Employee background checks — how far is too far?

Davinia Brennan, Associate in the Litigation and Dispute Resolution department at A&L Goodbody, discusses the extent to which employers can legitimately ascertain prospective employees suitability for job roles using pre employment background checks

Pre-employment background checks on employees are becoming increasingly common. Employers should be cautious when conducting such checks, particularly as it is now an offence — as a result of the recent commencement of section 4(13) of the Data Protection Acts 1988 and 2003 ('DPAs') on 18th July 2014 — to compel a potential employee to make an access request, such as to the Garda, and reveal the response. Employers who fail to comply with the DPAs may be subject to a fine of up to €100,000.

This article considers the methods available to employers to screen prospective employees in compliance with the DPAs.

Data protection issues

Conducting background checks on prospective employees often involves liaising with third parties, such as private investigators or previous employers. In doing so, employers are processing applicants' 'personal data' and in many instances their 'sensitive personal data' (such as criminal convictions and medical data), for the purposes of the DPAs.

Transparency

The Data Protection Commissioner ('DPC') has highlighted that the key to compliance with the DPAs is for employers to be transparent when conducting background checks. This means employers should inform applicants as early as possible in the recruitment process of any potential checks that might be undertaken and how they will be conducted, and seek specific consent to same (see 'FAQs: Data Protection in the Workplace', copy available via www.pdp.ie/docs/10059).

In practice, employers might inform and obtain consent from applicants to verification and/or vetting on job application forms or other recruitment material. However, as there is doubt as to whether consent can be freely given in the context of the employer/employee relationship, an employer should ensure that the vetting is necessary to protect the employer from an identified legitimate business risk.

Verification versus vetting

The Information Commissioner's Office ('ICO') in the UK has issued 'The Employment Practices Code' ('the Code', copy available at: www.pdp.ie/docs/10060) which contains some helpful guidance on pre-employment verification and vetting.

The Code suggests that employers should, where practicable, obtain relevant information directly from the applicant and, if necessary, verify it rather than undertake pre-employment vetting. Verification covers the process of checking that details supplied by applicants (for example, qualifications) are accurate and complete, whilst vetting occurs where the employer actively makes its own enquiries from third parties about an applicant's background and circumstances. The Code states that, as vetting is particularly intrusive, it should be confined to areas of special risk.

Blanket vetting

The Code warns against blanket vetting of all prospective employees, or even shortlisted applicants, suggesting instead that vetting should only occur:

- in respect of people actually selected for the job;
- where there are particular and significant risks involved to the employer or customers or others; and
- where there is no less intrusive and reasonably practicable alternative.

Communicating background check results

The Code also recommends that when an employer finds something on a background check that might affect its decision to recruit an employee, it should inform the employee of same, and take into account their response when making the recruitment decision.

Types of background checks

Employers carry out a broad range of pre-employment checks on prospective employees during the recruitment process in an effort to verify the accuracy of their job application forms or CVs, and to gather as much relevant information as possible about an applicant before hiring them. Types of background checks conducted by employers include:

- verifying qualifications with educational establishments;
- checking medical history;
- requesting references from previous employers;
- checking for any criminal convictions;
- checking creditworthiness; and
- checking social media profiles.

These are considered in more detail below.

1. Garda vetting of employees working with children and vulnerable adults

There is no comprehensive legislation in Ireland governing the vetting of prospective employees, other than in relation to working with children or vulnerable adults. The DPC has issued a guidance note on 'Data protection considerations when vetting prospective employees' (copy available at: www.pdp.ie/docs/10061) which considers the procedure in relation to Garda vetting of persons working with children and vulnerable persons.

"Employers should be cautious about how they conduct social media searches. To avoid risk of any legal challenge, applicants should be notified in advance that their social media profiles may be screened, and be given a chance to respond if some aspect of their social media profile has negatively influenced their application. Such searches should be targeted on finding information relevant to the hiring decision, rather than a fishing expedition."

