MAYER·BROWN

The Use of Social Media in the Workplace

Introduction

There has been an explosion in the popularity of social media sites such as Facebook, MySpace, Twitter, Bebo and LinkedIn in recent years. Their popularity has transcended languages, borders and cultures, and it is probably no exaggeration to say that we are witnessing a social media revolution. Facebook alone currently has over 500 million users, equating to roughly 1 in every 13 people on this planet. It is estimated that over 50 per cent of these users log on to Facebook every day. By anyone's standards, these are staggering figures and yet they relate only to one social media site. It is therefore no surprise that social media is beginning to permeate almost every aspect of our lives, whether it be on a personal, social or professional level.

Many businesses have been adept at harnessing the power of social media to their advantage. Others have been less so, but they are catching on. However, it is never plain sailing in the world of social media. As well as the benefits, social media throws up some huge challenges and real problems. It is now clear that employers and employees both need to consider how social media sites may affect employment.

Many employers have been quick to use social media to recruit staff. Others have been adept at allowing employees to use social media in the workplace to develop business and commercial relationships. Some employers have simply been keen to use social media as a better way of engaging with its staff and fostering a more collegiate environment. But many will be all too familiar with the news stories of employees misusing social media at or outside of work to the disadvantage of their employer. Some stories have featured employees who have been dismissed after posting inappropriate comments about colleagues or their employer. Quite often, the legal issues that lie beneath these stories are overlooked. For example, is it lawful to vet job applicants using social media sites? What legal risks arise when permitting employees to use social media at work? How can an employer manage the risks that arise?

It is with these legal issues in mind that we have put together this publication, which covers 44 different jurisdictions in EMEA, Asia and the Americas. For each of the jurisdictions covered, we asked the following questions:

1. **Are there any risks for employers that use social media sites to vet job applicants?**
2. **What steps can be taken by employers to minimise such risks?**
3. **What problems could an employer face as a result of employees using social media sites?**
4. **What steps can be taken by an employer to minimise the risks associated with employees using social media sites?**

We have set out the answers to each of these questions in two different formats. Section 1 contains an Executive Summary of each jurisdiction's response. This is intended to be a short – "at a glance" – overview of the position. Section 2 contains the more substantive answers to the questions.

What we have discovered from all of the jurisdictions is that, although the risks that arise from the use of social media sometimes vary, the solutions that have been recommended to manage these risks are more or less the same. In most jurisdictions, it is recommended that social media policies be put in place, appropriate training be provided to employees and appropriate confidentiality clauses and post-termination restrictive covenants be incorporated into contracts of employment. It is also good news for employers that, in most jurisdictions, disciplinary action can be taken where there has been a misuse of social media. All of this will provide some comfort to global businesses that strive to have common standards and harmonise the approach that it takes towards its employees.

We do hope that you find this publication useful. It has been made possible with the input from lawyers in leading law firms in each of the jurisdictions. Not all of these law firms are part of Mayer Brown, but all of them have worked closely with us over the years. Should you wish to contact the lawyers in any of the jurisdictions, their contact details are set out in the last section of this publication.

Duncan Abate
Debra Hoffman
Nicholas Robertson
Anna Rogers
Guido Zeppenfeld

Firm Practice Leaders
Employment and Benefits Group
Mayer Brown

Asia

AUSTRALIA

1. *Are there any risks for employers that use social media sites to vet job applicants?*

   Employers who use social media sites in this way run the risk of infringing Australian laws that relate to discrimination and data protection.

2. *What steps can be taken by employers to minimise such risks?*

   - Inform recruitment and other relevant personnel of the requirements and prohibitions contained in the relevant legislation.
   - Update recruitment policies and procedures to prohibit actions that are unlawful.
   - Run training sessions for recruitment and other relevant personnel to ensure that they are aware and reminded on an ongoing basis of the employer's legal obligations.
   - Ensure that adequate systems are in place to protect the personal information of job applicants once it has been collected.
   - Draft a Privacy Policy that applies to all staff and covers all relevant principles.

3. *What problems could an employer face as a result of employees using social media sites?*

   Aside from the obvious risk of a loss of productivity within the workforce, the conduct of employees on social media sites could leave employers open to claims of unlawful discrimination or harassment or claims in relation to 'cyber-bullying'.

   Employees' posts could also breach confidentiality, cause damage to the reputation of the employer (or a third party) or contain defamatory material.

AUSTRALIA

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

- Ban the use of social media.
- Introduce or update a social media policy.
- Provide training.
- Introduce contractual provisions governing the use of social media.

Contributed by Corrs Chambers Westgarth

HONG KONG

1. *Are there any risks for employers that use social media sites to vet job applicants?*

   Yes. Employers face potential data protection-related risks arising from the Personal Data (Privacy) Ordinance. An employer could also run the risk of facing claims for unlawful discrimination if it rejects an application on the basis of information it has obtained from a social media site that relates to one or more protected characteristics of the applicant.

2. *What steps can be taken by employers to minimise such risks?*

   - Inform applicants at the start of the recruitment process that vetting of social media sites will form part of the process.
   - Provide applicants with a personal data collection statement.
   - Provide training to employees who have responsibility for vetting social media sites.
   - Put in place a social media policy.
   - The person scanning social media sites should not be the same person who makes the hiring decision.
   - Put in place an anti-discrimination policy.

3. *What problems could an employer face as a result of employees using social media sites?*

   An employee could post information on a social media site that breaches their obligations of confidentiality to their employer and damages the reputation of their employer. An employer could also be held liable for any postings by employees that constitute unlawful discrimination or harassment against other employees. The use of social media sites could also result in a loss of productivity within the workforce.

HONG KONG

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

- Ban the use of social media sites at work or during work hours.
- Provide training to employees on the pitfalls of using social media sites.
- Put in place a social media policy.
- Consider whether the use of social media sites could and should be monitored.
- Incorporate appropriate confidentiality clauses and post termination restrictive covenants in employment contracts.
- Take disciplinary action against employees who misuse social media sites.

Contributed by Mayer Brown JSM

INDIA

1. *Are there any risks for employers that use social media sites to vet job applicants?*

   Yes. Only a state-owned entity would run the risk of facing claims for unlawful discrimination if it rejects an application on the basis of information it has obtained from a social media site that relates to one or more protected characteristics of the applicant. In relation to employers in both the private and public sectors, there exist risks in relation to a breach of privacy.

2. *What steps can be taken by employers to minimise such risks?*

   - Try to seek the consent of applicants before using social media sites to vet their applications.
   - Adopt a consistent method for screening applicants.
   - Take steps to verify any information obtained from social media sites.
   - Keep records of any information that is reviewed and relied upon.
   - Implement an anti-discrimination policy.
   - Provide training to its recruiters.

3. *What problems could an employer face as a result of employees using social media sites?*

   An employee could post information on a social media site that breaches their obligations of confidentiality to their employer. An employee could also post information that damages their employer's reputation. Social media sites could be used by a former employee as a medium to solicit employees of the employer. A state-owned employer could also be held liable for any postings by employees that constitute unlawful discrimination or harassment against other employees. The use of social media sites could also result in a loss of productivity within the workforce.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

- Block access to social media sites.
- Put in place a social networking policy.
- Provide training to employees on the pitfalls of using social media.
- Incorporate within employment contracts confidentiality clauses and non-solicitation covenants.

Contributed by Trilegal

INDONESIA

1. *Are there any risks for employers that use social media sites to vet job applicants?*

   Employers could face discrimination claims if they use information such as an applicant's sex, marital status or race to vet that applicant.

2. *What steps can be taken by employers to minimise such risks?*

   - The employer should publish the job requirements in a public advertisement in order to notify all job applicants of the company's needs on a transparent basis.
   - If there is a job that requires a specific ethnicity, gender or religion, the employer should explain the business reasons for such requirements to the job applicants.
   - The company could issue a policy indicating that social media websites are a possible source of information in determining both the qualifications of job applicants and compliance with company policies by existing employees.

3. *What problems could an employer face as a result of employees using social media sites?*

   Employees could, deliberately or accidentally, post confidential information on such sites. Posts could also include content that causes damage to the reputation of the employer and/or a third party.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

   - The employer could prohibit access to social media websites at work or during working hours.
   - Alternatively, the employer could draw up guidelines regarding the use of social media.

INDONESIA

- Employers should stipulate a confidentiality clause in both the Employment Contract as well as in the Company Regulation.
- Finally, they should make clear guidelines for possible disciplinary action against employees who misuse social media websites.

Contributed by Soewito Suhardiman Eddymurthy Kardono

JAPAN

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Employers could infringe Japanese law relating to the collection and use of individuals' personal information.

2. *What steps can be taken by employers to minimise such risks?*

- Applicants should be told at the start of the recruitment process that the employer will conduct a vetting exercise using information from social media sites.
- Employers should provide, and comply with, a personal data collection statement.
- Guidelines and training should be provided.
- A social media policy should be implemented.
- The person scanning the social media sites should not be the same as the person making recruitment decisions.

3. *What problems could an employer face as a result of employees using social media sites?*

As well as the obvious risk of a loss of productivity within the workforce, the content of employees' posts could breach obligations of confidentiality, cause damage to the reputation of the employer (and/or third parties) or lead to claims against the employer for harassment. In addition, employees could use work contacts built up on social media sites to solicit clients away from the employer once their employment has ended.

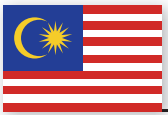
4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

- Impose an outright ban on the use of social media sites at work.
- Put in place a social media policy.

JAPAN

- Provide awareness training to employees around issues such as discrimination, harassment and bullying.
- Monitor the use of social media sites by employees.
- Incorporate appropriate confidentiality clauses and post-termination restrictive covenants within employment contracts.
- Take disciplinary action against employees who misuse social media sites.

Contributed by Anderson Mori & Tomotsune



MALAYSIA

1. *Are there any risks for employers that use social media sites to vet job applicants?*

When the relevant legislation (Personal Data Protection Act 2010) comes into force, employers who use social media sites in this way run the risk of infringing Malaysian law relating to the protection of personal data.

2. *What steps can be taken by employers to minimise such risks?*

- Employers should familiarise themselves with the requirements of the Personal Data Protection Act 2010 to ensure compliance when it comes into force.
- Guidelines should be put in place for employees who collect and use personal data as part of the recruitment process.

3. *What problems could an employer face as a result of employees using social media sites?*

Aside from the obvious risk of a loss of productivity within the workforce, employees' posts could also breach confidentiality and cause damage to the reputation of the employer or a third party.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

- Impose a ban or restriction on the usage of social media websites during office hours.
- Have in place guidelines that deal with the use of social media websites during and outside office hours.
- Monitor the use of social media sites by employees.

MALAYSIA

- Include confidentiality clauses in employment contracts to cover instances where confidential information is submitted on social media sites.

Contributed by Shearn Delamore

NEW ZEALAND

1. *Are there any risks for employers that use social media sites to vet job applicants?*

   Yes. Employers risk unlawfully discriminating against an applicant if they use information related to a protected characteristic, which they have taken from a social media site, as the basis for refusing employment. There are also privacy issues to consider.

2. *What steps can be taken by employers to minimise such risks?*

   - Update privacy and discrimination policies.
   - Advise applicants that social media sites are reviewed as part of the recruitment process.
   - Only extract legitimate and relevant information. A social media policy should set out guidelines to this effect.
   - Social media checks should be performed consistently.
   - The person scanning the social media site should not be the same as the person determining the outcome of the recruitment process.
   - Be aware that the information may not be reliable.

