RadcliffesLeBrasseur

BRIEFING

Number 9

Data Protection: Employee Records

CARE HOMES BRIEFING

Our Care Homes Briefing Number 3 discussed some of the requirements of the Data Protection Act 1998 (the "Act"), particularly in relation to patient and health records. This briefing now deals with the rules governing employee records and the processing of personal data about employees. Breach of these rules can result in criminal penalties, so it is essential that your systems comply with the law.

Under the Act, "personal data" means information about individuals ("data subjects") who are either named or identifiable from the data, and it can include expressions of opinion and visual data such as photographs. "Processing" of personal data encompasses virtually every activity carried out with data, including storing, sorting and analysing it. The only significant exception is manual records made before October 1998, which are exempted from certain provisions of the Act until October 2007.

The following points should be borne in mind when dealing with personal data in the course of recruiting and managing employees.

Vetting applicants

There are various types of job for which vetting is appropriate, such as those involving children or vulnerable adults. The applicant must be informed that vetting is being done and must be given an opportunity to make representations about any adverse findings, particularly if the vetting involves not only checking official records - such as the Department of Health register for the protection of children - but also discussing the applicant with third parties.

Verifying job applications

Employers must tell applicants if they propose to verify the statements in their job applications, and how they propose to do it. If any discrepancies are thrown up, the applicant must be given an opportunity to make representations.

Retaining recruitment records

There are no fixed guidelines in the Act on this, so you must decide what is necessary. The information should be kept for, say, six months in case there is any come-back following the recruitment process, for example from an unsuccessful candidate. You also need to consider what information needs to be transferred to the personnel file of the successful applicant or applicants. Interview notes and internal memoranda about applicants and the recruitment process need to be dealt with in the same way as the application forms themselves. If you wish to retain the application to enable you to consider the applicant for future vacant posts, he or she should be told this and given the opportunity to request that you do not retain their application.

RadcliffesLeBrasseur
5 Great College Street
Westminster
London SW1P 3SJ

Tel +44 (0)20 7222 7040
Fax +44 (0)20 7222 6208
LDE 113

6-7 Park Place
Leeds LS1 2RU

Tel +44 (0)113 234 1220
Fax +44 (0)113 234 1573
DX 14086 Leeds Park Square

25 Park Place
Cardiff CF10 3BA

Tel +44 (0)29 2034 3035
Fax +44 (0)29 2034 3045
DX 33063 Cardiff 1

info@rlb-law.com
www.rlb-law.com

Racial or ethnic origin

Obtaining and storing information about racial or ethnic origin is permitted so long as it is necessary for monitoring purposes, or the employee has specifically consented to it. The information should be retained on an anonymous basis.

Disability

Information on an applicant's disability is clearly sensitive personal data but employers can often justify obtaining and keeping such data – it is good practice to ask whether an applicant needs any special facilities to enable him or her or attend the interview, and you need to know about employees' disabilities to be able to ensure their health and safety at work.

Criminal records

If necessary, employers can seek information on applicants' criminal records. The Criminal Records Bureau will disclose details of unspent convictions to the individual in question – not to the employer – but standard disclosure permits prospective employers to obtain information on spent convictions for prospective employees in categories of employment excluded by the Rehabilitation of Offenders Act 1974, such as working with vulnerable adults.

This information is obviously highly sensitive and you must ensure that it is kept secure and not shared with another employer or prospective employer. You should also keep records to a minimum – for example, retaining a note that a search was made and the results of that search, rather than detailed records. You may need to keep the information for, say, 6 months in case there is any come-back, for example from an unsuccessful applicant who alleges that they have been discriminate against in the recruitment process.

Monitoring of communications

It is now estimated that misuse of email and the internet is the single biggest ground for disciplinary action by employers. Monitoring email, internet access and telephone calls is permissible in certain cases, and the draft code under the Act (the "Code") describes monitoring as "a recognised component of the employer/worker relationship". The key for the employer is to comply with the statutory requirements and not go too far. You also need to consider the Regulation of Investigatory Powers Act 2000, which covers interception of communications, and the employee's service contract will also be relevant.

The Act and the regulations made under it prohibit the monitoring of communications without lawful authority. The regulations authorise monitoring which is limited to communications relating to the employer's business, but you must inform staff that you may intercept their communications. If the employer operates an email and internet policy which restricts employees' use of communications for personal purposes, the employer can monitor the communications to check whether the communications are relevant to the business, although the employer must decide if it really needs to access the content of the emails, rather than just checking the names of the recipients. The Act also allows recording of data to establish facts relevant to the business, for example, to ensure compliance with applicable regulations.

The consent of the data subject must normally be obtained before any processing of data. Even if the employee's contract incorporates a provision giving the employee's consent to monitoring, you should still assess the impact of the monitoring and ensure that it is as non-intrusive as possible. You are likely to obtain sensitive personal data through monitoring, so you need to ensure that you can satisfy one of the criteria in the Act concerning the processing of sensitive personal data.

