Data protection and employment — Part 3

Oisin Tobin and Phillip Nolan, from Mason Hayes & Curran, analyse the implications of transferring information outside of the organisation

Few organisations keep all aspects of employee administration in-house. Many firms outsource certain HR functions, such as payroll processing or pension administration, to specialist providers. While such outsourcing is common and generally accepted, in practice, it can give rise to certain data protection issues. These challenges flow from the fact that the employer, a data controller, is transferring employee personal data to another entity. This recipient may hold the personal data as either a data processor or a data controller. A transfer of personal data must comply with a number of requirements under the Data Protection Acts 1988 and 2003 ('the DPAs'). These obligations differ depending upon whether the recipient is a data controller or a data processor.

This article sets out a framework that employers can use to evaluate their responsibilities when transferring employee data. This requires a consideration of a number of separate issues:

- has a data transfer taken place?;
- is the recipient a data controller or a data processor?;
- what are the requirements for a transfer to a data controller?;
- what are the requirements for a transfer to a data processor?; and
- has the personal data left the European Economic Area?

Has a transfer taken place?

In many cases, the issue of whether a transfer has taken place will be obvious when an employer is transferring employees' personal data. However, there may also be cases where matters are not so clear cut. This is particularly the case where the transfer is being made between different legal entities that form part of the same corporate group.

Many modern businesses are structured as a group of separate companies controlled, via shareholdings, by a single parent company. For example, in a retail chain, each individual shop might be owned and operated by a separate company, operating under the direction of a central parent company.

It is important to bear in mind that the DPAs do not contain any specific exemptions for data sharing within the corporate group. If one company in the group transfers personal data about its employees to another company in the same group, then it will still need to ensure that the relevant requirements for a transfer of personal data have been met. This is so even if, from the outside, the separate companies all appear to form part of the same business.

Data controller or data processor?

Before an employer transfers employee personal data to a third party, it must first ascertain whether the recipient will hold that information as a data controller or a data processor. Different steps must be taken to ensure compliance in a data controller to data controller transfer, and a data controller to data processor transfer.

In its Opinion on the concepts of controller and processor (Opinion 1/2010), the Article 29 Working Party stressed that the classification of an entity as a data controller or a data processor is fundamentally a factual assessment and is not dependent upon the labels the parties chose to use to describe themselves. The DPAs define a data controller as being an entity that controls the "content and use" of personal data. Consequently, a recipient will likely be classed as a data controller where it has some flexibility in how it can use the employee data it receives. The Working Party advises that "being a controller is primarily the consequence of the factual circumstance that an entity has chosen to process personal data for its own purposes."

If the employer is transferring employee information to an entity that is likely to use that personal data to further its own objectives, the transfer is likely to be a data controller to data controller transfer. Common exam-

ples are the provision of employee information to the Revenue Commissioners, or the sharing of employee information between various companies in the same corporate group.

In contrast, if the recipient of the personal data is only entitled to process that information on behalf of the employer, the recipient is likely to be classed as a data processor. Payroll suppliers are usually in this category.

Data controller transfer

To ensure that any transfer to a data controller is lawful, the employer should confirm, in particular, that:

- one of the pre-conditions to processing has been met; and
- the transfer is transparent.

The transfer of employee data is a form of processing. Consequently, one of the pre-conditions for processing set out in Section 2A DPAs (or Section 2B in the case of sensitive personal data) must be met.

For non-sensitive personal data, the most important justifications that an employer may invoke to justify the transfer are employee consent, the contract of employment and the legitimate interests of the employer.

Where feasible, an employer should seek specific employee consent for any transfer outside of the organisation. It may be possible to obtain such consent as part of a general data protection policy. However, it should be noted that the Article 29 Working Party has questioned the validity of consent given in the employment context. Consequently, an employer would be ill-advised to rely solely on consent as a justification for transfer.

In certain cases, an employer may be able to rely on the contract of employment to justify the transfer. However, this pre-condition only applies if the transfer is necessary for the performance of the contract. It is arguable that if the employment contract can be performed without the transfer of personal data, this justification may fail.

"In certain cases, an employer may be able to rely on the contract of employment to justify the transfer. However, this pre-condition only applies if the transfer is necessary for the performance of the contract. It is arguable that if the employment contract can be performed without the transfer of personal data, this justification may fail."

