Data protection and employment — Part 4

Oisin Tobin and Phillip Nolan, from Mason Hayes & Curran, discuss the data protection compliance issues involved in managing employee records and files

Virtually every employer has to deal with the vexing question of managing employee records and files. Employers considering this issue often find themselves caught between two competing sets of legal requirements.

On the one hand, data protection law embodies a principle of 'data minimisation' and directs that personal data must be deleted when no longer necessary for the purposes for which they were collected, or legitimately further processed. In contrast, employment law lays down mandatory time limits for which certain types of employee records must be kept. An employer who believes that it is robustly implementing data protection best practice by destroying old employee records may in fact find that it is breaking employment law by failing to keep those files for the relevant time period. Compliance in this area is akin to walking across a tight rope. Employers who lean too far on either the side of undue retention or undue minimisation could find themselves in difficulty.

To navigate through this issue, we recommend that employers apply a three-legged test when considering whether they need to, or can, retain employee files.

First, employee data *must* be retained for any time period mandated by statute. This is the case even if the employer does not have an internal reason (save for compliance with applicable law) for keeping the information. Employers should be aware that failing to retain relevant records may amount to a criminal offence. Second, employee data *should* be retained if an employer may legitimately require that information for the defence of legal proceedings down the line. Third, employee personal data *may* be retained in excess of the statutory time period or limitation period if they are still required in light of the purpose for which they were collected.

The background to all these issues is Section 2(1)(c)(iv) of the Data Protection Acts 1988 and 2003 (the 'DPA') which provide that 'data shall not be kept for longer than is necessary' for the specified, explicit and legitimate purpose or purposes for which they were obtained. When considering this issue, employers should be consistently asking whether it is necessary to continue to retain the relevant personal data.

Scope of personal data

From the outset, it should be remembered that employee personal data extends far beyond the mere content of an employee's HR file. The DPA defines personal data as including all data relating to an identifiable living person. Records generated which directly concern the employee (such as performance appraisals) are obviously personal data. However, other information held by an employer might relate to an employee, or ex-employee, and thus also fall within the scope of this definition. For example, emails or memos written and/or signed by an employee may constitute his or her personal data.

For how long *must* employee data be held?

At an absolute minimum, employee data must be retained for any mandatory time period laid down by statute. Various minimum retention periods flow from numerous separate statutes, and lack any obvious consistency or underpinning logic. While the most important of the current retention periods are set out below, these retention periods are not exhaustive and are subject to change. We would strongly advise that employers seek out specific and specialist legal advice to confirm how the various periods may apply to their given situation.

Wage information: The National Minimum Wage Act 2000 requires that employers keep such records as are necessary to show compliance with that Act's provisions (e.g. pay slips showing that employees were paid at least the national minimum wage). Such records must be maintained for three years from the date of creation.

Employment of minors: If an employer employs persons under 18 years of age, it must retain records showing that they have not breached the Protection of Young Persons (Employment) Act 1996 (i.e. that it has not employed children under the age of 16, except where permitted to do so). Again, these records should be kept for three years

from date of creation.

Hours worked: As most employers are well aware, strict rules govern employee working hours, breaks and leave. These rules are primarily set out in the Organisation of Working Time Act 1997. The 1997 Act, coupled with the Organisation of Working Time (Records) (Prescribed Form and Exemptions) Regulations 2001, require that records of weekly working hours (including holidays), the name and address of each employee, the employee's PPS number and a brief statement of his or her duties as an employee, be maintained. These records should be held for three years from the date of their creation.

Collective redundancies: If an employer is obliged to make collective redundancies, it is required to retain the documents necessary to show that the provision of the Protection of Employment Acts 1977—2007 were complied with. These obligations primarily relate to employee consultation and the provision of information. These records should be kept for three years from their date of creation.

Parental/force majeure leave: The Parental Leave Acts 1998 and 2006 require that an employer make a record of any parental or force majeure leave taken by their employees. This record should show the period of employment of the employee and set out the dates and times upon which the employee was on such leave. These records should be retained for eight years.

Tax records: Records of tax payments must be retained for a period of six years in accordance with accounting requirements under the Companies Acts and the Taxes Consolidation Act 1997.

Health and safety records: The Safety, Health and Welfare at Work (General Applications) Regulations 1993 require that records of accidents and dangerous occurrences in the workplace be retained. These should be held for ten years from the date of the accident.

For how long *should* employee data be held?

Certain types of employee data may need to be retained to defend any actions brought against the company. The most obvious examples would be personal injuries claims or actions for breach of contract. Civil procedure lays down various time limits (called limitation periods) in which different types of claim may be brought. If a claim is brought after the relevant limitation period has expired, it is said to be 'statue barred' and cannot be successfully prosecuted.

Limitation periods are crucial in determining how long records should be held. The retention period is essentially determined by the relevant limitation period. Records should be kept for so long as is necessary to defend any potential claim. If such a claim has been statute barred, it may be difficult to justify the continued retention of the records in the absence of some other justification.

If litigation is specifically threatened or commenced against the employer, the relevant files should not be destroyed at the end of the limitation period, but will usually be handed over to either the in-house legal team, or outside counsel, who may rely on their contents to defend the proceedings. It should be remembered that, once a dispute starts, the relevant employee records may amount to evidence in the proceedings, and their destruction at this stage could have very serious consequences.

Contracts: The Terms of Employment (Information) Act 1994 requires that an employee's terms and conditions of employment be maintained for the duration of the employment. There is no legislative obligation on an employer to maintain a copy of the terms and conditions after the contract has concluded. However, under the Statute of Limitations 1957, a claim for breach of contact can be brought for up to six years from the date of breach. It would be rather difficult for any employer to defend an alleged breach of contract claim without a copy of the original signed agreement. Consequently, contracts should be kept for at least six years from the date of the termination of the contract. It is generally recommended that contracts and data relating to any contractual relationships be retained for 7 years (to allow for claims which might be commenced towards the end of the limitation period).