Even assuming your impact assessment justifies your proposed monitoring, there are other considerations to bear in mind. For example, access to the information obtained in the course of

RadcliffesLeBrasseur
5 Great College Street
Westminster
London SW1P 3SJ

Tel +44 (0)20 7222 7040
Fax +44 (0)20 7222 6208
LDE 113

6-7 Park Place
Leeds LS1 2RU

Tel +44 (0)113 234 1220
Fax +44 (0)113 234 1573
DX 14086 Leeds Park Square

25 Park Place
Cardiff CF10 3BA

Tel +44 (0)29 2034 3035
Fax +44 (0)29 2034 3045
DX 33063 Cardiff 1

info@rlb-law.com
www.rlb-law.com

monitoring should be kept to an absolute minimum. The information should only be used for the purpose for which the monitoring itself was carried out, unless it is in the employee's best interest for you to use the information or if it contains something which an employer cannot be expected to ignore, such as fraudulent activity. Interestingly, the Code also says employers should take

account of the risk of unintentional access. Finally, don't forget to give your employee an opportunity to make representations about any adverse results of the monitoring before you reach any conclusions.

It is good practice to set up policies on the use of email and the internet, specifying what employees can and cannot do and what monitoring you will be doing, so your staff know what to expect.

Covert Monitoring

Employers must be extremely circumspect about using covert monitoring and should only do it if there are grounds for suspecting that criminal activity has taken place and that the investigation will be compromised if employees are told about the monitoring. The covert investigator must comply with the Act in relation to any data obtained, and the Regulation of Investigatory Powers Act 2000 may also apply. You should also limit covert monitoring to a specific timeframe and not retain any information which is not relevant to the purpose for which the monitoring is being done, unless it is of a kind that an employer could not be expected to ignore.

Disciplinary and grievance records

Data subjects have rights of access to documents relating to disciplinary and grievance procedures. If you are providing information to an employee's representative prior to disciplinary proceedings, for example, you should make sure that the employee has agreed to this. Where an allegation has not been substantiated, your records should be kept to a minimum, with essential information only. You should also set up a clear policy concerning records of spent warnings.

You may be able to justify providing this information in connection with legal proceedings. To protect yourself, one option would be to insist that someone obtains an order from the Employment Tribunal for the disclosure of the records so that you have no choice but to supply them and, even then, it would be advisable to omit sensitive data which is not relevant to the case.

Giving references

The duty of care owed by a referee to a prospective employer and a current or former employee puts him in a very difficult position, with the risk of claims from an employee complaining about a negative reference, or an employer who says it was too favourable. Difficulties over references have led many employers in the commercial sector to refuse to give references at all and to simply respond by confirming the employee's job description and period of employment.

The referee should only give a reference if the employee wishes him to do so and, when an employee leaves, should ask whether or not he should respond to future requests for a reference.

The employee does not have the right under the Act to obtain a copy of the reference from the referee, but he can obtain it from the new employer. In addition, if the employee were to take proceedings against the referee, he could obtain a copy of it in the course of the litigation.

Consequences of breach

If a breach of the Act results in damage to a data subject, he or she has a right to compensation unless the data controller can prove that it took reasonable care to comply with the relevant requirement. The data subject may also claim compensation for any distress suffered. The Information Commissioner has powers of enforcement under the Act, ultimately backed by criminal sanctions – for example, where a

RadcliffesLeBrasseur
5 Great College Street
Westminster
London SW1P 3SJ

Tel +44 (0)20 7222 7040
Fax +44 (0)20 7222 6208
LDE 113

6-7 Park Place
Leeds LS1 2RU

Tel +44 (0)113 234 1220
Fax +44 (0)113 234 1573
DX 14086 Leeds Park Square

25 Park Place
Cardiff CF10 3BA

Tel +44 (0)29 2034 3035
Fax +44 (0)29 2034 3045
DX 33063 Cardiff 1

info@rlb-law.com
www.rlb-law.com

data controller ignores the requirements of the Information Commissioner. Directors or other officers of the data controller may also be prosecuted – for example where a failure to notify the data subject or an unlawful sale of data is due to their personal negligence.

Conclusion

The above is only a summary of the rules on data processing. The law in this area is complex and detailed and readers are advised to take specific advice before acting in reliance on the matters set out in this briefing.

November 2003

FUTURE TOPICS FOR OUR CARE HOMES BRIEFINGS

If there are specific topics you would like us to address in our future Care Homes Briefings, please let us know by sending an email to andrew.parsons@rlb-law.com

For more information on Care Home Law contact Andrew Parsons at RadcliffesLeBrasseur on 020 7227 7282, or email: andrew.parsons@rlb-law.com.

Out of office emergency advice available 24hrs on 07802 506 306.

Readers are advised to take specific advice before acting in reliance on the matters set out in this briefing.
Future editions can be received by email. Please e-mail: marketing@rlb-law.com or telephone 020 7227 7388.

RadcliffesLeBrasseur
5 Great College Street
Westminster
London SW1P 3SJ

Tel +44 (0)20 7222 7040
Fax +44 (0)20 7222 6208
LDE 113

6-7 Park Place
Leeds LS1 2RU

Tel +44 (0)113 234 1220
Fax +44 (0)113 234 1573
DX 14086 Leeds Park Square

25 Park Place
Cardiff CF10 3BA

Tel +44 (0)29 2034 3035
Fax +44 (0)29 2034 3045
DX 33063 Cardiff 1

info@rlb-law.com
www.rlb-law.com