3. *What problems could an employer face as a result of employees using social media sites?*

   Employees using social media sites could breach confidentiality and cause damage to the employer's or a third party's reputation. Employers could also face a loss of productivity across the work force and have to deal with work-place bullying.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

   - Ban access to social media sites at work.

NEW ZEALAND

- Produce a social media policy, setting out the rules and standards expected, including the consequences of any breach.
- Provide employees with training.
- Include a confidentiality clause in employment contracts.
- Incorporate appropriate restraint of trade clauses into employment contracts.
- Take disciplinary action.

Contributed by Simpson Grierson

PAKISTAN

1. *Are there any risks for employers that use social media sites to vet job applicants?*

   The risks involved are extremely low.

2. *What steps can be taken by employers to minimise such risks?*

   As the risks are very low, there are no steps which must be taken. However, employers may wish to take some of the following steps as best practice:

   - The information which an employer takes from a social media site must be publicly available.
   - Only relevant information should be extracted.
   - A social media policy should be produced.
   - Advise applicants that social media sites are reviewed.
   - The applicant should confirm the content of any relevant information extracted.

3. *What problems could an employer face as a result of employees using social media sites?*

   Employees using social media sites could breach confidentiality and cause damage to the employer's or a third party's reputation.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

   - Ban access to social media sites at work.
   - Produce a social media policy, setting out the rules and standards expected, and the consequences of any breach.
   - Provide employees with training.
   - Include a confidentiality clause in employment contracts.

Contributed by Meer & Hasan

PEOPLE'S REPUBLIC OF CHINA

1. *Are there any risks for employers that use social media sites to vet job applicants?*

   Yes. Employers risk unlawfully discriminating against an applicant if they refuse to employ them based on information related to a protected characteristic, which they have taken from a social media site. There may also be issues with the applicant's right to privacy.

2. *What steps can be taken by employers to minimise such risks?*

   - Inform applicants that social media sites are reviewed as part of the vetting process.
   - Inform applicants as to how their personal data will be collected, used and handled.
   - Provide training to employees vetting job applicants in this way, and put in place an anti-discrimination policy.
   - Only extract legitimate and relevant information. A social media policy should set out guidelines to this effect.
   - The person scanning social media sites should not be the same as the person determining the outcome of the recruitment process.

3. *What problems could an employer face as a result of employees using social media sites?*

   Employees using social media sites could breach confidentiality and cause damage to the employer's or a third party's reputation. Employers could face a loss of productivity across the work force and, in some circumstances, be liable for discriminatory comments made by its employees.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

- Ban access to social media sites at work.
- Produce a social media policy, setting out the rules and standards expected, including the consequences of any breach.
- Provide employees with training.
- Monitor use of social media sites.
- Include a confidentiality clause in employment contracts.
- Consider whether the post-termination restrictive covenants prevent ex-employees from using a client list built up through a networking site.
- Take disciplinary action if appropriate.

Contributed by JSM Shanghai Representative Office

PHILIPPINES

1. *Are there any risks for employers that use social media sites to vet job applicants?*

   Employers may infringe Phillipine law relating to discrimination, data protection and privacy.

2. *What steps can be taken by employers to minimise such risks?*

   - Seek the applicant's individual written consent for the collection, storage, maintenance, transfer, processing, handling and use of personal information by the employer.
   - Disclose to the applicant that the employer will conduct a vetting exercise using information available on social media sites.
   - The employer should provide guidelines and training to employees responsible for vetting applicants to ensure that only information that is relevant and necessary for the recruitment process is retrieved.
   - Access to applicants' personal information files must be limited to authorised officers and agents of the company who are under strict confidentiality obligations to ensure the protection of the applicants' privacy rights, and that information is used only for legitimate business and other lawful purposes.

3. *What problems could an employer face as a result of employees using social media sites?*

   Aside from the obvious loss of productivity in the workforce, if, during the course of their employment, an employee posts comments on a social media site which causes harm to others, for example, by posting hostile or defamatory statements or by revealing confidential information, then the employer could be liable for any damage caused. Employers could also suffer significant reputational damage as a result of employee's activities.

PHILIPPINES

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

- Impose an outright ban on access to social media sites at work.
- Develop a policy regarding the use of social media sites during work hours.
- Provide training to employees on their obligations.
- Monitor the employees' activities in regard to their use of social media sites.
- Incorporate an appropriate confidentiality clause into contracts of employment.

Contributed by SyCip Salazar Hernadez & Gatmaitan

SINGAPORE

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Employers who use social media sites in this way run the risk of infringing Singaporean law relating to discrimination and data protection.

2. *What steps can be taken by employers to minimise such risks?*

- Employers should only use information that is publicly available.
- A Social Media Policy should be introduced, setting out guidelines for employees who collect information on applicants.
- It is recommended that the person collecting and extracting the information and the decision maker be different individuals.
- Applicants should ideally be notified that any publicly available information about them may be used by the employer in making a decision about whether to employ them.
- Employers should remain abreast of legal developments to ensure that their practices remain compliant with the changing regulatory landscape.

3. *What problems could an employer face as a result of employees using social media sites?*

Employers could be vicariously liable if the conduct of their employees on social media sites causes damage to fellow employees or third parties. In addition, employees who access external sites could expose the employer's computer system to malicious software.

Finally, there is the inevitable risk of a loss of productivity within the workforce.

SINGAPORE

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

- Impose an outright ban.
- Implement a Social Media Policy governing employees' use of Social Media Sites.
- Provide training.

Contributed by Rajah & Tann

SOUTH KOREA

1. *Are there any risks for employers that use social media sites to vet job applicants?*

The risks are not significant, assuming employers comply with relevant anti-discrimination laws. There are general laws that protect the personal data privacy of individuals, but the mere use of information that is already provided on social media sites to vet job applicants does not raise any significant risks to employers.

2. *What steps can be taken by employers to minimise such risks?*

To the extent that an applicant may reasonably argue that his/her personal data privacy right has been violated, the following steps can be taken to minimise any such risk:

- Applicants should be provided with a personal data collection statement.
- Provide training to employees who have responsibility for recruitment.
- Put in place a social media policy.
- The person scanning social media sites should not be the same as the person who makes the hiring decision.
- Put in place an anti-discrimination policy.

3. *What problems could an employer face as a result of employees using social media sites?*

An employer could be faced with cases where employees have posted information on social media sites that is in breach of confidentiality and damages the employer's reputation. Former employees could also use networking sites such as LinkedIn to solicit former clients and employees. Employees could also use social media sites to engage in conduct towards other employees that constitutes unlawful discrimination and/or harassment. Social media sites could also result in a loss of productivity within the workforce.

SOUTH KOREA

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

- Impose an outright ban on the use of social media in the workplace.
- Put in place a social media policy.
- Provide training to employees on the problems associated with using social media sites.
- Consider whether social media sites at work could and should be monitored.
- Incorporate confidentiality clauses and restrictive covenants within employment contracts.
- Take disciplinary action against employees who misuse social media sites.

Contributed by Kim & Chang

SRI LANKA

1. *Are there any risks for employers that use social media sites to vet job applicants?*

   Potentially, employers risk unlawfully discriminating against an applicant if they use information about a person's caste (i.e. social status in society), taken from a social media site, as the basis for refusing employment.

2. *What steps can be taken by employers to minimise such risks?*

   Avoid any discriminatory conduct and have in place clear guidelines as to what type of information can be gathered.

3. *What problems could an employer face as a result of employees using social media sites?*

   - Reputational damage.
   - Risk that confidential information will be disclosed.
   - Ex-employees continuing to access client lists through social media sites.
   - Loss of productivity.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

   - Ban access to social media sites at work.
   - Produce a social media policy, setting out the rules and standards expected, and the consequences of any breach.
   - Provide employees with training.
   - Monitor use of social media sites.
   - Include a confidentiality clause in employment contracts.

Contributed by John Wilson Partners

TAIWAN

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Employers who use social media sites in this way run the risk of infringing Taiwanese law relating to discrimination and data protection.

2. *What steps can be taken by employers to minimise such risks?*

- Job applicants should be informed in advance that Cyber Vetting will be carried out, and their prior written consent to this should be obtained.
- Only information that is relevant to the job applicant's suitability for the role they have applied for should be collected and used.
- The recruitment process should be carefully documented.
- Applicants should be provided with feedback regarding the recruitment process, setting out why their application has been accepted or rejected. This could minimise the risk of a claim for unlawful discrimination.
- The recruitment team should receive training on the employer's anti-discrimination policy, and how to carry out the recruitment process in a non-discriminatory way.
- Job applicants should be provided with the opportunity to correct personal data collected from social media sites to ensure accuracy.

3. *What problems could an employer face as a result of employees using social media sites?*

Aside from the obvious risk of a loss of productivity within the workforce, the conduct of employees on social media sites could leave employers open to claims for harassment.

Employees' posts could also breach confidentiality, cause damage to the reputation of the employer (or a third party), contain defamatory material or infringe third parties' intellectual property rights.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

Employers should develop a practical and enforceable social media policy dealing with the above issues.

Contributed by Lee, Tsai & Partners

THAILAND

1. *Are there any risks for employers that use social media sites to vet job applicants?*

   Employers who use social media sites in this way run the risk of infringing Thai law relating to discrimination, data protection and privacy. However, these risks are currently extremely small.

2. *What steps can be taken by employers to minimise such risks?*

   Not applicable. However, when the Personal Data Protection Bill becomes law, this issue may need to be revisited. This Bill has been under consideration for a number of years and, at the time of writing, no date has been set for it to come into force.

3. *What problems could an employer face as a result of employees using social media sites?*

   Aside from the obvious risk of a loss of productivity within the workforce, employees' posts could breach confidentiality, cause damage to the reputation of the employer (or a third party) or contain defamatory material. There is also the risk that bad feeling will be created within the workplace if employees behave negatively towards each other on such sites, although employers are unlikely to be found to be vicariously liable.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

   - Impose a total ban on access to such sites at work.
   - Amend Work Rules to provide clear standards of acceptable conduct.
   - Monitor employee usage of the employer's IT systems and equipment.

THAILAND

- Include contractual provisions in employment agreements that impose obligations of confidentiality on employees.

Contributed by Mayer Brown JSM (Thailand) Limited

VIETNAM

1. *Are there any risks for employers that use social media sites to vet job applicants?*

   Yes. Employers risk unlawfully discriminating against an applicant if they refuse to employ them based on information related to a protected characteristic, which they have taken from a social media site. There may also be data protection-related issues.

2. *What steps can be taken by employers to minimise such risks?*

   Written consent should be obtained before information is collected from social media sites.

3. *What problems could an employer face as a result of employees using social media sites?*

   Employees using social media sites could breach confidentiality and cause damage to the employer's or a third party's reputation. In some circumstances, employers can be liable for discriminatory comments made by one employee against another. The State could also impose sanctions on the employer if an employee accesses a prohibited site or makes derogatory comments against the State.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

   - Ban access to social media sites at work.
   - Produce a social media policy setting out the rules and standards expected.
   - Provide employees with training.
   - Use firewalls to prevent access to particular sites.
   - Include a confidentiality clause in employment contracts.

Contributed by Mayer Brown JSM (Vietnam)

AUSTRALIA

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Introduction

It is becoming more common in Australia for employers to use social media to increase their knowledge of job applicants. One recent survey found that over a third of employers in the accounting and finance sector consider applicants' Facebook profiles before offering them employment.[1]

However, whilst Facebook and other social media sites can be a useful recruitment tool, employers need to be aware of the associated risks. In particular, inappropriate use of social media may constitute unlawful discrimination or a breach of privacy law.

