process the personal data fairly; and
- from the rights of subject access in relation to such data, referred to in this article as the 'Non-Disclosure Provisions'.

Section 8(b) enables an organisation to consider whether it could disclose information that has been requested for any of the following 'Crime and Taxation Purposes':

- the prevention, detection or investigation of offences;
- the apprehension or prosecution of offenders; or
- the assessment or collection of any tax, duty or other moneys owed or payable to the State, a local authority or a health board, and where the application of one or more of the non-disclosure provisions in relation to the particular disclosure would be likely to prejudice one or more of the crime and taxation purposes.

The crime and taxation exemption under Section 8(6) is not a 'blanket' exemption from all of the non-disclosure provisions. 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 Acts would be inconsistent with the particular disclosure in question.

Although these 'non-disclosure provisions' exist to enable personal data to be disclosed under the Acts in circumstances in which it is in the public interest, 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 request for information (from, for example, An Garda Síochána) 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.

There is, unfortunately, no clarification in the Acts as to what is meant by 'likely to prejudice'. The UK Data Protection Act is not clear on this point either, although it is interesting to note that the guidance of the UK regulator on this point states that: 'for these 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'.

What does seem clear is that Section 8 (b) of the Acts should not be seen as a blanket exemption 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.

This means that the appropriate data controller needs to make a judgment about whether or not prejudice is likely in relation to each individual case. 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 An Garda Síochána and, instead await a court order requiring disclosure. As it is not an easy task, decisions should be made at a senior level within organisations and should be documented in case of future challenge.

Whilst there are, unfortunately, no easy and straightforward answers to whether a request should be complied with or not, without considering the particular facts relating to each request for information made for crime and taxation purposes, what is abundantly clear is that employee information should not be readily handed over without a careful assessment and, ideally, a written record of this assessment. Organisations are advised to carry out careful staff training, particularly to those tasked with handling Garda requests for employee information, and have in place a clear policy to ensure all staff are aware of how to handle them. It is also usual to ask the requestor to confirm any request in writing, and data controllers may also wish to provide template forms to record the organisation's assessment process as to whether or not to disclose.

"Organisations are advised to carry out careful staff training, particularly to those tasked with handling Garda requests for employee information, and have in place a clear policy to ensure all staff are aware of how to handle them."

We have not considered any further in this article requests for information received by employers from other third party organisations (such as the Irish Revenue, public sector organisations) or individuals (such as private investigators or others). In all such situations, employers should of course comply with the Acts and the Data Protection Commissioner's guidance on data sharing. There is a multitude of helpful information out there, but in some cases, data controllers may of course wish to seek legal advice.

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

Data on staff members should only be disclosed to others within the organisation in compliance with the Acts. Going back to basics, it is always a good idea to consider the following sections of the Acts before making any disclosure of staff data internally:

Sections 2(1)(a), 2(A), 2(B) and 2(D) — Have you provided the relevant staff members with fair processing information advising them with whom their data may be shared internally and the purposes for this? Before making the disclosure, can you show that the disclosure is necessary for one or more of the reasons set out under the Fair Processing Conditions under Section 2(A) of the Acts? Given that sickness information often contains physical or mental health 'sensitive personal data' about the individual, can you also claim a fair processing condition under Section 2(B) of the Acts? Even where you have told the staff that you are planning to make the disclosure and can show compliance with the Sections 2(A) and 2(B) conditions, do you believe the disclosure is generally fair? If not, alarm bells should still be ringing and a more careful impact assessment undertaken.

Section 2(1)(c)(i) and (ii) — For what reasons did you initially collect the information from your member of staff? Is the disclosure that you are now planning to make to other members of staff consistent with those reasons? If not, there may be a breach of Section 2(1)(c)(i) and (ii).

Section 2(1)(c)(iii) — Was the collection of information from your staff member adequate, relevant and not excessive to the initial reasons for collection? Would the onward disclosure to the intended recipients be adequate, relevant and not excessive? Unless this can be clearly established, the disclosure should not be made without risk of breaching Section 2(1)(c)(iii). By way of example, 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 would help ensure that only those that have a legitimate need to know the actual details of the sickness have it disclosed to them.

Section 2(1)(b) — Is the information

(Continued on page 6)

(Continued from page 5)

that you have collected about the staff member accurate? If you are not sure, further checks should be made and evidence collected where necessary before onward disclosures are made to further compound the potential damaging effect on the individual of inaccurate information being disclosed. Furthermore, how long has this information been held for? Is it appropriate that the organisation still has these sickness records and is now planning to use and disclose them?

Sections 4 and 6 — Can we comply with the individual staff member's subject access rights under the Acts 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 as it will cause them damage or distress if we do so, can we respect that request or have we made a careful assessment as to why we need to disclose it regardless?

Sections 2.1(D) and 2(C) — When disclosing the 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 won't be further disclosed without careful compliance checks (i.e. limited access rights etc.)?

Section 11 — 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 Section 11 of the Acts.

We have not considered in this article a situation in which we are also required to share sickness records *externally*. For example, HR departments often need to obtain advice from doctors or external occupational health providers and consultants (who may or may not be treating the employee) and which involves disclosing sensitive personal data to third parties. Any such sharing of information externally must, of course, also be made in compliance with the Acts. It is good practice to only disclose employee health information 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 you may not be able to lawfully use the evidence obtained during that monitoring for internal disciplinary and external legal proceedings. Clearly, this rather defeats the point!

