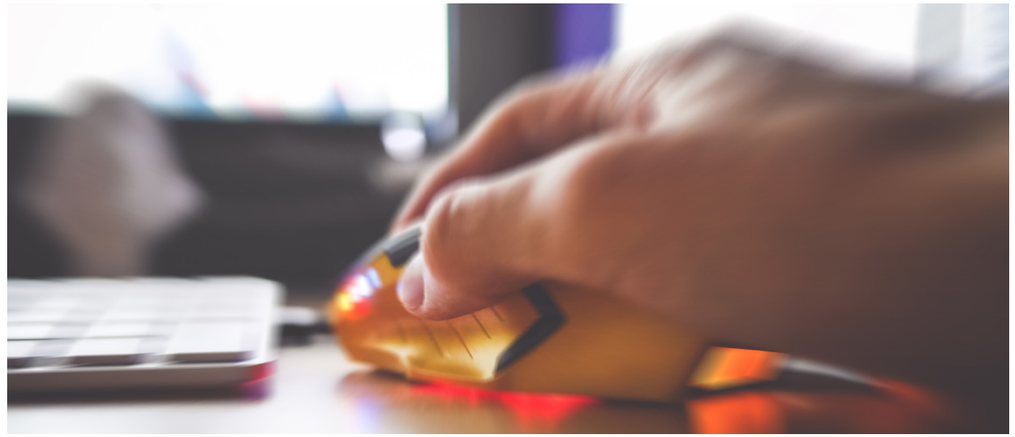
# *Data Sharing in the Public Sector*

Fleur O'Shea is a solicitor in leading law firm ByrneWallace and practices exclusively in the area of employment law. Fleur advises on all aspects of contentious and non-contentious employment law and has particular expertise in the area of data protection.



Data-sharing has been on the Government's agenda for quite some time now. As far back as November 2012, the Department of Public Expenditure and Reform (DPER) released a Circular noting that,

> "(t)here are significant benefits to be gained from the greater sharing of data held by public service organisations both to achieve greater efficiency in the delivery of public services and to maximise convenience and other benefits for the user of those services ...".

In a policy paper on data-sharing and governance published by DPER in 2014, it was noted that,

> "(d)ata is the single most important resource available to public bodies, and is fundamental to the effective performance of the multiple roles and responsibilities of public bodies".

Following a consultation process, the Government approved the drafting of a Data-Sharing and Governance Bill in July 2015 and we wait to see what happens next. While the benefits of data-sharing are easy to see, to avoid falling foul of data protection law, the possible legal implications of data-sharing must be considered by public sector bodies in each and every case.

**Data Protection – the Basics**

The Data Protection Acts 1998 and 2003 (hereafter "the DP Acts") require data controllers to adhere to eight golden rules when processing data. These rules require the data controller to:

- Obtain and process data fairly;
- Keep the data only for one or more specified, explicit and lawful purpose(s);
- Use and disclose the data only in ways compatible with these purposes;
- Keep the data safe and secure;
- Keep the data accurate, complete and up to date;
- Ensure that the data is adequate, relevant and not excessive;
- Retain the data for no longer than is necessary for the purpose or purposes; and
- Give a copy of any personal data to an individual data subject, on request.

The Office of the Data Protection Commissioner (ODPC) has prepared a range of useful guidance notes to assist a data controller in complying with these rules. However, the positon becomes considerably more complicated when the original data controller wishes to share data with another public body.

The problem with data-sharing is that, while the original data controller may have complied with its obligations to the data subject at the time the data is first collected, the sharing of the data with another public body constitutes further processing of the data. This means that, unless one of the permitted exceptions applies, the original data controller will be in breach of its legal obligations unless the data subject was given details of the future sharing of the data at the time of collection, or the data controller can establish that the sharing was one of the purposes for which the data was collected.

**The European Angle**

The difficulties posed by the sharing of data between public bodies were highlighted in the case of *Bara* & *Ors*[i]. Ms Bara was a self-employed Romanian citizen who challenged the lawfulness of the transfer of her personal data by the national tax authority to the national health insurance authority. Romanian law permitted public bodies to transfer personal data to the national health authority to enable it to determine whether an individual could be categorised as an insured person. In order to carry out this assessment, the national health authority required a range of data, but did not require details of an individual's income. Romanian law provided that these data transfers could be carried out by reference to an agreed protocol concluded between the public bodies. This protocol was akin to an administrative measure, rather than a legislative provision.

Ms Bara argued that the transfer of personal data relating to her income was not necessary as the national health authority did not need this information to carry out its assessment. She also argued that the personal data had been transferred and used for purposes other than those that had initially been communicated to her, without her prior explicit consent, and in reliance on an administrative protocol. The Romanian Court of Appeal decided to refer the matter to the Court of Justice of the European Union to establish whether or not a public body could transfer personal data to another public body for further processing in these circumstances.

Finding in favour of Ms. Bara, the Court noted that the Data Protection Directive (95/46/EC) permits Member States to restrict the scope of individual obligations and rights provided elsewhere in the Directive when such restriction constitutes

> "a necessary measure to safeguard … an important economic or financial interest of a Member State … including monetary, budgetary and taxation matters … [or] … a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority [in certain cases]".

The Court noted, however, that the Directive expressly requires that any such restriction is imposed by a legislative measure. The Court found that, as the transfer had been effected in reliance on an administrative protocol and not a legislative measure, the transfer of data between the national tax authority and the national health insurance authority was in breach of the Directive.

