TRAVERS SMITH

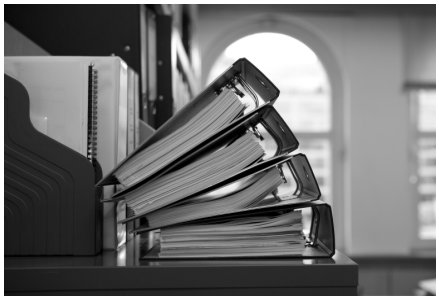
Data protection

Is your business doing enough?

With stories of "lost lap-tops" and "system security breaches" hitting the headlines and new enforcement powers on the way, is your business doing enough to comply with data protection laws? In this briefing, we look at some of the key issues for businesses which handle personal data.

What does the law say?

In the UK anyone who is responsible for the use or storage of "personal data" is required to comply with the Data Protection Act 1998 (the "Act"). Amongst other things, this means that any data which is held must be kept safe and secure, must be accurate and up-to-date and must be erased when it is no longer needed. The underlying theme of these requirements is that personal data should be obtained and used "fairly".



Most businesses hold personal and potentially confidential information relating to employees (e.g. salary and health details) and customer contacts. The more personal data a business holds, the more likely it is to attract scrutiny from the data protection authorities.

What happens if you fail to comply?

Until recently, the Act has largely been viewed as fairly toothless when it comes to penalties for non-compliance, with the enforcement authorities often unable to do more than issue a 'slap on the wrist' (although the Financial Services Authority has imposed significant fines on firms which it regulates for breach of its own data protection rules).

However, new legislation allows fines of up to £500,000 to be levied for any "serious contraventions" of the Act.

In practice it is likely that enforcement will be targeted at organisations which fail to keep their large databases secure.

Owners of databases also need to consider the potentially damaging reputational risks and the administrative cost of trying to rectify data protection breaches, both of which could be significant.

How good are your systems?

Recently there have been well-publicised examples of junior employees putting their employers in serious breach of the Act, for example by putting unencrypted disks in the post or leaving unencrypted laptops unattended.

"From 6 April 2010, substantial fines can be levied for 'serious contraventions'."

It is worth considering whether you and/or any third party to whom you have delegated processing of personal data have policies, procedures and training which are adequate to minimise these mistakes and whether your/their staff are alive to the risks. Even where you have engaged a third party to process data on your behalf, these are responsibilities which you cannot delegate, so you need to ensure that your processor meets best practice.

A proper contract

When you appoint someone to handle personal data for you, the Act requires both due diligence and a formal written contract satisfying minimum criteria.

Moreover, if the data is to be processed outside the EEA (e.g. in India) further complex issues arise. Do your arrangements comply? Has your outsourced processor contracted to take responsibility and/or indemnify you if they get things wrong?

Passing data to other people

- Does your business regularly pass personal data to third parties?
- Are procedures in place to ensure that subject access requests are genuine and are handled promptly?

In each of these instances you will need to ensure that appropriate steps have been taken to avoid a breach of the Act.

Key questions to ask

In our experience, the following matters also require careful consideration:

- Is data kept securely? Where appropriate, are relevant computer files encrypted? Are regular data protection risk reviews carried out?
- Is data taken off-site (e.g. on laptops)? Is this actually necessary?
- Do you carry out a regular "weeding out" process to make sure you are not holding out-of-date or irrelevant data?
- Do you keep paper records? Data protection law can apply to these documents as well as computer records.
- If you lost data or committed some other significant breach of the data protection laws, how would you minimise the damage? Should you notify the individuals concerned that the confidentiality of their details has been put at risk? Should you notify the regulatory authorities? Do you have contingency plans in place?

How we can help

We are always happy to discuss any data protection questions with you. We won't charge you for straightforward queries and if we think there isn't a problem, we'll tell you. We also have substantial experience of carrying out thorough data protection "health checks" to identify potential problems and of assisting in compiling data protection policies and handbooks. We have recently advised:

The pension fund trustees of a major UK plc

on a thorough data protection compliance review, with particular emphasis on intra-group data transfers, subject access requests, overseas transfers and system security.

A well-known UK financial services group

in relation to widespread subject access requests being made on behalf of customers by a consumer credit compensation scheme.

A major UK group active in the leisure sector

in relation to its data protection policies and procedures, with particular reference to direct marketing.

"Clients say Travers Smith's Dan Reavill is 'tactically astute with a tremendous eye for detail'."

Chambers Guide to the UK Legal Profession

"A good straight-talking team" [that] "doesn't over-lawyer things."

Chambers Guide to the UK Legal Profession

"Travers Smith is able to present clients with consistent teams of uniformly excellent lawyers."

The Legal 500

Travers Smith LLP
10 Snow Hill
London EC1A 2AL
T +44 (0)20 7295 3000
F +44 (0)20 7295 3500

www.traverssmith.com

The Data Protection Team

Dan Reavill
dan.reavill@traverssmith.com
+44 (0)20 7295 3260

Alistair Wilson
alistair.wilson@traverssmith.com
+44 (0)20 7295 3345