Personal injury claims: Personal injury claims (including claims for psychological damage such as stress) must generally be taken within 2 years of the date of the cause of action (i.e. the event that caused the damage). A minimum retention period of 3 years is generally recommended, again to allow for any claims which might be taken toward the end of the statutory period.

Matters are somewhat complicated by the possibility of 'latent injury'. If the injured employee is not, and could not, be expected to be aware of their injuries, the statutory time limit will only start to run when they become so aware. The classic example of latent injury is asbestos exposure. Even if an individual is exposed to asbestos, the relevant injury may remain hidden for a number of years. In a case like this, the clock only starts ticking once the employee realises that they have been harmed.

For this reason, if employees are coming into contact with potentially hazardous chemicals or substances, the potential effects of which are not yet known, or which are known to give rise to latent illness, the relevant records might be retained indefinitely. It should be noted that the risk of latent injury does not justify the indefinite retention of all employee records. Only those records which may be relevant to defending proceedings alleging that the employer is responsible for the relevant personal injury ought to be retained.

In the case of minors, the statutory time limit for taking a personal injury claim only starts to run on the date the person turns 18. Therefore, records relating to data subjects under 18 years of age, which may be relevant in the context of a personal injury claim, should be retained until that person turns 18 and then further in accordance with the above guidelines.

Equality claims: Employers may, on occasion, find that they are subject to

(Continued on page 6)

(Continued from page 5)

claims by unsuccessful candidates for employment. The Employment Equality Acts 1988 — 2008 prohibit, among other things, discrimination with respect to access to employment. An unsuccessful candidate, who is of the view that they were passed over for a position due to a protected ground, such as race, sexual orientation or gender, may seek to bring equality proceedings. Such proceedings must be brought within 6 months (extendable to 12 months for reasonable cause) from the last act of discrimination.

In defending such proceedings, an employer will need to show that its hiring decision was not tainted by such discriminatory considerations. To this extent, it is useful to retain interview notes, the job specification and the candidate's CV. These records should be retained for one year from the date that the position is filled.

For how long *may* employee data be held?

Where employee records are not required to be held by law or to defend future proceedings, employers may retain the relevant data for so long as is necessary for the purpose or purposes for which they were collected or legitimately further processed. This needs to be ascertained on the facts of each specific case; there are no concrete periods of time on which data controllers can rely to comply with this requirement.

The Data Protection Commissioner's ('DPC') approach to this issue is best seen in his published Audit Report into the activities of *Facebook Ireland Limited*. On page 74 of this report, the DPC noted that "all periods chosen for the retention of personal data must be fully evidence based, and the period chosen cannot seek to cover all possible eventualities where personal data may be useful to the company."

It is the authors' experience that the DPC places a firm focus on the requirement that the relevant periods be 'evidenced based'. It is not acceptable to retain data indefinitely or for excessive periods simply on the assumption that it might 'come in useful' at some point. If there is no good reason for retaining personal data, then it should be deleted. Employers need to consider for how long they actually need to hold employee data (in light of the purpose for which it was collected) and then delete it after that period has elapsed. Provided that the retention periods adopted are not arbitrary and are backed up by clear and sustainable arguments as to why those periods are justified, employers may be able to justify their retention policies as being in accordance with the DPA. The primary compliance risk flows from situations where employers have not given any thought to this issue, and have simply stored data indefinitely.

From theory to practice

To adopt best practice, employers should review all the categories of employee data processed and consider the purposes for such processing. Data controllers should then consider how long these data need to be kept for the relevant purposes. A useful tool for demonstrating compliance is to compile a 'data retention policy' that sets out the relevant periods of time for which data in relevant categories may be held. Any data retention policy should be informed by the mandatory periods for which data must be retained. If employee data are being retained for an extended period of time, or in excess of the statutory periods set out above, the reasons for such retention should be documented in writing. On an investigation by the DPC, such documents show that thought has been given to the relevant data retention periods.

When archiving employee personal data, employers should be alert to the fact that employees, or ex-employees, can exercise their full suite of data protection rights in respect of the archived data. For example, they may seek access to the data by making a subject access request, or may require that the employer alters any incorrect records. Archived records must be securely stored.

When destroying personal data at the end of the retention period, employers should be aware that the destruction will itself amount to 'processing' and must be undertaken in compliance with the DPA. Particular care should be paid to ensure that the data are destroyed securely. Any hard copy documents should be properly shredded in-house or by a reputable outside company; employee files and contracts should not simply be thrown out with other waste. Employers should also note that the DPA only apply to data which relate to an identifiable individual. If an employer believes that there is merit in retaining data over a longer period of time (such as for statistical analysis) it may be worth considering the possibility of anonymising the records. This may allow for the data to be retained indefinitely. Care must be taken to ensure that the anonymisation process is done properly. If it is possible to 'reverse' the anonymisation and relate given pieces of data to employees or ex-employees, then these files may still fall to be counted as personal data.

Conclusion

The retention of employee records sits at the junction of employment and data protection law. This is a complex area and one where great care needs to be taken. To navigate the thicket of regulations, an employer would be well advised to formulate and implement a data retention policy. Such a policy must be driven by evidenced based justifications for the retention of various forms of employee data. In particular, employers must be aware of the fact that certain types of data must be retained to comply with the strictures of employment law, whereas other forms of data constitute vital evidence that an employer may need to defend itself in the event of a legal dispute down the line.

Philip Nolan and Oisin Tobin
Mason Hayes & Curran
pnolan@mhc.ie
otobin@mhc.ie