Unlawful discrimination and adverse action

When vetting job applicants, employers must ensure that they are not acting in breach of anti-discrimination legislation or the adverse action provisions of the *Fair Work Act 2009* (Cth) (**Fair Work Act**). Federal, state and territory anti-discrimination statutes prohibit discrimination against workers, including in relation to the offering of employment. The Fair Work Act prohibits adverse action being taken against prospective employees, in addition to employees. Generally, an employer will be liable for the actions of their workers unless certain actions are taken, which steps are discussed below.

[1] Legal Online Current Awareness, *FED: Bosses peek at Facebookers' privates*, 25 May 2010.

AUSTRALIA

(a) Unlawful discrimination

Australian anti-discrimination legislation prohibits discrimination on the basis of various grounds (**relevant attributes**). The prohibitions are contained in federal, state and territory statutes. Although definitions vary between jurisdictions, in all states and territories discrimination is prohibited on the basis of age; breast feeding; impairment/disability; marital or relationship status; parental status; status as a carer or family responsibilities; pregnancy; race; and sex. A number of jurisdictions have additional grounds, such as political belief or activity and sexual orientation that employers, where these additional attributes are relevant, should also be aware of and should consider.

Both direct and indirect discrimination are generally prohibited. Direct discrimination occurs when a person is treated less favourably because of a relevant attribute, or a characteristic that generally appertains or is imputed to a relevant attribute. Indirect discrimination happens when an unreasonable condition, requirement or practice is imposed, and this condition, requirement or practice has, or is likely to have, the effect of disadvantaging persons with a relevant attribute.

Many relevant attributes may be revealed when using social media to evaluate a potential worker. Employers must ensure that they do not reject an application on the basis of a relevant attribute, or treat a potential employee less favourably because of the relevant attribute, unless an exception applies.

(b) Adverse action

In addition to anti-discrimination laws, the Fair Work Act states that an employer must not take adverse action against an employee, or prospective employee, 'because of the person's race, colour, sex, sexual preference, age,

physical or mental disability, marital status, family or carer's responsibilities, pregnancy, religion, political opinion, national extraction or social origin'. Adverse action includes refusing to employ a prospective employee because of one of the attributes listed above. This means that employers must ensure that their use of social media to vet job applicants is not related to any relevant attributes.

Privacy laws

Although neither common law nor legislation provides an unequivocal and legally enforceable right to privacy, there are certain obligations imposed on employers relating to the collection, use and disclosure of personal information.

(a) The Privacy Act 1998 (Cth) (**Privacy Act**)

There is currently no common law tort of privacy in Australia. However, the Privacy Act contains two sets of principles, the Information Privacy Principles (**IPPs**), which apply to agencies, and the National Privacy Principles (**NPPs**), which apply to organisations.

Section 6C(1) of the Privacy Act defines 'organisation' to include an individual, body corporate, partnership, any other unincorporated association or a trust, with some exceptions (for example, small business operators). Therefore, many private entities will be bound by the NPPs.

Both the NPPs and IPPs contain various requirements relating to matters such as the collection, use, disclosure and security of personal information, even if the data is publicly available. For example, NPP 1 relates to the collection of information and says that an organisation must not collect personal information unless that information is 'necessary for one or more of its functions or activities'. The data must only be collected

by lawful and fair means, and the organisation must take reasonable steps to ensure that the individual is informed of certain factors, including the identity of the organisation and the purposes for which the information is collected. Personal information is defined in section 6 of the Privacy Act as:

> *information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion*

NPP 2 relates to use and disclosure of information and includes a requirement that organisations must not use or disclose personal information for a purpose other than the primary purpose of collection. This means that organisations must not collect information about a potential employee for the purposes of recruitment, and then use that information for another purpose, unless certain conditions are met.

Other requirements imposed on organisations include:

(i) taking reasonable steps to make sure that personal information collected, used or disclosed is 'accurate, complete and up-to-date' (NPP 3);

(ii) a responsibility to take reasonable steps to protect personal information from loss and unauthorised access, modification or disclosure, and to destroy or permanently de-identify unneeded personal information (NPP 4);

(iii) maintaining openness (NPP 5), access and correction (NPP 6); and

(iv) prohibiting the collection of sensitive information except in limited circumstances (NPP 10). Sensitive information is defined in section 6 of the Privacy Act as information or an opinion about an individual's racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual preferences or practices; or criminal record; that is also personal information. Heath and genetic information is also sensitive information.

An individual has the right to complain to the Commissioner about a breach of privacy under the Privacy Act. After investigating the matter, pursuant to section 52, the Commissioner is able to:

(i) make a determination dismissing the complaint;

(ii) declare that there has been a breach of privacy and that certain behaviour must not be repeated or continued;

(iii) declare that the respondent 'should perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant' or that the complainant is entitled to a specified amount by way of compensation;

(iv) declare that it would be inappropriate to take further action; or

(v) in some situations, make an order or other determination.

(b) International law

Article 17 of the International Covenant on Civil and Political Rights to which Australia is a signatory states that 'no one shall be subjected to arbitrary or unlawful interference with his privacy' and may be raised by employees seeking to challenge information collection.

2. What steps can be taken by employers to minimise such risks?

Although there are variations between jurisdictions, an employer is generally liable for discriminatory acts by employees that occur during the course of employment. This means that an employer will be held responsible if recruitment or other personnel discriminate against job applicants, for example, by seeing that an applicant has a relevant attribute on Facebook, and then deciding on that basis not to offer that person employment.

It is sometimes possible to avoid vicarious liability if an employer can establish that all reasonable steps or precautions were taken to prevent the unlawful discriminatory conduct occurring.

In order to minimise the risks of unlawful discrimination, adverse action or a breach of privacy, employers can take the following steps:

(a) Inform recruitment and other relevant personnel of the requirements and prohibitions contained in anti-discrimination legislation, the Fair Work Act and the Privacy Act.

(b) Update recruitment policies and procedures to prohibit actions that are unlawful.

(c) Run training sessions for recruitment and other relevant personnel to ensure that they are aware and reminded on an ongoing basis of their legal obligations.

(d) Ensure that adequate systems are in place to protect the personal information of job applicants once it has been collected.

(e) Draft a Privacy Policy that applies to all staff and covers all relevant NPPs or IPPs.

3. *What problems could an employer face as a result of employees using social media sites?*

There are a number of risks associated with employees' use of social media sites, both during and outside of work hours. In addition to harm that may be caused to an employer, inappropriate social media use by employees can have disastrous personal consequences for employees.

Breach of confidentiality, reputation damage, defamation and loss of productivity

Employees may deliberately or inadvertently disclose confidential information on social media sites. The disclosure of confidential information could have the consequence of waiving privilege or causing a breach of a confidentiality agreement between the employer and a third party.

Social media posts by employees may also cause damage to the reputation of an employer or another party and constitute defamation. One example of serious reputation damage caused by social media use occurred when employees of a fast-food retail chain filmed themselves apparently tampering with customers' food. Productivity loss is another risk, for example, if employees spend too much time using social media instead of working, or have their productivity affected due to the impact of discrimination, harassment or cyberbullying.

AUSTRALIA

Potential claim for unlawful discrimination, harassment or adverse action

As discussed above, employees are protected by anti-discrimination and adverse action laws. An employer will generally be vicariously liable for unlawful discriminatory actions by employees against other employees, unless the employer can show that it has taken all reasonable steps or precautions to prevent the discriminatory conduct occurring.

As well as unlawful discrimination on the basis of a relevant attribute, all state and territory anti-discrimination legislation prohibits sexual harassment, which, like discrimination and adverse action, could occur through the use of social media.

Breach of privacy or surveillance laws

As discussed above, the Privacy Act imposes obligations on employers in relation to the collection, use and disclosure of personal information. These obligations would apply both in relation to potential and current employees.

There are also a number of laws in Australia to regulate surveillance, including surveillance by employers of employees.

Cyberbullying and occupational health and safety responsibilities

Like discrimination and harassment, cyberbullying can have disastrous consequences for employees and their families. For example, more recently, the courts have been asked to consider circumstances where a death has followed bullying on social networking sites.

(a) Occupational Health and Safety legislation

WorkSafe Victoria, who are responsible for the enforcement of occupational health and safety legislation in Victoria, define bullying as 'repeated, unreasonable behaviour directed to an employee or group of employees that creates a risk to health and safety'. Employers'

responsibility in relation to the prevention of bullying, including cyberbullying, is contained in occupational health and safety legislation.

Occupational health and safety in Australia is currently regulated by various state and territory statutes. For example, in Victoria, an employer is under an obligation to 'so far as is reasonably practicable, provide and maintain for employees of the employer a working environment that is safe and without risks to health'. A breach of this section is an indictable offence. In this way, the law places a responsibility on employers to, so far as is reasonably practicable, prevent bullying in the workplace.

The responsibility to prevent workplace bullying is also contained in the Model Work Health and Safety Act (**Model Act**). It has been agreed by all states and territories that this Model Act will be reflected in all state and territory legislation by 1 January 2012.

Section 19 of the Model Act places a responsibility on a person conducting a business or undertaking (**PCBU**) to 'ensure, so far as is reasonably practicable, the health and safety of... workers engaged, or caused to be engaged by the [employer]... while the workers are at work in the business or undertaking'.

Importantly, section 27 of the Model Act places a positive duty on officers to exercise due diligence to ensure that the PCBU complies with its duties and undertakings under the Model Act. Due diligence is defined to include the acquisition and maintenance of up-to-date knowledge of work health and safety matters; ensuring appropriate resources and processes are available to minimise risk and comply with the Model Act; and verifying the provision and use of resources and processes for complying with obligations under the Model Act.

(b) Crimes Amendment (Bullying) Act 2011 (Vic)

In Victoria, the Crimes Amendment (Bullying) Act 2011 (Vic) amended the Victorian Crimes Act to make the offence of stalking apply to situations of bullying. The criminalisation of bullying could impact on employers where bullying in the workplace meets the definition in the amended Crimes Act, because outcomes include prosecution, incarceration and intervention orders.

Unfair dismissal claims may arise for employers who use information from social media sites as a basis to terminate employment

Another risk arising from the use of social media by employees is the possibility of an unfair dismissal claim if an employer terminates employment for using social media in an inappropriate manner. An employee may bring a claim under Part 3-2 of the Fair Work Act alleging that their termination was 'harsh, unjust or unreasonable' and 'not consistent with the Small Business Fair Dismissal Code' and 'not a case of genuine redundancy'.

Case law to date indicates that the Court will consider the following factors when deciding whether dismissal for inappropriate social media or internet use (**inappropriate conduct**) was unfair:

(i) whether the inappropriate conduct is connected to the employee's employment;

(ii) whether the employer had a policy in place stating that the inappropriate conduct was prohibited (though this is not essential);

(iii) whether the employer warned the employee that their behaviour would be monitored;

(iv) whether it could be reasonably expected that the inappropriate conduct would be circulated in the workplace;

(v) the content of the post/online behaviour and whether it is/was detrimental to the employer's business;

(vi) whether the employer is named in the post/online behaviour;

(vii) whether the content was removed within a reasonable time;

(viii) whether an apology was offered.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

Employers are able to minimise the risks associated with the use of social media. In addition to the risk management steps outlined above, employers can take the following actions:

Ban use of social media

Employers are able to ban the use of social media in the workplace and during work hours. However, there is evidence to suggest that this may decrease an employer's appeal for new recruits. Even if social media use is prohibited during work hours and at a workplace, employers still need to consider adopting a social media policy to govern out-of-hours and off-premises behaviour.