The GCVU: The Garda Central Vetting Unit ('GCVU') currently conducts vetting on a non-statutory basis, for organisations that are registered with it for that purpose.

The GCVU only conducts vetting in relation to persons in contact with children or vulnerable adults, State employees, and employees covered by the Private Security Services Act 2004 (such as doormen and women and night-club security staff).

In order for vetting to take place, data subjects must complete a Garda Vetting Application Form, providing their written consent for the GCVU to disclose to the authorised liaison person in the registered organisation, details of all prosecutions, successful or not, pending or completed and/or details of all convictions, recorded in the State or elsewhere.

Since 31st March 2014, an 'Administrative Filter' has been applied to all Garda vetting applications, which allows certain minor convictions over seven years old to be removed from disclosures.

The DPC does not deem it appropriate for vetting information disclosed by the GCVU to one named organisation to be shared subsequently with any other organisation, even with consent, except where the registered organisation is clearly undertaking the vetting on behalf of a related organisation. However, individuals that have been vetted by the Garda have a statutory right to a copy of their vetting information from the registered organisation, under section 4 of the DPAs.

The National Vetting Bureau: The National Vetting Bureau (Children and Vulnerable Persons) Act 2012 ('the 2012 Act') will make Garda vetting of individuals seeking positions of employment relating to children or vulnerable persons mandatory for the first time. Once enacted, the National Vetting Bureau will replace the GCVU.

The 2012 Act was passed by both Houses of the Oireachtas in December 2012. However, the Act's commencement has been delayed due to the UK's Supreme Court decision in *R (On the application of T and another) v Secretary of State for Home Department and another* [2014] UKSC 35 (18th June 2014). In that case, the Court held that the UK government rules requiring blanket disclosure of spent convictions (i.e. minor past convictions) were unlawful and incompatible with the right to respect for private life under Article 8 of the European Convention of Human rights.

The Irish government has indicated that the 2012 Act will be amended as a result of this decision, so as to provide that there will be no obligation to disclose certain minor past convictions. It is expected that the 2012 Act will be amended via the Criminal Justice (Spent Convictions) Bill 2012, which is currently before the Oireachtas. This means that where a person is asked about his criminal record, the question will be treated as not extending to 'spent' convictions.

2. Criminal background checks in other sectors

An Garda Siochána will only carry out vetting for organisations registered with it in designated sectors. If an individual working in another sector wishes to obtain access to personal

(Continued on page 6)

(Continued from page 5)

data held about him/her by the Garda, then he/she may make an access request to the Garda under the DPAs. In this case, the Garda will issue the information directly to the person for his/her own personal use. However, the Garda has warned that any responses to such an access request are not of the standard applied to vetting applications and 'cannot be construed as Proof of No Convictions, a Police Certificate, or a Garda Reference'.

As mentioned above, it is now an offence in Ireland for employers to make enforced subject access requests. Accordingly, employers that require individuals to make access requests and disclose the results to them, risk being prosecuted.

The DPC has indicated that an employer is entitled to ask a prospective employee to declare if they have any previous criminal convictions which might impact on the desirability of them performing a particular task. However, an employer should only be concerned about convictions that relate to the particular job on offer. For example, a job involving cash-handling at a bank may justify the employer asking about previous convictions for theft. An employer should be able to show particular justification for any intrusive enquiry of potential employees.

In practice, employers might directly ask prospective employees if they have ever been convicted of a criminal offence on a character enquiry form that is separate to the main job application form. Alternatively, in order to avoid any accusations of discrimination, an employer might interview and consider all applicants equally, and then run a background check on selected applicants, at offer stage. Employment contracts might also provide for termination of employment if an employer discovers an employee has provided inaccurate or untruthful information in relation to any relevant previous convictions.

3. Education and employee references

Employers may want to verify an applicant's qualifications and experience with educational establishments and/or previous employers. Such third parties will need the applicant's authorisation before disclosing any personal information to the prospective employer. In practice, it may be easier for an employer to seek a prospective employee's written permission, and pass it on to the third party, rather than for the third party to seek permission directly. Employers should be aware that if they mislead a third party into giving them personal information about an applicant without authorisation, they may be committing an offence.