It is difficult to carry out lawful monitoring of employees, particularly of email, internet and telephone use. Suffice to say that lawful monitoring requires compliance not only with the Acts and the Data Protection Commissioner's guidance (such as 'Guidance Notes - Monitoring of Staff' and 'Data Protection and CCTV'), but also with laws which allow employees a right to privacy — such as the European Convention of Human Rights and the Irish Constitution. Discussion of these other regimes is beyond the scope of this article.

Considering compliance from the perspective of the Acts, various parts must be considered — primarily: Sections 2(1)(a), 2(A), 2(B) and 2(D) — has detailed Fair Processing Information been provided to employees about the employer's monitoring activities? It is good practice for employers to be pro-active in communicating information about the monitoring being carried out — i.e. not just posting the policy on the intranet and then hoping employees read it. Employers should instead ensure that training is provided on the monitoring from employees' induction stage onwards; and 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 Sections 2(A) and 2(B) (where sensitive personal data are processed before the monitoring is carried out).

Section 2(1)(c)(i) and (ii) — 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 it had 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. For example, such activity might be criminal activity, gross misconduct or health and safety breaches that jeopardise others.

Section 2(1)(c)(iii) — Is the monitoring being carried out and the personal data collected during the process, adequate, relevant and not excessive for 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 Acts. By way of example, 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.

Sections 4 and 6 — Is the monitoring of personal data being carried out in accordance with the rights of the data subjects under the Acts? For example, employees have the right to request access to the results and records of monitoring that has been carried out.

Sections 2.1(D) and 2(C) — 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? By way of example, staff

with access to information obtained through monitoring should be limited and should have received appropriate training as well as ensuring that data obtained through monitoring is secure.

Section 11 — This section 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 good practice points to consider in relation to lawful monitoring are as follows:

- an impact assessment should be undertaken before carrying out any monitoring to help ensure that carrying it out is proportionate. For example, monitoring should 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;
- if the results of monitoring might have an adverse impact for a worker (because, for example, it reveals evidence of a disciplinary offence) you 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.

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

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

"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."

Where an employer outsources staff data functions (for example: payroll, headhunting, data back-up etc.) to a third party individual or organisation that is to process personal data on behalf of that employer as a data controller, the Acts therefore require 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 to 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 in Sections 2.1(D) and 2(C). 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 Acts 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 in order to assist the data controller in complying with its obligations under the Acts;
- to ensure that it complies with Section 11 of the Acts, where it outsources those functions internationally (either directly or as part of a contractual chain — for example, an organisation outsources payroll to an Irish provider who in turn subcontracts some of the data processing internationally — say to a data back-up provider based in the UK or 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

Under the Acts, employees have a right to make a subject access request ('SAR') to access data held about them by their employer, provided they make the request in writing and pay a small fee. Employ-

(Continued on page 8)

(Continued from page 7)

ers should be aware that employees often exercise this right as a tactic to determine if the employer has complied with the Acts when processing their personal data — often in the middle of a grievance or disciplinary procedure.

Appropriate handling of SARS is therefore an issue regularly faced by HR departments — both how to deal with them and what should be provided when handling particular requests. One example could be where witness statements have been taken identifying third parties and whether the HR manager can disclose those statements without redaction or permission.

Appropriate handling of SARS is a subject that has been dealt with in numerous articles published in journal previously so will not be repeated here, other than to say that it is good practice to put a system in place so that SARs are always recognised and referred to appropriately trained staff for handling.

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

Gone are the days when we could bury our head in the sands when faced with a data protection breach or remain blissfully unaware that they were even taking place. On investigation, the Data Protection Commissioner will expect organisations to demonstrate awareness of the day to day breaches faced by the organisation, evidenced by a centrally maintained internal data protection breach register. The idea is that the breach register will help the organisation to pinpoint areas where there may be compliance gaps, a change in policy or training is required, or where a report needs to be made to the Data Protection Commissioner about the breach.

Employers should ensure that staff are appropriately trained 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 Data Protection Commissioner's Data Security Breach Code of Practice, which addresses situations where personal data have been put at risk of unauthorised disclosure, loss, destruction or alteration.

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 Section 2(1)(c)(iv) of the Acts — that information is not held for longer than is necessary for its particular use. Although the retention period will often be based on the business need of the particular 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 and all the information about that individual is needed. As the Acts do 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 and best practice requirements.

See 'How long should I keep data for?', in Volume 4, Issue 1 of *Data Protection Ireland,* for a more detailed discussion of the requirements for retaining and destroying data.

Final thoughts

HR teams have a great deal of responsibility vis a vis the information they hold about employees, and few would argue with the fact that they face a substantial challenge in carrying out their modern business functions in full compliance with the Acts. We hope that this brief look at some of the common issues faced by HR teams has at least conveyed a sense of what is required, and ways in which good practice can be built into processes so it becomes second nature. 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

Stephanie Pritchett leads PDP's training course, 'Data Protection Essential Knowledge Level 2', with dates in Cork and Dublin. For further details, please visit www.pdp.ie/training