Introduce or update a social media policy

In order to minimise the risks associated with employees' use of social media, it is recommended that employers implement a social media policy. This policy should be reviewed regularly to ensure that it is up to date and covers the constantly evolving uses and forms of social media sites. The policy should cover the following:

(i) Provide employees with clear boundaries and rules.

(ii) Detail the process, including the complaints procedure, the consequences of non-compliance and dispute resolution procedures.

(iii) Explain how compliance will be monitored.

(iv) Ban the inappropriate use of social media whilst at work, during work hours or while using the employer's property.

(v) Explain that discrimination, adverse action, harassment and bullying can occur online, and that existing policies apply to online behaviour. Explicitly ban actions that would constitute discrimination, adverse action, harassment or bullying, regardless of when or where they occur, given that social media posts do not disappear during work hours, and therefore could be deemed to occur at work.

(vi) Provide rules to protect the employer's reputation, intellectual property and confidential information.

(vii) Explain and prohibit defamation.

This list is by no means exhaustive. Every workplace will have unique circumstances that affect the requirements and operation of a social media policy.

It is worth considering the impact and utility of existing policies when reviewing or implementing your social media policy. Cases before the courts have shown how a policy can enable employers to legitimately monitor employee behaviour and impose penalties for behaviour that an employer deems inappropriate.

Training

As discussed above, it is important that training accompany any new or updated policy. This training should be provided to new and existing staff.

Contractual provisions

In addition to a social media policy, employers may wish to include terms in the contract of employment to govern social media use.

Contributed by Corrs Chambers Westgarth

AUSTRALIA

HONG KONG

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Unlawful discrimination

Information on social media sites will often contain personal details of the job applicant, which may include the protected attributes under the four anti-discrimination ordinances. These protected attributes are sex, marital status, pregnancy, disability, family status and race (which includes the colour, descent or national or ethnic origin of an individual). An employer who treats a job candidate less favourably on the grounds of any of these protected attributes (e.g. decides not to hire the candidate) will be engaging in unlawful discrimination.

Potential implications under the Personal Data (Privacy) Ordinance ("PDPO")

The collection, use and handling of personal data of an individual is governed by the PDPO. "Personal data" is essentially any data relating to a living individual from which it is practicable, for the identity of the individual, to be directly or indirectly ascertained, and in a form which is practicable to access or process. The requirements of the PDPO are principally contained in six data protection principles ("**DPPs**"), and an employer who collects an individual's personal data must comply with those principles in dealing with the personal data.

Information about a job applicant on a social media website will most likely contain personal data of the job applicant. As such, where an employer collects information or personal data of a job applicant from a social media site for the purpose of vetting that job applicant, such collection and subsequent handling of the personal data will be subject to the PDPO.

Under DPP1, an employer must have a lawful purpose for the collection of personal data, the data collected must be necessary for, or directly related to, that purpose, and the amount of data collected is adequate, but not excessive, in relation to that purpose. In addition, the employer is required to take all reasonably practicable steps to ensure that the job applicant is informed, at the time of or before the collection of personal data, of the purpose for which the data is to be used, and the classes of persons to whom the data may be transferred.

Under DPP2, an employer must ensure that the personal data collected from the social media site is accurate. Therefore an employer must be careful not to collect and rely on personal data that is inaccurate or out of date.

An employer must also not, without the prescribed consent of the job applicant, use the personal data for any purpose other than the purpose for which the data was to be used at the time of the collection of the data, or a purpose directly related to that purpose (DPP3).

An employer must take all practicable steps to ensure that personal data (including data in a form in which access to, or processing of, the data is not practicable) collected is protected against unauthorised or accidental access, processing, erasure or other uses (DPP4).

The employer must take all practicable steps to ensure that a job applicant can ascertain its policies and practices in relation to personal data, be informed of the kind of personal data held by the employer and be informed of the main purposes for which personal data are to be used (DPP5).

A job applicant can apply to access the personal data held by the employer and make corrections to the personal data (DPP6).

If the employer is in breach of the DPPs, the job applicant may make a complaint to the Privacy Commissioner for Personal Data. The Privacy Commissioner may investigate the matter and issue an enforcement notice requiring remedy of breach. Failure to comply with the enforcement notice issued by the Privacy Commissioner is an offence, and the employer may be subject to a fine of HK$50,000 and two years' imprisonment. For a continuing offence, a daily penalty of HK$1,000 may be imposed.

2. What steps can be taken by employers to minimise such risks?

Assuming employers do not wish to take steps to ban all vetting of job applicants using information from social media, there are a number of steps which can be taken to minimise the legal risks of using the social media sites to vet a job applicant:

(a) Applicants should be told at the start of the recruitment process that the employer will conduct a vetting exercise using information available on the social media site.

(b) Applicants should be provided with a personal data collection statement which sets out the arrangement on the collection, use and handling of personal data. The employer should comply with the provisions in the statement.

(c) An employer should provide guidelines and training to employees responsible for vetting the application using information on the social media sites to ensure that only relevant and necessary information for the recruitment process will be retrieved. Those scanning social media sites as part of the recruitment process should be instructed to extract only legitimate and relevant information for the job application process.

(d) A social media policy or other written guidelines should back this up, so that the employer can demonstrate an intention to extract only relevant information.

(e) Ideally, the person scanning the social media sites should not be the same as the person who makes the hiring decision. This way, the irrelevant material (which might contain details of protected attributes) will not make its way through to the decision maker.

(f) An employer should put in place and implement an anti-discrimination policy and to conduct training for, among others, the employees responsible for the recruitment exercise.

3. *What problems could an employer face as a result of employees using social media sites?*

(a) *Breach of confidentiality*

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social media platforms, it is possible that an employee may post confidential information about the employer and/or other employees (whether inadvertently or deliberately). This could result in significant damage to the employer's business and reputation.

Networking sites such as LinkedIn allows an individual to connect online with others whom they may encounter during employment (e.g. customer contacts and suppliers) and provide the individual with a ready "contact list" or "client list" which may be accessed after cessation of employment. While banning the use of such networking sites might be impractical, an employer should consider whether its legitimate interests could be protected through the use of appropriately worded post-termination restrictive covenants.

(*b*) *Damage to employer's or third party's reputation*

Employees could post information on a social media site that causes damage to the reputation of the employer and/or a third party. An employer may be vicariously liable for the defamatory conduct of an employee. The fact that an employer may have a claim against the employee concerned could be of little comfort compared to the damage to the reputation of the employer.

(*c*) *Potential claim for Unlawful discrimination and harassment*

An employee could post negative comments about a fellow employee on social media sites. The comments could relate to a protected attribute, such as disability, race or sex. If an employee were to make such comments 'in the course of their employment', and a reasonable person would be offended, humiliated and intimidated by such comments, there is a danger that such comments could constitute unlawful harassment under the relevant anti-discrimination ordinance. In such circumstances, an employer could be vicariously liable for the actions of that employee.

If an employer permits access to social media sites using work equipment and systems during work hours, and the conduct took place in the workplace such as to create a hostile or intimidating work environment, this could amount to unlawful sexual harassment or racial harassment (as the case may be).

An employer could also risk facing other discrimination claims if employees use information they have obtained from social media sites about other employees relating to a protected attribute as the basis for treating them in a detrimental way.

An employer will not be held vicariously liable for any claim of unlawful discrimination or harassment if it has taken reasonably practicable steps to prevent the employee from committing the relevant act in question.

(*d*) *Loss of productivity*

There is a clear risk that employees will be less productive if they use social media sites during working hours.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

An employer can take the following steps:

(a) Impose an outright ban on access to social media sites at work. This approach could prove to be unpopular amongst employees and have an adverse impact on the morale within a workforce. Ultimately, the employer would need to weigh up the potential advantages and disadvantages in deciding whether to permit employees to access social media sites at work. A complete ban would not address the potential problems that could arise from postings by employees outside of working hours. Employers can easily find themselves liable for comments made after hours by employees, particularly where there is an obvious and clear link to the employment. Accordingly, comments posted by one employee about another employee after hours on a social networking site could still end up as the responsibility of the employer.

(b) Put in place a social media policy which deals with the use of social media sites during and outside of work hours. Such a policy should have provisions dealing with social media activity but, in particular:

- set out the parameters governing the use of the employer's IT systems;

- remind employees that social media activity may not necessarily be private;
- prohibit discrimination, harassment or bullying of other employees, which could include negative comments about employees posted on social media sites;
- prohibit negative comments about the employer, its employees or third parties; and
- prohibit the disclosure of any confidential information that relates to the employer and/or other employees.

The policy should set out the consequences of a breach of the policy, which could include disciplinary action and, ultimately, dismissal.

(c) Provide awareness training to employees on conduct that could constitute discrimination, harassment and bullying. To the extent that one does not already exist, put in place and implement a written anti-discrimination and anti-harassment policy and conduct training to the employees. An employer would have a defence to any claim for unlawful discrimination or harassment if it can show that it took all reasonably practicable steps to prevent the employee from committing the discriminatory act in question.

(d) Monitoring the use of social media sites at work could help to determine whether there is a loss of productivity as a result of employees accessing such sites. However, it is important to bear in mind that such monitoring may be subject to the PDPO. Legal advice should be sought before engaging in any such monitoring.

(e) Incorporate within employment contracts an appropriate confidentiality clause, which could afford protection to the employer in the event that an employee posts confidential information on a social media site.

(f) Consider the use of post-termination restrictive covenants where an employee could build a "client list" of contacts acquired during employment through a networking site (like LinkedIn) which the employee can subsequently use after cessation of employment.

(g) Disciplinary action may be taken against an employee who misuses a social media site to the detriment of the employer. In some cases, an employer could consider dismissal. Each case will turn on its facts and an employer might want to obtain legal advice before proceeding to dismiss the employee in question.

Contributed by Mayer Brown JSM

INDIA

1. *Are there any risks for employers that use social media sites to vet job applicants?*

The potential risks that may arise when an employer includes cyber-vetting as a step in the recruitment process are:

Allegations of unlawful discrimination

Social media sites often contain personal information of the job applicant such as sex, race, caste, religion, place of birth, marital status, pregnancy, disability, family status and sexual orientation. Key recruitment decisions are sometimes made on the information available on such sites. In India, there is no comprehensive anti-discrimination code, and the concept of anti-discrimination is largely based on the constitutionally guaranteed 'right to equality', which is a 'fundamental right' available to all citizens. Under the Indian Constitution, no citizen shall be ineligible for, or discriminated against in respect of, any employment or office under the State, only on the grounds of religion, race, caste, sex, descent, place of birth or residence. The Constitution provides the ability to enforce fundamental rights only against State-owned entities, and a citizen may not be able to enforce this right against a private employer. However, if a State-owned employer discriminates against an applicant on the basis of his or her religion, race, caste, sex, descent, place of birth or residence based on information derived from a social media site or elsewhere, then the individual would have the ability to obtain relief against the employer by seeking appropriate remedial directions from a relevant court.

In the context of employment in the private sector, in the event that an applicant challenges the employer's apparent discriminatory practices based on the information available on social media sites, the credibility and reputation of the employer could be significantly affected.

Privacy issues

Currently, there is no specific statute that governs data privacy in India, and protection is largely based on the constitutionally guaranteed 'right to privacy'. However, most of the jurisprudence in this area has focused on the rights of citizens against illegal invasion of privacy by government enforcement agencies.

