Wrestling with the Data Protection Act 1998

BY BRIDGET PETHERBRIDGE
counsel, WilmerHale

THE BEGINNING OF ANY KIND OF INTERNAL investigation is a fraught time for in-house lawyers. Whether the investigation has been triggered by suspected corrupt conduct, accounting irregularities or the inklings of attention from a prosecutor, things usually need to happen fast and thinking time can be scarce.

While all minds are focused on the problem in issue, however, some care needs to be taken to avoid the rock lying below the swirl of activity, otherwise known as the Data Protection Act 1998. While all responsible corporate entities will already have data protection policies and procedures in place to cover their day-to-day operations, a number of 'one off' events may arise in the course of investigations which raise issues of data protection. Some forethought is wise to ensure that enforcement action by the information commissioner's office (ICO) and/or complaints from data subjects do not compound the woes of a company already embroiled in a difficult scenario.

OBLIGATIONS UNDER THE ACT

The Data Protection Act 1998 is notoriously convoluted, but basically provides that the handling (which includes collection, storage and just about everything in between) of 'personal data' must be carried out in a way which is consistent with its eight principles. If the processing departs from these principles, a breach will occur unless a relevant exemption or derogation applies. They are, broadly, that data must be:

1) fairly and lawfully processed;

2) processed only for limited purposes;

3) adequate, relevant and not excessive for the above purposes;

4) accurate and up to date

5) not kept for longer than is necessary for the above purposes;

6) processed in line with the rights of the data subject;

7) kept secure;

8) not transferred to other countries outside the EEA without adequate protection.

WHAT IS CAUGHT? – 'PERSONAL DATA'

The provisions of the 1998 Act will need to be considered whenever 'personal data' is to be processed in the course of an investigation.

'Data' includes all information held on computers (entered either manually or scanned) or recorded with the intention that it be so held. Information in paper form is also 'data' where it is held in 'a relevant filing system', ie a filing system that permits ready access to information about particular individuals. The definitions of when this would and would not apply are legion but one should generally assume that anything other than hard copy information kept in a disorganised and impenetrable fashion might be considered 'data'.[1]

'Personal' data is that 'relating to a living individual who can be identified from the data or the data combined with other information in the control, or likely to come into the control, of the data controller'.[2] The question as to whether the data is capable of identifying a living person is a relatively straightforward one. The meaning of 'relate to' is more contentious, however. A Court of Appeal case[3] applied a definition which narrowed the concept of 'relate to' according to what was variously described as a 'continuum of relevance to the data subject', whether the data is 'biographical in a significant sense', or whether the data subject is the 'putative subject' of the data. It is, said the Court, 'information that affects his privacy; whether in his personal or family life, business or professional capacity.'

The ICO has since published lengthy technical guidance as to what 'personal data' is, which is broader than the CA's definition and extremely unwieldy to apply. Given the practicalities of the review process in most large-scale investigations, it is probably prudent to assume that all data capable of identifying a living individual is potentially 'personal data' and treat it accordingly.

WHO IS CAUGHT? – 'DATA CONTROLLER'

A word of warning for professional clients and their lawyers is to be found in guidance issued by the ICO, which deems them often both to be data controllers in respect of the material processed in the course of their relationship. While a lay client, such as a party to a divorce, is effectively deemed to hand over responsibility for data protection to their lawyer, the professional client and its lawyer will often be considered by the ICO jointly to share responsibility for compliance with the 1998 Act.[4]

Indeed, the ICO recommends that, where professional clients engage specialist advisers, contractual arrangements are put in place to determine who will take responsibility for data protection. Certainly, however dull the subject of data protection may appear in the midst of the more exciting topics of corruption, dishonesty or regulatory proceedings, these are matters to raise and discuss with lawyers at the outset of the engagement.

APPLYING THE DATA PROTECTION ACT IN THE CONTEXT OF INVESTIGATIONS

There are plainly many categories of 'personal data' that will be processed as part of normal business operations such as: employee and customer/client records; identifying data contained in e-mails and meeting notes and telephone recordings. All responsible businesses will have in place data protection policies to ensure that such data is gathered in accordance with the rights of data subjects, kept accurate, up to date and for no longer than necessary and kept under conditions of security appropriate to its sensitivity.