**Ireland – Ahead of the Curve**

A similar scenario had, in fact, already been considered by our own Data Protection Commissioner in 2002. In Case Study 8 of 2002[ii], a complaint was made by a serving member of the Defence Forces who had obtained damages arising out of a civil action taken by him against the Minister for Defence. The complainant alleged that details of the settlement had been forwarded by the Department of Defence (DOD) to the Department of Social and Family Affairs (DSFA), without his knowledge or consent, to check if he was in receipt of Social Welfare means-tested payments.

During the course of investigation, it emerged that the DSFA had sought details of compensation payments for hearing loss made to ex-members of the Defence Forces on the basis that "it is possible that some of the many compensation claims currently being paid to ex-members of the Defence Forces should be assessed as means for Social Welfare payments". On foot of this request, the DOD released a list containing the details of compensation claims made by 4,275 individuals who were in receipt of Social Welfare payments.

The Commissioner noted that

> "this case raised important and complex issues relating to the conditions which need to be met for personal data to be shared between Government Departments. Questions arose as to whether the Department's purpose in processing claims could be said to include the protection of public funds by another organ of the State, whether the disclosure to the Department of Social and Family Affairs could be considered to be a compatible purpose and whether the 'public interest' test could be used as a basis for the disclosure."

The DOD sought to justify the disclosure by asserting that:

1. The initiation and maintenance of legal proceedings in this case, as with others, was a matter of public record.
2. The settlement by the State of the claim, out of public funds, was not the subject of any agreement on confidentiality between the parties.
3. The provision of information on the fact and amount of the settlement by one Department of State to another to ensure the proper administration of the Social Welfare Code was entirely proper and appropriate.
4. The legal restrictions on the disclosure of personal data do not apply if the disclosure is "required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duties or other monies owed or payable to the State…".

The Commissioner firstly found that the data in question was generated by the DOD for the purposes of processing applications for compensation and for managing the civil actions and associated settlements that arose. It was not clear to the Commissioner that this purpose included the provision of assistance to other State agencies charged with investigating offences against the State. The DOD argued that the protection of public funds from the possibility of a second claim by any of the data subjects concerned was encompassed within the original purpose. The Commissioner disagreed, stating that:

> "While the Department, of course, has an obligation to ensure that it spends public funds appropriately … it has no direct responsibility or accountability for the expenditure of another Department. Indeed, I found it difficult to understand how, in the absence of clear evidence that public funds had been abused, that the data was released. In the absence of a statutory provision at the time, or clear evidence that public funds had been abused in specific cases, the Department of Defence could not assume a new purpose for the data retrospectively as a basis for disclosure."

The Commissioner did not accept that the disclosure was permitted on the ground that non-disclosure was likely to prejudice the prevention, detection or investigation of an offence, being one of the permitted exceptions to the legal rules pertaining to the disclosure of data. The Commissioner stated that this exception only applies where it is clearly established, in each specific case, that the non-disclosure of particular data would prejudice the prevention, detection or investigation of an offence.

Analysing whether or not the "public interest" and the aim of protecting public funds could justify the disclosure, the Commissioner noted that the Social Welfare (Consolidation) Act 1993 generally facilitated the exchange of data between the DSFA and other Departments for the specific purpose of controlling Social Welfare schemes in specific cases where there is a substantial risk that public funds could be abused. The Commissioner concluded, however, data could only be shared by a Department with the DSFA if there was a substantial risk, rather than a mere chance, that public funds could be abused.

Upholding the complaint, the Commissioner noted that

> "each government department is a data controller in its own right – Government is not a universal data controller – and there are mechanisms in place in Social Welfare and other Laws for the exchange of personal data, as necessary. I liken this to the bulkheads in a ship, so that data given for a particular purpose is compartmentalised and may not be used for other purposes without the consent of the citizen or without a statutory basis."

This case illustrates that the legal position in Ireland was already in line with the Data Protection Directive before the judgment in *Bara*. Nevertheless, after Bara, the ODPC took the opportunity to restate the importance of adherence to Data Protection law when sharing data. Commenting on the judgment, the ODPC stated that

> "(t)he consequences of this judgment are significant and potentially very far reaching. The Office of the Data Commissioner recommends that all public sector bodies complete a full review of their obligations and arrangements on the basis of the findings in this judgement to ensure that those arrangements are fully compliant with the Data Protection Directive 95/46/EC."

The ODPC recently updated its Guidance Note on Data-Sharing in the Public Sector to incorporate reference to the Bara judgment. The updated Guidance Note makes it clear that all data-sharing arrangements in the public sector should:

- have a basis in primary legislation;
- make it clear to individuals that their data may be shared and for what purpose;
- be proportionate in terms of their application and the objective to be achieved;

- have a clear justification for individual data-sharing arrangements;
- share the minimum amount of data to achieve the stated public service objective;
- have strict access and security controls; and
- ensure secure disposal of shared data.

**Conclusion**

The ODPC's Guidance Note provides a useful starting point for public bodies but does not offer sufficient clarity as to acceptable levels of security and access controls. Unauthorised access to data by individual employees, in both the public and private sectors, has been a frequently recurring theme over the last couple of years and our increasingly online world has created lucrative business opportunities for cyber-criminals making it even more important for minimum IT security standards to be agreed.

While there is certainly much to be gained from data-sharing in the public sector, the lessons learned illustrate that, to ensure legal compliance, careful and extensive planning is required before any steps are taken to share data, no matter how compelling the case for data-sharing may be.

**Notes**

i (Case Reference: C-201/14, 1 October 2015)

ii Available at: https://www.dataprotection.ie/view-doc.asp?Docid=117&Catid=39&StartDate=1+January+2016&m=