Recently, the Information Technology Act, 2000 has been amended to incorporate certain provisions relating to data protection. Under Section 43A, a body corporate can be made liable for damages in the event that it does not implement 'reasonable security practices and procedures' with respect to sensitive personal information stored on its computers or IT systems. The Government has recently brought into effect rules under Section 43A, setting out the practices and procedures that must be implemented by corporate bodies for the collection, transfer and disclosure of such sensitive personal information ("Privacy Rules"). The Privacy Rules have defined 'sensitive personal data' to mean personal information, such as passwords, financial information, physical, physiological and mental health conditions, sexual orientation, medical history and biometric information. However, information available in the public domain is excluded from the ambit of 'sensitive personal data'.

In the instant context, since information in the public domain is specifically excluded from the purview of 'sensitive personal data', there is very little risk associated with an Indian employer accessing or collecting any data relating to a job applicant that is available on publicly accessible social media sites.

The position would be similar in the context of State employment as well. As highlighted above, there is little risk that an individual would be able to allege a breach of his or her privacy should a State-owned employer access publicly

available sensitive personal information in relation to the recruitment process. That said, the risks associated with anti-discriminatory practices (discussed above) would remain and must be kept in mind.

Authenticity of information

The information available on social media sites may not be accurate and, in certain circumstances, may have been deliberately falsified, and employers should therefore not rely solely on these websites to obtain information relating to the applicant. This, however, is not a legal risk.

2. *What steps can be taken by employers to minimise such risks?*

As discussed earlier, under the current legal regime, the risks associated in accessing publicly available information about the applicant on social media sites are minimal in India – even more so in the context of private sector employers. However, as a matter of caution, the following steps may be taken to minimise the few risks that are associated with cyber-vetting:

- It is quite common for employers in India to carry out background checks of the information submitted by job applicants. The applicants could be informed that the company may access any publicly available information about him or her as part of the recruitment process. If the company intends to store, save or transfer such information, then it would be advisable to seek the consent of the applicant beforehand. The individuals in charge of recruitment should also ensure that methods such as hacking, the circumvention of privacy settings, obtaining access via third parties, the misuse of identities and coercion have not been adopted to access the applicant's information on the social media site.
- The employer must adopt a consistent method for screening all applicants.

- The employer should not rely solely on the information obtained on social media sites to make decisions on recruitment. Should any information that adversely impacts the decision to recruit come to light via a social media site, the employer should take steps to verify the information from reliable sources.
- Employers should keep records of the information reviewed and relied upon by them in taking any employment decisions, to be able to counter any potential discrimination claims.
- The employer can implement an anti-discrimination policy and provide training on the subject to all of its recruiters. The employer should also ensure that the person making the recruitment decision and the individual vetting the information on social media sites are not the same. The persons vetting the social media must be trained not to relay any information that could be used as the basis of a discrimination claim against the employer (for example, the applicant's religious belief). This will enable the employer to justify that the recruitment has not been discriminatory.

3. *What problems could an employer face as a result of employees using social media sites?*

The problems that an employer could possibly face as a result of employees accessing social media sites are:

Confidential Information

Social media presents an easy method of accessing and communicating information. Employees' use of social media sites, particularly professional networking forums, could result in the unauthorised disclosure of confidential information belonging to the employer. The informal nature of social media results in a higher risk of information being

leaked, since the employees are more often than not oblivious of the consequences of such disclosures.

Employee Solicitation

Employees are usually connected with their colleagues and other individuals within their field on professional networking sites. At the end of an employee's employment, social media sites could be used as a tool for soliciting ex-colleagues or customers.

Defamation and damage to reputation

Employees could post messages containing offensive comments about their employer or colleagues on social networking websites, which could result in damage to the reputation of the employer. Employees could also make offensive statements, which could be detrimental to the employer's business interests.

Discrimination

As highlighted above, social media websites could contain personal information of the employee such as sex, race, caste, religion, place of birth, marital status, pregnancy, disability, family status and sexual orientation. An employee could claim that any key employment decision made by the employer (such as decisions relating to promotion and pay increases) was discriminatory on the basis that the employer took into account personal information obtained from social media sites.

Loss of productivity

The use of social networking sites by employees during work hours could result in reduced efficiency and productivity. Also, extended working hours of an employee due to business hours being used for social networking activities could result in claims for overtime wages.

Harassment

Social media tools could also be used to harass colleagues by posting objectionable or offensive content. This could also detrimentally affect the reputation of the employer as it could be alleged that the employer failed to provide a healthy working environment.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

To minimise the risks associated with employees using social media sites, the employer could take the following steps:

- Block social networking sites. However, this does not minimise the risk of defamation and disclosure of confidential information as the employees have access to these sites outside work. This step could address any concerns surrounding productivity.
- Social Networking Policy – the employer could introduce a social media policy by setting out the obligations and responsibilities of the employees in relation to the use of social media sites during and beyond work hours. The social media policy should:
    - Define 'social media' – the policy should broadly define 'social networking' or 'social media' and specify names of sites that would be included within the definition. The definition should be wide enough to cover unknown future trends.
    - Access – the policy should address whether access to social media sites is allowed during work hours and the employer's level of tolerance towards personal use of social media.
    - Privacy – the policy should set out clearly that employees should have no expectation of privacy when using the employer's electronic equipment

or network, and that the employers have the ability to monitor all use of the employer's equipment or infrastructure for any purpose.

- Confidential Information – the policy should reiterate the employer's policy on the dissemination of proprietary or confidential information and trade secrets. The policy should make it abundantly clear that proprietary information is not to be discussed or referred to on such sites and spell out examples of information that may be considered to be confidential. The policy should state that such disclosure could result in disciplinary action, including termination of employment.
- Harassment – the policy should set out clearly that any form of harassment or bullying of other employees, including making libellous, defamatory or negative comments, on social media sites, is prohibited.
- References to clients/customers – the policy should make it clear that employees must not reference any clients, customers, or partners without obtaining the employer's express permission to do so. Employees can be prohibited from posting comments about clients, customers or third parties that may prove detrimental to the employer's business. The policy should, however, provide employees an alternative internal (non-public) forum to air their grievances with the employer so that the policy stands out as reasonable.
- Racial remarks – the policy should prohibit employees from posting messages that have racial or sexual connotations, or any other message that is inappropriate and/or has the potential to cause the

employer or customers and business partners, harm or embarrassment.

- Representation – the policy should require employees to obtain the employer's consent to identify themselves as representatives of the employer. If employees are allowed to advertise their association with the employer, the policy should require them to take on the responsibility for representing the employer in a professional manner. The employees should be required to use disclaimers with respect to their personal blogs that make it clear that the postings are solely those of the employee and do not represent the views of the employer.
- Copyright – the policy should require all employees to, at all times, comply with the law with regard to copyright.
- Miscellaneous – the policy should instruct employees to use good judgment and take personal and professional responsibility for content that is posted. It should prohibit employees from transmitting, uploading or downloading any material that potentially contains viruses, Trojan horses, worms, time bombs, or any other malicious code.

- Training – employees should be provided with training with regard to their obligations and responsibilities when using social media. During such training, the employees should be categorically informed that any violation of the social media policy will be taken seriously and could warrant disciplinary action, including termination of employment.

- Employment contracts – these must contain appropriate confidentiality and non-solicitation clauses, which could afford protection to the employer in the event of unauthorised disclosure of confidential information or solicitation of employees or customers.

Contributed by Trilegal

INDIA

INDONESIA

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Unlawful discrimination

The use by employers of information available on social media sites is not expressly regulated in Indonesia. However, in using such data to vet job applicants, or for any other purpose, the employer must not violate Articles 5 and 6 of Law Number 13 of 2003 regarding Employment (the "**Employment Law**"), which prohibit discrimination on the basis of sex, marital status, race, nationality and ethnic origin. Articles 5 and 6 of the Employment Law provide that every worker must have equal opportunity, without discrimination, to obtain a job, as well as being entitled to equal treatment without discrimination by the employer.

An employer that fails to comply with the above provisions could be subject to the following administrative sanctions:

a. reprimand action;

b. written warning;

c. restrictions on business activities;

d. suspension of all business activities;

e. cancellation of business license;

f. cancellation of business registration; or

g. suspension of part or all of the relevant production facilities.

2. *What steps can be taken by employers to minimise such risks?*

If employers wish to use information contained on social media sites for the purposes of vetting job applicants, they could take the following steps to minimise the risks that could arise:

a. The employer should publish the job requirements in a public advertisement in order to notify all job applicants of the company's needs on a transparent basis.

b. If there is a job that requires a specific ethnicity, gender or religion, the employer should explain the business reasons for such requirements to the job applicants.

   For example, if the employer needs security guards to be available to work during the Idul Fitri holiday, the employer should so indicate without stipulating that the candidate must be "non-Muslim".

   Similarly, for a Corporate Social Responsibility position in an outlying area, the employer may state that persons having fluency in the local language and experience with the relevant local community and its unique customs will have priority in the selection process, rather than specifying a particular ethnicity or religion as a requirement.

   As each job has different needs, the most important thing, when drawing up the job requirements, is to exercise common sense and diligence while ensuring that each requirement has legitimate business reasons.

c. The company could issue a policy indicating that social media websites are a possible source of information in determining the qualifications of job applicants and compliance with company policies by existing employees. Such policy may be included in the work rules, locally known as the "Company Regulation".

3. What problems could an employer face as a result of employees using social media sites?

With social media such as Facebook, Twitter, Myspace, LinkedIn and others, the way we interact with the public has changed. Individuals and employees are able to interact with each other directly, freely, anytime and anywhere.

In a corporate context, this carries various implications for external 'stakeholders' of the company, including existing and potential customers, clients, investors, government officials and the media, and the internal 'stakeholders' of the company (i.e. the employees). There are both advantages and disadvantages of the use of social media sites by their employees.

Advantages

Social media can be a positive and direct way of communicating with customers, clients or potential customers, as a marketing objective to increase credibility and brand awareness. For example, some employers encourage their employees to use social media websites such as Twitter to discuss their products. Employees discuss not only the product itself, but also internal company processes, such as product development, marketing initiatives and consumer testing.

Disadvantages

Companies face problems when employees misuse social media websites, and employees' employment could be terminated due to the inappropriate use of social media websites. These problems can include the discussion of proprietary corporate information in the public domain, neglecting confidentiality agreements and slandering their employers, as well as inappropriate online statements by disgruntled employees.

a. *Damage to the employer's or third party's reputation*

If the company does not put in place restrictions, employees are free to share their comments or documents, as they would through email. However, unlike email, information shared on social media websites is often public, and this can be damaging to the employer's image. Employees have also been known to

post controversial and inflammatory remarks that attract negative publicity, or are opposed to the company's marketing and communications objectives.

b. *Breach of Confidentiality*

Due to the nature of social media sites, posting information can be done easily and can be widely accessed. It is possible that an employee might deliberately or accidentally post confidential information about the employer, which could result in damage to the employer's reputation or business.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

The following are some examples of how an employer can minimise these risks:

a. The employer could prohibit access to social media websites at work or during working hours. Although this is an effective way to maintain the productivity of an employee, it does not provide a perfect solution to protecting the company's reputation and confidential information, since the employee can still access social media websites through mobile phones or personal laptops.

b. The employer can protect their reputation and confidential information by drawing up guidelines regarding the use of social media. By providing clear guidelines about the employee's code of conduct when using social media websites, any controversial issues or otherwise inappropriate postings by employees can be prohibited and expressly made grounds for termination, and thus discouraged. This way, the employer still benefits from the advantages of social media sites, but imposes guidelines and limitations on such access to social media sites. The company should

protect its interests by educating employees about social networking and also inform them that the company reserves the right to monitor the use of social media by employees, whether it is done in the office, outside the office or during personal time. With these guidelines and expectations, employees are more likely to be enthusiastic about using social media in a positive way, rather than if they only receive warnings about what not to do, which may be perceived as threatening their right of use outside office hours. Some large companies have imposed social media policies for employees in which they treat every employee as an 'individual brand manager'. Employees are provided with clear guidance and expectations, and are then allowed to act in accordance to achieve such goals.

c. Stipulate a confidentiality clause in both the Employment Contract as well as in the Company Regulation.

d. Provide clear guidelines for possible disciplinary action against employees who misuse social media websites.