Finally, the processing may be justified if it can be shown to be in the legitimate interests of the employer, or the third party to whom the data are disclosed, unless the processing amounts to an unwarranted interference with the rights and interests of the employee. In many cases, employers will be able to rely on this justification to transfer personal data, provided that the transfer does not unduly prejudice the rights of the employee. Employers seeking to rely on this justification should consider the intended recipient of the personal data and satisfy themselves that there are adequate safeguards in place to protect the employees' data.

It is possible to transfer sensitive personal data (such as details of trade union membership). However, in such circumstances at least one of a number of additional pre-conditions must be met. Notably, any employee consent to the transfer must be explicitly given. Alternatively, the employer may be able to effect the transfer, even without explicit consent, if it can show that the transfer is necessary for the employer to exercise any right, or comply with any obligation, imposed by law in connection to employment. Before any transfer takes place, an employer should form a view as to which, if any, of these pre-conditions for processing applies. As a matter of good practice, this determination should be in writing.

Even if one of these pre-conditions have been met, the transfer may be unlawful if it is unfair. Section 2D(2)(d) DPAs provides that fair processing may require that the employee be given information as to the recipients or categories of recipients of their personal data. Consequently, employers should disclose, to their employees, any individuals to whom they intend to transfer their personal data. Conversely, the principle of fair processing also requires that the recipient of personal data notify the employee of its identity and the manner in which they obtained the personal data.

Data processor transfer

If the recipient is a data processor, the employer must ensure that it complies comply with Section 2C(3) DPAs. A written agreement must be put in place between the employer and the proposed data processor. An oral agreement is insufficient.

In addition, this agreement must contain a number of terms to ensure compliance with the DPAs. It must explicitly provide that the data processor can only process the employee personal data on, and subject to, the instructions of the employer. The data processor must contractually agree to implement appropriate technical and organisational security measures to prevent unauthorised access to, or alternatively disclosure or destruction of, the employee data.

From a negotiation standpoint, employers should be aware that these terms are a legal requirement, as opposed to a "nice to have". In addition, employers should note that they are obliged to take "reasonable steps"

(Continued on page 6)

(Continued from page 5)

to ensure that the data processor complies with its commitment to keep the data secure. This is often done by seeking formal audit (entry and inspection) rights in the contract. Alternatively, the employer may seek detailed information about the security system in place to satisfy itself that sufficient safeguards are in place.

From a practical standpoint, it is advisable for any employer engaging an outsourcing provider, such as a payroll processor, to insist on receiving a copy of the provider's written terms of service. These should be checked to ensure that they contain the required limitations on the use of the data and contain the relevant commitments as to security. Any omissions should be queried and resolved.

In addition, it is worthwhile seeking details of any security procedures in place to ensure that they are satisfactory. The relevant documents, along with details of the reasonable steps taken by the employer to ensure compliance, should be kept on file.

In certain cases (such as a wholesale outsourcing of a key function) it may be prudent for an employer to engage outside counsel to negotiate the relevant agreement.

Where are the data being transferred to?

Section 11 DPAs imposes strict restrictions on the transfer of personal data outside of the European Economic Area. Consequently, if employee data are leaving Europe, the employer will need to ensure that one or more of the pre-conditions to data export has been met.

If the personal data are going to a jurisdiction that has been approved by the European Commission, the data export can go ahead with no further formalities. The key approved jurisdictions are Switzerland, Argentina and Israel. Canada has been approved for certain types of data.

If the transfer is going to a US entity that participates in a voluntary 'Safe Harbor' scheme, operated by the US Department of Commerce, the transfer can go ahead. From a practical standpoint, it is worth checking if a US recipient is participating in this scheme. If the data are being exported to another jurisdiction, or a US entity that is not in Safe Harbor, it will generally be necessary to obtain the specific consent of the employees to the export of the data to that jurisdiction.

If such consent is impracticable or not forthcoming, an employer may wish to consider entering into a special EU-approved contract, called a model form agreement, with the recipient. The use of such a contract is generally regarded as best practice and would be advisable (bearing in mind the question mark hanging over consent in the employment context) if a considerable export of data is to take place.

Model contracts for data exports can be downloaded from www.pdp.ie/documents

Conclusion

Transferring employee information can be tricky. Employers should be alert to the fact that transfers can happen frequently, particularly within a corporate group. The steps that need to be taken to ensure compliance will depend on whether the recipient will be treated as a data processor or a data controller. In either case, it is important to be able to show that the employer thought through the issues and took documented steps to ensure compliance with the DPAs.

Additional challenges can be encountered if the data are to be exported outside of Europe. However, these challenges are usually manageable with effort and fundamentally come down to obtaining employee consent and/or putting a proper agreement in place between the employer and the recipient.

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