Once such data comes within the purview of an internal investigation, however, new considerations arise and given the paucity of case law or specific ICO guidance to assist. In many respects, judgement will need to be exercised at a number of stages such as:

- gathering personal information from employees in interviews;
- building and reviewing databases containing personal data;
- transferring material to lawyers in the UK;
- transferring material to third-party vendors;
- transferring material to lawyers outside the UK, eg in the US;
- disclosing material to UK regulators; and
- disclosing material to US or other regulators.

> ***'"Personal" data is that "relating to a living individual who can be identified from the data or the data combined with other information in the control, or likely to come into the control, of the data controller."'***

LEGITIMISING CONDITION

The first consideration before any processing takes place is that a 'legitimising condition' must exist, which is a precondition to processing the data at all.[5] This will not usually prove to be an obstacle but the fact that the requirement has been considered should be documented if it is felt that a processing is out of the ordinary or may be questioned in the future.

There are a number of potential 'legitimising conditions', the first of which is the consent of the data subject to the processing. Consent is a gateway in respect of many of the 1998 Act's provisions but, while superficially attractive, it can, in practice, be problematic. It will usually be difficult to gain consent of third parties and, as consent must be both informed and freely given to be effective, the disparity of influence between employer and employee may invalidate it.

The legitimising condition most likely to be relied upon in the context of internal investigations or voluntary co-operation with regulators is, therefore, that the processing[6] is 'necessary for the purposes

NOTES

1) Health, educational and certain housing/social services records as well as all information held by public authorities is also 'data', however held.
2) Data Protection Act, s1(1).
3) *Durant v Financial Services Authority* [2003] *EWCA Civ 1746*, a case which dealt with the data subject's attempts to exercise his right under the Act to access data rather than with a potential breach.
4) 'Identifying Data Controllers and Data Processors – Data Protection Act 1998'.
5) Principle 1, Schedules 2 and 3.
6) Where the data is 'sensitive personal data', more stringent 'legitimising conditions' apply but this type of data is far less likely to be encountered in commercial entities (outside of the HR arena) than within the type of public bodies that have received the vast bulk of monetary penalties to date for breaches of the Act.
7) Principle 6 relates to the data subject's rights of access that address different issues to those usually encountered in these contexts.
8) The same criteria as those legitimising the processing of sensitive data but applied in a different context.
9) An online scheme of self certification overseen by the Federal Trade Commission.
10) Commission Decision 2001/497/EC15 15 June 2001; Commission Decision 2004/915/EC17 27 December 2004.
11) The Eighth Data Protection Principle and International Data Transfers, ICO guidance, ICO website.

of legitimate interests pursued by the data controller or third party or parties to whom the data are disclosed'. That will permit processing other than where 'the processing is unwarranted by reason of prejudice to the rights and freedoms or legitimate interests of the data subject'. There is thus a balancing act to be performed but the very substantial interests engaged in the context of potential criminal or regulatory sanctions would ensure that such an exercise would usually reasonably conclude in favour of processing.

Consideration must then be given to the remaining principles. Some could prove problematic in terms of an internal investigation which might, for example, fall foul of the requirement that personal data be used only for a purpose for which it was gathered or would have been within the contemplation of the subject.

The relevant exemptions require close attention, therefore. s35 provides such an exemption in respect of the 'disclosure principles' (principles 1, 2, 3, 4 and 5[7]) where a disclosure is contemplated that is either required by 'any enactment, rule of law or court order', or is 'necessary for the purpose of legal proceedings or for the obtaining of legal advice or for establishing, exercising or defending legal rights'.[8]

Where there is a compulsory request in play, the situation is straightforward. Where, however, an entity is contemplating voluntary disclosure to regulators the 'necessity' requirement must be taken seriously. The assertion that material was necessary simply because a regulator has asked for it may not satisfy that test. Rather the controller should take steps to satisfy themselves that the request is relevant, reasonable and rational and to ensure that only relevant material, necessary to the purpose in question, is disclosed or processed.

Section 29 of the 1998 Act provides an overlapping exemption to the 'disclosure principles' where any processing is for the purpose of 'the prevention or detection of crime' as may very often be the case in the course of an internal investigation.

> ***'The sensitivity of data may increase considerably as it is deployed in a potentially criminal investigation and security measures may need to be reconsidered accordingly.'***

The exemption applies, however, only insofar as the application of those principles would prejudice the purposes of the prevention and detection of crime. The correct approach in respect of applying s29 to these principles is t herefore to ask whether there is any reason NOT to follow them. If they can be observed, they should be.