Contributed by Soewito Suhardiman Eddymurthy Kardono

INDONESIA

JAPAN

1. *Are there any risks for employers that use social media sites to vet job applicants?*

(a) *Personal Information Protection Act 2003 ("PIPA")*

The collection, use and handling of the personal information of an individual are governed by the PIPA. The requirements under the PIPA apply to a person or entity that holds the personal information of five thousand (5,000) or more persons on any day in the past six months, and uses a personal information database for its business.

"Personal information" means information regarding a living person that would allow identification of the person as a certain individual (including such information which can easily be viewed together with other information, and subsequently enable the identification of a certain individual). Information of a job applicant on a social media website will most likely contain personal information of the job applicant. As such, where an employer collects information or personal information of a job applicant from a social media site for the purpose of vetting that job applicant, the collection and subsequent handling of the personal information will be subject to the PIPA.

In particular, based on the PIPA, if an employer has not publicly announced the purpose of use of the personal information, it must, without delay, upon receipt of the personal information, notify the applicant or publicly announce the purpose of use of the personal information (Article 18). Further, an employer may not use the personal information obtained for a purpose other than the specified purpose without obtaining prior consent from the relevant individual (Article 16). Accordingly, when an employer collects personal information of a job applicant using social media, the employer must publicly announce the purpose of use of the collected personal information or notify the purpose to the job applicant.

If the employer is in breach of the PIPA, the relevant Minister may issue an improvement order. Failure to comply with such an order may lead to imprisonment of up to 6 months or a fine of up to 300,000 yen.

(*b*) *Employment Security Act 1947 ("ESA")*

The ESA prohibits employers from acquiring certain sensitive information about applicants. Article 5-4 of the ESA and the relevant guidelines issued by the Ministry of Health, Labor and Welfare (*Kokuji* No. 141 of 1999, as amended) restrict an employer's right to acquire the following types of sensitive personal information about job applicants:

(a) information regarding their race, ethnicity, social status, family origin (*monchi*), legal domicile (*honseki*), place of birth or other information which might result in social discrimination;

(b) information regarding their political opinions or religious beliefs; and

(c) information about their membership of labour unions.

However, these guidelines do provide an exception in the case where such an employer has a high need to know such sensitive personal information in order to conduct their business (for example, to judge whether an applicant is able to perform the job for which he or she is applying). In this case, the employer must acquire the information directly from the applicant, and expressly explain why the employer needs to know this information.

If an employer violates this provision of the ESA, the Minister of Health, Labor and Welfare may issue an improvement order. Failure to comply with such an order may lead to imprisonment of up to 6 months or a fine of up to 300,000 yen (Articles 48-3 and 65 of the ESA).

2. What steps can be taken by employers to minimise such risks?

Assuming employers do not wish to take steps to ban all vetting of job applicants using information from social media, there are a number of steps which can be taken to minimise the legal risks of using social media sites to vet a job applicant:

(a) Applicants should be told at the start of the recruitment process that the employer will conduct a vetting exercise using information available on social media sites.

(b) Applicants should be provided with a personal data collection statement which sets out, among other things, the purpose of use of the personal information collected in the course of recruitment process. The employer should comply with the provisions in the statement.

(c) An employer should provide guidelines and training to employees responsible for vetting the application using information on social media sites to ensure that only relevant and necessary information for the recruitment process will be retrieved. Those scanning social media sites as part of the recruitment process should be instructed to extract only legitimate and relevant information for the job application process.

(d) A social media policy or other written guidelines should back this up, so that the employer can demonstrate an intention to extract only relevant information.

(e) Ideally, the person scanning social media sites should not be the same as the person who makes the hiring decision. This way, irrelevant material (which might contain prohibited information) will not make its way through to the decision maker.

3. What problems could an employer face as a result of employees using social media sites?

(a) *Breach of confidentiality*

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social media platforms, it is possible that an employee may post confidential information about the employer and/or other employees (whether inadvertently or deliberately). This could result in significant damage to the employer's business and reputation.

Networking sites such as LinkedIn allow an individual to connect online with others whom they may encounter during employment (e.g. customer contacts and suppliers), and provide the individual with a ready "contact list" or "client list" which may be accessed after cessation of employment. While banning the use of such networking sites might be impractical, an employer should consider whether its legitimate interests could be protected through the use of appropriately worded post-termination restrictive covenants.

(b) *Damage to employer's or third party's reputation*

Employees could post information on a social media site that causes damage to the reputation of the employer and/or a third party. An employer may be vicariously liable for the defamatory conduct of an employee. The fact that an employer may have a claim against the employee concerned could be of little comfort compared to the damage to the reputation of the employer.

(c) *Potential claim for harassment*

An employee could post negative comments about a fellow employee on social media sites. If the comments are detrimental to the fellow employee's reputation or otherwise deemed as harassment, the employee may be responsible for

damages based in tort. In such circumstances, an employer could be vicariously liable for the actions of that employee.

(*d*) *Loss of productivity*

As well as the legal issues described above, the use of social media sites by employees could impact their efficiency and productivity if this takes place during working hours.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

An employer can take the following steps:

(a) Impose an outright ban on access to social media sites at work. This approach could prove to be unpopular among employees and have an adverse impact on the morale within a workforce. Ultimately, the employer would need to weigh up the potential advantages and disadvantages in deciding whether to permit employees to access social media sites at work. A complete ban would not address the potential problems that could arise from postings by employees outside of working hours. Employers can easily find themselves liable for comments made after hours by employees, particularly where there is an obvious and clear link to the employment. Accordingly, comments posted by one employee about another employee after hours on a social networking site could still end up as the responsibility of the employer.

(b) Put in place a social media policy which deals with the use of social media sites during and outside of work hours. Such a policy should have provisions dealing with social media activity but, in particular:

- set out the parameters governing the use of the employer's IT systems;
- remind employees that social media activity may not necessarily be private;

- prohibit discrimination, harassment or bullying of other employees, which could include negative comments about employees posted on social media sites;
- prohibit negative comments about the employer, its employees or third parties; and
- prohibit the disclosure of any confidential information that relates to the employer and/or other employees.

The policy should set out the consequences for a breach of the policy, which could include disciplinary action and, ultimately, dismissal.

(c) Provide awareness training to employees on conduct that could constitute discrimination, harassment and bullying. To the extent that one does not already exist, put in place and implement a written anti-discrimination and anti-harassment policy and conduct training in this respect for employees. An employer may have a defence to a harassment claim if it can show that it took all reasonably practicable steps to prevent the employee from committing the harassment in question.

(d) Monitor the use of social media sites at work to help determine whether there is a loss of productivity as a result of employees accessing such sites. However, it is important to bear in mind that such monitoring may be subject to the PIPA and also involve privacy issues. Legal advice should be sought before engaging in any such monitoring.

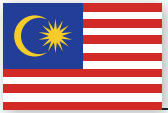
(e) Incorporate, within employment contracts and the rules of employment, an appropriate confidentiality clause, which could afford protection to the employer in the event that an employee posts confidential information on a social media site.

(f) Consider the use of post-termination restrictive covenants where an employee could build a "client list" of contacts acquired during employment through a networking site (like LinkedIn) which the employee can subsequently use after cessation of employment.

(g) Take disciplinary action against an employee who misuses a social media site to the detriment of the employer. Each case will turn on its facts, and an employer might want to obtain legal advice before proceeding to take disciplinary action against the employee in question.

Contributed by Anderson Mori & Tomotsune

JAPAN



MALAYSIA

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Application of the Personal Data Protection Act 2010

There may be risks associated with the use of social media websites to vet job applicants by employers, following the enactment of the Personal Data Protection Act 2010 ("PDPA"). The PDPA is not yet in force. However, once PDPA comes into force, it is important that employers comply with the PDPA when dealing with personal information of job applicants.

The PDPA governs the collection, use and handling of personal data. Social media websites will, in all likelihood, contain personal information regarding the job applicant, and therefore the collection and subsequent processing of such information will be governed by the PDPA.

When processing personal data, an employer must comply with the seven Personal Data Protection Principles, which are as follows:

a. the General Principle;

b. the Notice and Choice Principle;

c. the Disclosure Principle;

d. the Security Principle;

e. the Retention Principle;

f. the Data Integrity Principle; and

g. the Access Principle.

A failure to comply with any of the above principles (subject to certain exceptions) constitutes an offence and, upon conviction, is punishable by a fine not exceeding RM300,000 and/or imprisonment for a term not exceeding 2 years.

The General Principle

In essence, under this principle, personal data can only be processed if the data subject has given his consent to the processing of the personal data.

Notice and Choice Principle

The general rule is that the data subject must be informed in writing by the data user that personal data will be processed. The data user must provide the description of such personal data to the data subject.

Disclosure Principle

Under this principle, personal data should not be disclosed without the consent of the data subject, unless it is for the stated purpose behind the collection of the personal data.

Security Principle

The data user shall, when processing personal data, take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

Retention Principle

The PDPA provides that personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose. It imposes a duty on a data user to take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed.

Data Integrity Principle

The Data Integrity Principle imposes an obligation on a data user to take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up-to-date, by having regard to the purpose, including any directly related

purpose, for which the personal data was collected and processed.

Access Principle

This principle provides that a data subject shall be given access to his personal data, held by a data user, and be able to correct that personal data where the personal data is inaccurate, incomplete, misleading or not up-to-date (except where compliance with a request to such access or correction is refused under certain circumstances as set out in the Act).

Unlawful discrimination

Under Article 8 of the Federal Constitution, discrimination against citizens on the grounds of religion, race, descent, place of birth or gender is unlawful, but only in the context of employment with a public authority.

2. *What steps can be taken by employers to minimise such risks?*

a) Employers should comply with the provisions of the PDPA once it comes into force.

b) Guidelines should be put in place for employees who collect and use personal data in the recruitment process to ensure only relevant information is collected and to ensure the confidentiality of the data subject's personal data is not compromised. This way, the employer will minimise the risk of breaching the PDPA.

3. *What problems could an employer face as a result of employees using social media sites?*

(a) *Breach of confidentiality*

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social media platforms, it is possible that an employee may post confidential information about the employer

and/or other employees (whether inadvertently or deliberately). This could result in significant damage to the employer's business and reputation.

(*b*) *Damage to reputation*

Employees could post information on a social media site that causes damage to the reputation of the employer and/or a third party. An employer may be vicariously liable for the defamatory conduct of an employee. The fact that an employer may have a claim against the employee concerned could be of little comfort compared to the damage to the reputation of the employer.

(*c*) *Loss of productivity*

There is a risk that the use of social media websites during offices hours may result in a reduction in productivity in the workplace.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

An employer can take the following steps:

- Impose a ban or restriction on the use of social media websites during office hours. However, such a move may prove unpopular and could be easily circumvented by the use of personal smart phones by employees.
- Have in place guidelines that deal with the use of social media websites during and outside offices hours, which should include the following content:
  - guidelines for the use of the employer's IT systems;
  - a prohibition on the disclosure of the employer's confidential information on social media sites;
  - notification that the use of social media sites may be monitored by the employer;

  - a prohibition on discriminatory or defamatory comments on social media sites;
  - notification that a breach of the guidelines could result in disciplinary action being taken by the employer.
- Monitoring the use of social media sites by employees. However, such activities/conduct could be covered by the provisions of the PDPA and legal advice should be sought before engaging in such monitoring.
- The inclusion of confidentiality clauses in the employment contract to cover instances where confidential information is submitted on social media sites.