4. Medical History

Medical information constitutes 'sensitive personal data' under the DPAs and should therefore be obtained only with the data subject's explicit consent. However, as previously noted, employers should be wary of relying solely on consent to legitimise the processing of data. Employers may be justified in carrying out pre-employment medical checks on employees where health or fitness is a relevant factor for the job in question. In view of the sensitivity of such information, it would be sensible for employers not to seek it before the offer stage of the recruitment process.

5. Creditworthiness

Employers seeking to access information held by a credit referencing organisation about prospective employees could present data protection concerns. Individuals can seek access to their own credit history by making a request to the Irish Credit Bureau. But any requirement for potential employees to seek credit history information from the Irish Credit Bureau, and reveal same to employers, might constitute a forced access request, which, as discussed earlier, is an offence under the DPAs.

An employer may however carry out judgment and bankruptcy searches against a prospective employee, as such databases are accessible by the general public. The DPC has indicated that any information that is already in the public domain can be accessed without giving rise to any data protection concerns. However, the data subject should be provided with a copy of any such information so that they can provide comments on it.

6. Social media checks

Employers are increasingly using social media networks such as Facebook, Twitter, and LinkedIn to screen prospective employees. Employers should be cautious about how they conduct social media searches. To avoid risk of any legal challenge, applicants should be notified in advance that their social media profiles may be screened, and be given a chance to respond if some aspect of their social media profile has negatively influenced their application. Such searches should be targeted on finding information relevant to the hiring decision, rather than a fishing expedition.

The UK's ICO has warned employers that it would have 'very serious concerns' if they were to ask for Facebook login and password details from prospective employees, following reports of such demands in the US. In Ireland, requiring such information would most likely constitute a breach of the DPAs, as it would mean employers would be processing excessive personal information about applicants.

Facebook has also warned employers not to ask job applicants for their passwords to the site so they can poke around on their profiles, noting that it would break its terms of service.

Hiring private investigators

If engaging private investigators to carry out background checks, then the DPAs require the employer to enter into a processing contract with the investigators. The employer should ensure applicants are informed that background checks will be carried out by such third party private investigators, and that the private investigators comply with the DPAs when gath-

ering personal data about applicants. The District Court recently prosecuted an Irish private investigation firm, MCK Investigations, and two of its directors €10,500 for unlawfully obtaining personal data. It found that the directors had used 'subterfuge' to unlawfully obtain the addresses of credit union clients in arrears. The directors posed as a VEC, and hospital worker, to obtain the information, via telephone calls, from employees at the Department of Social Protection, and the Health Services Authority. These were the first prosecutions taken by the DPC against private investigators, and the first occasion where company directors were prosecuted as well as the company itself.

The DPC stated that the prosecutions send 'serve to remind all companies and businesses who hire private investigators or tracing agents that they have onerous responsibilities under the Data Protection Acts to ensure that all tracing or other work carried out on their behalf by private investigators or tracing agents is done lawfully'.

Compliance 'hot tips'

What follows are some steps that organisations can take to avoid falling short of the compliance requirements discussed above:

- Do not carry out any background checks unless you have clearly informed the applicant that you will be doing so.
- Ensure that all background checks are necessary, proportionate, fair and not excessive in light of the role in question.
- Ensure that any professional agency used to process background checks on your behalf conducts its business in compliance with the DPAs.
- Do not carry out background checks before offer stage of recruitment process.
- Do not force applicants to use their subject access rights to request records from another organisation (for example, the Garda or Irish Credit Bureau).

Conclusion

It is important for employers to take great care in conducting background checks, and ensure they do not flout data protection laws when doing so.

Verification and vetting is permissible, so long as prospective employees are notified in advance, and the information sought is necessary, proportionate and fair having regard to the legitimate business risk the employer seeks to protect itself against.

Davinia Brennan
A&L Goodbody
dbrennan@algoodbody.com