One consequence of such application is that, where new personal data is collected in the course of the investigation such as in the course of witness interviews, data subjects should be informed of the purpose for which their data is being used unless that will jeopardise the whole purpose of the investigation.

Most crucially, neither of these exemptions has any impact on the requirement in principle 7 to take appropriate organisational and technical measures against unauthorised processing or accidental loss or destruction of personal data. The sensitivity of data may increase considerably as it is deployed in a potentially criminal investigation and security measures may need to be reconsidered accordingly. Both client and outside counsel should be well aware of the security measures that the other is implementing and ensure that contracts with processors, such as database hosts or contracted reviewing lawyers, are properly reviewed for data protection clauses.

THE 'EXPORT BAN' AND ITS DEROGATIONS

A further layer of complication arises where there is a need or desire to transfer personal data out of the European Economic Area (EEA), an export that is *prima facie* forbidden by the Principle 8 'export ban'. Such may often occur either where the primary lawyers are located out of the EEA, or where requests for disclosure of material are received from overseas regulators with whom entities under investigation will wish to cooperate, often on a voluntary basis.

The 1998 Act prima facie permits transfer of personal data to areas outside the EEA such as the US only where there is some means of assuring its protection on arrival. Those means might be via the 'Safe Harbor'[9] scheme, suitable contractual arrangements[10] or binding corporate rules (BCRs) approved by the Commissioner.

None of those arrangements are often practicable in the course of a one-off, fast moving investigation, however. Consent is a potential gateway to transfer but, for the reasons explored above, might be a difficult criterion actually to fulfill.

The gateway most appropriate in the context of regulator's requests or internal investigations uses the same words as s35 so that transfer out of the EEA is permitted if it is:

> '...necessary for the purpose of or in connection with any legal proceedings, necessary for the purpose of obtaining legal advice or otherwise necessary for the purposes of establishing, exercising or defending legal rights'.

The legal proceedings do not have to involve the transferring entity[11] as a party and the legal rights do not have to be those of either that entity or the data subject. Again, however, the term 'necessary' is key.

The ICO states that the condition would be met where, for example:

> 'A parent company based in a third country is sued by an employee based at one of the European subsidiaries, and the company requests the European subsidiary to transfer certain data relating to the employee as the data is necessary for the defence'.

The example does not clarify what is meant by 'necessary' to any great extent, however. Should the data first be reviewed within the EEA and only that which is to be disclosed or relied upon transferred? Should non-EEA lawyers move to the data to assess it for relevance/necessity or can it go to them?

The line is not a clear one and the reasons why it may be 'necessary' to export any particular piece of data will always depend on the circumstances. Plainly, as the review process progressively requires higher levels of expertise and familiarity with the case which reside outside of the EEA, the justification for export for review purposes grows. The more urgent the legal matter, the greater the necessity to get material to the core advisers quickly. The data controller should always consider, however, whether the legal purposes in question can be achieved without exporting any or all of the personal data. If, for example, anonymised information would suffice, why can the relevant redactions not be carried out within the EEA? If personal data will be filtered out by a review process, why can that process not be conducted within the EEA? There must always be an answer to the question as to why particular data has to be transferred and cannot be dealt with within the EEA if transfer is to be compliant.

Durant v Financial Services Authority [2003] *EWCA Civ 1746*

POST-EXPORT CONSIDERATIONS

Once data has been transferred out of the EEA, it potentially passes outside the jurisdiction of the Act so that only local law then applies. That will not always be the case, however, where control continues to rest with an entity established in the UK. The extent to which such an entity may be deemed to continue to pursue a common purpose with the transferee such that they remain jointly liable for any breaches of the Act will require careful consideration. Any transferor of data outside of the EEA (to either a joint controller or a mere processor) that proposes to retain some control over that data should ensure that it will be dealt with in a manner consistent with the 1998 Act.

CONCLUSION

The terms of the 1998 Act, which provides exemptions and derogations based on necessity and legal interest imperatives, should not operate to prejudice a data controller in the conduct of its legal affairs. There should always be mechanisms and procedures to ensure that the overriding purpose of an internal investigation or dealings with regulators is met. What the Act requires, in essence, is that these operations be conducted with due regard to the rights of data subjects or that their rights are never compromised for no proper reason. Careful thought and some planning should avoid data protection pitfalls, however urgent and compelling the wider legal context.

By Bridget Petherbridge, counsel, WilmerHale
E-mail: bridget.petherbridge@wilmerhale.com.