Contributed by Shearn Delamore

MALAYSIA

NEW ZEALAND

1. *Are there any risks for employers regarding use of social media sites to vet job applicants?*

The use of social media sites to vet job applicants primarily raises issues of discrimination and privacy.

Unlawful discrimination

Information on social media sites often contains an applicant's personal details, such as their age, sex, marital status, religious belief, ethical belief (i.e. lack of a religious belief), colour, race, ethnic or national origins, disability, age, political opinion, employment status, family status and sexual orientation. These are all grounds of discrimination that are prohibited by the Human Rights Act 1993 (**HRA**).

If an employer takes the above information into account in deciding whether to hire or decline an applicant, this could give rise to claims of unlawful discrimination under the HRA.

Privacy Act 1993

The Privacy Act 1993 (**PA**) defines personal information as "*information about an identifiable individual*". "Personal information" extends to information that is "*personal*" to the individual concerned, in the sense of being "*private*" or "*sensitive*", and case-law demonstrates that the term is defined widely. So long as information has the capacity to identify an individual to some members of the public, it may be regarded as "*personal information*" for the purposes of the PA.

As the information posted on a prospective employee's social media profile is likely to include information about the individual, it is likely to be "*personal information*" for the purposes of the PA. Various Information Privacy Principles (**Principles**) within the PA will therefore apply to the collection, use and storage of such information:

(a) Principle 1: An employer may only collect information relating to prospective employees for lawful purposes

connected with the function or activity of the employer's organisation. Any information collected by an employer from social media sites must be lawful and necessary for the purposes of recruitment.

(b) Principle 2:

(i) Except in limited circumstances, an employer must collect personal information directly from the individual concerned.

(ii) One exception to this requirement is if the employer believes, on reasonable grounds, that the information is publicly available information.

(iii) A social media site may contain public information about an applicant for employment, and an employer may legitimately collect this information, even though it is not collected directly from the applicant.

(iv) However, if some or all information on a social media site can be accessed only by an applicant's authorised "friends" or "contacts", an employer may not collect or use this restricted private information without the applicant's express authorisation.

(c) Principle 3:

(i) Where an employer collects information from an applicant, the employer must take reasonable steps to ensure that the applicant is aware of:

- the fact that the information is being collected;
- the purpose for which the information is being collected;
- the intended recipients of the information;

- the name and address of the agency collecting and holding the information; and
- the rights of access to, and correction of, personal information provided by these principles.

(ii) The applicant should be informed of the above before the information is collected, or, if that is not practicable, as soon as practicable after the information is collected.

(iii) Collecting personal information from an applicant's public social network page without taking the above steps will expose the employer to a breach of Principle 3.

(d) Principle 4:

(i) An employer may not collect information by unlawful means, or by means that are unfair or unreasonably intrude into the personal affairs of a prospective employee.

(ii) Although searching the public aspects of social media sites may not necessarily be an unreasonable intrusion into the personal affairs of an applicant, if some or all information within the social media site is private and restricted, an employer would be acting in breach of Principle 4 if it was able to somehow collect this private information (unless it collected the information directly from the applicant or had their express authorisation to do so).

(e) Principles 6 and 7: An applicant is entitled to request access to, and correction of, any information that the employer has collected from a social media site (subject to limited exceptions).

(f) Principle 10: Subject to limited exceptions, information obtained in connection with one purpose should not be used for any other purpose. One exception to this Principle is where the information is publicly available.

(g) Principle 11: Subject to limited exceptions, information obtained should not be disclosed to any other person or agency. One exception to this Principle is where the disclosure of the information is one of the purposes for which the information was collected, or a directly related purpose.

Any person may make a verbal or written complaint to the Privacy Commissioner if they believe any of the Principles have been breached. If the complaint cannot be resolved informally (including by mediation) the Privacy Commissioner, or the individual, may pursue a claim in the Human Rights Review Tribunal. The Tribunal can order various remedies, including damages of up to $200,000, for any breach of the PA (although awards over $15,000 are rare).

2. What steps can be taken by employers to minimise such risks?

If employers wish to use social networking sites as part of the recruitment process, requirements should be put in place to ensure there is no unlawful discrimination or any breach of the Principles of the PA.

Privacy and discrimination policies, along with pre-employment forms, should be updated to reflect their application to social media sites, and all staff in contact with any information collected from these sites should be properly trained on the application of the policies.

At the start of the recruitment process, applicants should be notified of all of the requirements within Principle 3 of the PA, including that any information the employer may find on public social media sites may be used in determining the applicant's suitability for the position. Applicants should

also be informed of their rights to access and correct any such information (although exceptions within the PA may potentially apply, and allow the employer to withhold some or all of it).

An employer should ensure that only relevant and necessary information is gathered from social media sites. Searches should be limited to publicly available information, and employers must not fraudulently gain access to users' profiles by posing as friends, or by any other inappropriate means.

Any social media site checks should be performed in a consistent manner for every applicant to avoid unfair treatment.

Social media checks should also ideally be done by someone who is not the decision-maker in the recruitment process. The decision-maker should be prevented from examining all information that is collected from social media sites. Only non-discriminatory factors that are relevant to a hiring decision would then be reported back to the decision-maker, as required.

An employer should be careful not to place too much weight on information found through social media sites because of the risk of unreliability. An applicant's profile on a social media site may, inadvertently or intentionally, contain false information about them.

3. What problems could an employer face as a result of employees using social media sites?

(a) **Breach of Confidentiality**

As social media sites provide an open forum for individuals to post and exchange information, there is a risk employees could (either inadvertently or intentionally) post confidential information about their employer, the employer's clients/customers/suppliers, and other employees.

(b) **Damage to Reputation/Defamation**

Information posted on employees' social media sites may be embarrassing and potentially damaging to the employer's (or a third party's) reputation in the marketplace. In some situations, the information may be defamatory. An employer may be vicariously liable for the conduct of an employee in such situations.

(c) **Virtual workplace bullying**

Social media sites are increasingly being seen as part of workplace bullying and harassment claims.

In a recent case, an emergency dispatcher was dismissed because she had harassed colleagues by sending them offensive Facebook and text messages. Although the employee's dismissal was found to be unjustified for procedural flaws in the disciplinary process, the Authority refused to order reinstatement of the employee because the offensive Facebook and text messages reinforced that reintegration of the employee in the workplace was not practicable.

(d) **Loss of Productivity**

Another potential negative impact of an employee using social media sites during working hours is a loss of productivity.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

(a) **Impose an outright ban on access to social media sites at work**

This approach could prove to be unpopular among employees and have an adverse impact on the morale within a workplace.

Ultimately, the employer would need to weigh up the potential advantages and disadvantages in deciding whether to permit employees to access social media sites at work.

A complete ban would not address various potential problems (outlined above) that could arise from postings by employees outside of working hours, such as breaches of confidentiality, etc.

(b) **Update the company's internet and email policy:**

A key step to reduce the risks of employees' use of social media sites is for employers to implement sound policies regulating their use.

Such a policy should state that, when engaging in social networking, the employee must not:

(i) Make any statement that could be read as though they are writing on behalf of, or expressing the views of, the employer or any of its employees;

(ii) Reveal any confidential information about the employer that they obtained during the course of their employment;

(iii) Use the company's logos or trademarks;

(iv) Make any disparaging comments about the company, its employees, or its customers or competitors; or

(v) Let social media activities unreasonably interfere with work commitments.

The company's internet and email policy should also:

(i) Set out the parameters governing the use of the employer's IT systems, including the following:

- the employer owns its business tools, including the equipment/devices employees take home;

- business tools are predominantly for work purposes, and specify whether reasonable personal use may be permitted;
- employers can monitor employees' use; and
- employers may also access data about how employees use its business tools;

(ii) Remind employees that social media activity may not necessarily be private;

(iii) Prohibit discrimination, harassment or bullying of other employees, which could include negative comments about employees posted on social media sites;

(iv) Prohibit negative comments about the employer, its employees or third parties; and

(v) Prohibit the disclosure of any confidential information that relates to the employer, other employees and/or third parties.

Such a policy should set out the consequences of a breach of the policy, which could include disciplinary action up to and including dismissal.

(c) **Training to employees**

Employers should provide training to employees on conduct that could constitute discrimination, harassment and/or bullying.

To seek to avoid vicarious liability for an employee's discriminatory actions under the HRA, employers must establish that they took all reasonably practicable steps to prevent the employee from committing the discriminatory action. Adequate training is one of the key elements in an employer seeking to rely on such a defence.

(d) **Incorporate an appropriate confidentiality clause**

Employers should incorporate appropriate confidentiality clauses within employment agreements, which ideally explicitly refer to the prohibition on disclosing confidential information in social media sites.

(e) **Incorporate an appropriate restraint of trade clause**

Employers should consider the use of post-termination restrictive covenants to address the scenario of an employee building up a client list of contacts acquired during employment through social media sites, and using this list to the employer's detriment (for example to solicit clients after termination of employment).

(f) **Take disciplinary action**

Disciplinary action (up to and including summary dismissal) may potentially be taken against an employee who misuses a social media site to the detriment of their employer, a third party or co-worker.

The New Zealand Employment Relations Authority (**Authority**) has indicated that such postings need to meet a relatively high threshold, and be more than simply "disparaging" or "derogatory" about an employee's workplace, to constitute grounds for dismissal.

In a recent case, the Authority decided that an employee's description of herself on Facebook as "*a government employee and a very expensive paperweight who is highly competent in the art of time wastage, blame shifting and stationery theft*" was insufficient to alone justify her dismissal.

Contributed by Simpson Grierson

NEW ZEALAND

PAKISTAN

1. *Are there any risks for employers that use social media sites to vet job applicants?*

There are no laws in Pakistan which govern data privacy within the context of an employment relationship.

Discrimination on the basis of sex, religion, race, caste, residence or place of birth is prohibited in Pakistan. Although these rights can be enforced in the courts, there have been no reported cases where this has happened in the context of employment. Therefore in practice, the risk to employers using social media sites to vet job applicants is low.

2. *What steps can be taken by employers to minimise such risks?*

As stated above, the risks attached to such vetting of job applicants are very low. However, the steps set out below are generally recommended.

Assuming employers do want to vet job applicants using information from social media sites, there are a number of steps which can be taken to guard against unnecessary risk:

- Those scanning social media sites as part of the recruitment process should be instructed to extract only legitimate and relevant information for the job application process.
- A social media policy or other written guidelines should back this up, so that the employer can demonstrate an intention to extract only relevant information.
- Ideally, the person scanning the social media sites should not be the same as the person who is determining the job application process or interviewing the individual. This way, the irrelevant material (which might contain sensitive personal data) will not make its way through to the decision maker.

- Applicants should be told, at the start of any application process, that a vetting or verification exercise using social media sites forms part of the process.
- Job applicants who are rejected because of information gleaned from social networking should be given an opportunity to correct that information before any final decisions are taken.

3. *What problems could an employer face as a result of employees using social media sites?*

Breach of confidentiality

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social media platforms, it is not uncommon for employees to end up posting confidential information about the employer and/or other employees. This could result in significant damage to the employer's business and reputation.

Damage to employer's or third party's reputation

Employees could post information on a social media site that causes damage to the reputation of the employer and/or a third party. An employer may be vicariously liable for the defamatory conduct of an employee. The fact that an employer may have a claim against the employee concerned could be little comfort compared to the damage to the reputation of the employer.

Harassment/Unlawful discrimination

It is not uncommon for employees to post negative comments about fellow employees on social media sites. The comments could relate to a characteristic which is protected from discrimination such as sex, religion or race. If an employee were to make such comments, there is a danger that these could constitute unlawful discrimination. However, as

mentioned above, the likelihood that this would impact on an employer is low.

Loss of productivity

Employers could struggle with issues of loss of productivity if staff can access and use social media sites during work hours.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

An employer can take the following steps:

- Impose an outright ban on access to social media sites at work. This approach could prove to be unpopular amongst employees and have an adverse impact on the morale within a workforce. Ultimately, the employer would need to weigh up the potential advantages and disadvantages in deciding whether to permit employees to access social media sites at work. A complete ban would not address the potential problems that could arise from postings by employees outside of working hours. Employers can easily find themselves liable for comments made after hours by employees if there is an obvious and clear link to the employment. Accordingly, comments posted by one employee about another employee after hours on a social networking site could still end up as the responsibility of the employer.
- Put in place a social media policy which deals with the use of social media sites during and outside of work hours. Such a policy should have provisions dealing with social media activity, but in particular:
    - set out the parameters governing the use of the employer's IT systems;
    - remind employees that social media activity may not necessarily be private;

- prohibit discrimination, harassment or bullying of other employees, which could include negative comments about employees posted on social media sites;
- prohibit negative comments about the employer, its employees or third parties; and
- prohibit the disclosure of any confidential information that relates to the employer and/or other employees.

The policy should set out the consequences of a breach of the policy, which could include disciplinary action and, ultimately, dismissal.

- Provide awareness training to employees on conduct that could constitute discrimination, harassment and bullying. An employer would be able to defend any subsequent claim for discrimination or harassment if it can show that it took all reasonable steps to prevent the employee from committing the discriminatory act in question.
- Monitoring the use of social media sites at work could help to determine whether there is a loss of productivity as a result of employees accessing such sites. However, employers may be required to obtain the employees' consent before accessing such information. Legal advice should be sought before engaging in any such monitoring.
- Incorporate within employment contracts an appropriate confidentiality clause, which would afford protection to the employer in the event that an employee posts confidential information on a social media site.
- Disciplinary action may be taken against employees who misuse a social media site to the detriment of the

employer. In some cases, an employer could consider dismissal. Each case will turn on its facts and an employer might want to obtain legal advice before proceeding to dismiss the employee in question.

Contributed by Meer & Hasan

PAKISTAN

PEOPLE'S REPUBLIC OF CHINA

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Unlawful discrimination

Information on social media sites will often contain personal details of the job applicant, which may include the protected attributes under the People's Republic of China (PRC) Labour Law and other employment-related regulations. These protected attributes are nationality, race, sex, religious belief and disability. The PRC Employment Promotion Law further prescribes that, during the recruitment process, discrimination against women, ethnic minorities, disabled people, rural workers or carriers of epidemic pathogens (for example, Hepatitis B) is prohibited. If an employer treats the job applicant/employee less favourably on the grounds of any of the protected attributes above, the job applicant/employee can bring legal proceedings in case of any employment discrimination above.

Infringement of privacy rights

There are no dedicated laws or regulations for the collection, use and handling of personal data of an employee/job applicant in mainland China. However, the right of privacy has been expressly recognised under PRC Tort law as one of the civil rights and interests enjoyed by an individual, infringement of which constitutes an actionable civil tort and may sometimes be viewed as a civil tort of infringing reputation.

In addition, under the Employment Services and Management Regulations, the employer is obliged to keep the applicant's personal data confidential, and has to obtain the employee's written consent before it publicises any such personal data. The law does not specify what information should be considered as "personal data". Generally, any information relating to the applicant should fall within this

category. Therefore, if the employer obtains such information from a social media site and discusses this information among its employees or third parties, it may arguably be regarded as a "publication of personal data". Such publication would be unlawful, unless, of course, the applicant consents to this.

The PRC law does not specify what penalties will be imposed as a result of the employer's infringement of the applicant's privacy rights, as set out above. However, general remedies provided under the PRC Tort law should be available to the job applicant as well, i.e. if the right of privacy of the job applicant has been infringed, he/she may have a right to demand the cessation of such infringement, restoration of reputation, elimination of adverse impact, issuance of an apology and payment of damages (which could include damages to compensate an individual for severe mental distress suffered).

2. What steps can be taken by employers to minimise such risks?

Assuming employers do not wish to take steps to ban the vetting of job applicants using information from social media sites, there are a number of steps which can be taken to minimise the legal risks of using the social media sites to vet a job applicant:

(a) Applicants should be told at the start of the recruitment process that the employer will conduct a vetting exercise using information available on social media sites.

(b) Applicants should be provided with a personal data collection statement, which sets out the arrangements that will be put in place in relation to the collection, use and handling of personal data. For example, employers would only use information that is generally available to the public via the social media site, instead of attempting to gain access through covert means. The employer should comply with the provisions set out in this statement.

(c) An employer should provide guidance and training to employees responsible for vetting job applications, and those scanning social media sites as part of the recruitment process should be instructed to extract only legitimate and relevant information for the job application process.

(d) A social media policy or other written guidelines addressing, amongst other things, the use of social media sites to screen job applicants should be put together, so that the employer can demonstrate an intention to extract only relevant information.

(e) Ideally, the person scanning the social media sites should not be the same as the person who makes the hiring decision. This way, the irrelevant material (which might contain details of protected attributes) will not make its way through to the decision maker.

(f) An employer should put in place and implement an anti-discrimination policy and to conduct training to, amongst others, the employees responsible for the recruitment exercise.

3. What problems could an employer face as a result of employees using social media sites?

(a) *Breach of confidentiality*

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social media platforms, it is possible that an employee may post confidential information about the employer and/or other employees (whether inadvertently or deliberately). This could result in significant damage to the employer's business and reputation.

Popular networking sites in China, such as MSN and QQ, allow an individual to connect online with others whom

they may encounter during their employment (for example, customer contacts and suppliers), and provide the individual with a ready "contact list" or "client list", which may be accessed after the end of their employment. While banning the use of such networking sites might be impractical, an employer should consider whether its legitimate interests could be protected through the use of appropriately worded post-termination restrictive covenants.

(*b*) *Damage to employer's or third party's reputation*

Employees could post information or negative comments on a social media site that causes damage to the reputation of the employer and/or a third party. An employer may be vicariously liable for the defamatory conduct of an employee caused to any third party. The fact that an employer may have a claim against the employee concerned could be of little comfort compared to the damage to the reputation of the employer.

(*c*) *Potential claim for unlawful discrimination and harassment*

An employee could post negative comments about a fellow employee on social media sites. The comments could relate to a protected attribute, such as disability, race or sex. If an employee were to make such comments 'in the course of their employment', and a reasonable person were to be offended, humiliated and intimidated by such comments, there is a danger that such comments could constitute unlawful discrimination and/or harassment under the relevant anti-discrimination laws and regulations. In such circumstances, an employer could be vicariously liable for the actions of that employee.

An employer will not be held vicariously liable for any claim of unlawful discrimination or harassment if it has taken reasonably practicable steps to prevent the employee from committing the relevant act in question.

(*d*) *Loss of productivity*

Aside from the potential legal issues, there could be the obvious negative impact on productivity in the workforce, should an employer permit its employees to access and use social media sites using its equipment during work hours, especially if the employee conducts online activities not related to work.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

An employer can take the following steps:

- Ban access to social media sites at work. This approach is common, in practice, as it is technically practicable and straightforward. However, the approach could prove to be unpopular amongst employees and have an adverse impact on morale within a workforce. Also, a complete ban would not address the potential problems that could arise from postings by employees outside of working hours. Employers can easily find themselves liable for comments made after hours by employees, particularly where there is an obvious and clear link to the employment. Ultimately, the employer would need to weigh up the potential advantages and disadvantages in deciding whether to permit employees to access social media sites at work.
- Put in place a social media policy which deals with the use of social media sites during and outside of work hours. Such a policy should have provisions dealing with social media activity but, in particular:
    - set out the parameters governing the use of the employer's IT systems;
    - remind employees that social media activity may not necessarily be private;

- prohibit discrimination, harassment or bullying of other employees, which could include negative comments about employees posted on social media sites;
- prohibit negative comments about the employer, its employees or third parties; and
- prohibit the disclosure of any confidential information that relates to the employer and/or other employees.

If the employer would like to conduct monitoring of the employees' online activities, this should be made clear to the employees in advance in the policy, and also make clear that personal online activity not related to work is prohibited during work hours.

The policy should set out the consequences of a breach of the policy, which could include disciplinary action and, ultimately, dismissal. However, this policy should avoid being too broad and infringing the rights of employees while outside of work.

- Provide awareness training to employees on conduct that could constitute discrimination, harassment and bullying, as well as what conduct is prohibited on social media sites during working hours. To the extent that one does not already exist, put in place and implement a written anti-discrimination and anti-harassment policy and provide training to the employees. An employer would have a defence to any claim for unlawful discrimination or harassment if it can show that it took all reasonably practicable steps to prevent the employee from committing the discriminatory act in question.
- Monitoring the use of social media sites at work could help to determine whether there is a loss of productivity as a result of employees accessing such sites. However,

it is important to bear in mind that such monitoring may be subject to the infringement of privacy rights of the employees. Legal advice should be sought before engaging in any such monitoring.

- Incorporate within employment contracts an appropriate confidentiality clause, which could afford protection to the employer in the event that an employee posts confidential information on a social media site.
- Consider the use of post-termination restrictive covenants where an employee could build a "client list" of contacts acquired during employment through a networking site (like MSN or QQ) which the employee can subsequently use after cessation of employment.
- Disciplinary action may be taken against an employee who misuses a social media site to the detriment of the employer. In some cases, an employer could consider dismissal. Each case will turn on its facts, and an employer might want to obtain legal advice before proceeding to dismiss the employee in question.

Contributed by JSM Shanghai Representative Office

PRC

PHILIPPINES

1. *Are there any risks for employers that use social media sites to vet job applicants?*

There are currently no laws, rules or regulations in the Philippines which specifically prohibit employers from using social media sites to vet job applicants. However, there are restrictions on the way in which information obtained from these sites can be used. Since social media sites usually contain an individual's personal details, it might yield information that, by law, cannot be considered by the employer in its hiring process.

Unlawful discrimination

The use of social media sites as a source of information is not specifically prohibited by the law of the Philippines. However, what matters is the use of information obtained from said social media sites, and the effect of such in the decision-making process of the employer. Given that social media sites provide a wide spectrum of demographic information (gender, race, age, beliefs, status, disabilities, etc.), using such information could pave the way for allegations of discrimination. It is not unthinkable that an applicant may accuse the employer of using such information to make an adverse employment decision.

Equality of opportunity is enshrined in the Philippine Constitution. The Philippine Labour Code and other special laws therefore contain provisions which prohibit discrimination on the following grounds: sex, race, religion or creed, age, marital status and disability. There are also specific laws concerning an individual's actual or perceived HIV status.

Data Protection

At present, there is no specific and comprehensive law on data protection. However, there is a pending bill in the Philippine Congress which seeks to protect the right of its citizens to

privacy and the confidentiality of their personal information. The bill was approved on third reading by the House of Representatives on March 9, 2011, and was transmitted to the Senate on March 15, 2011. The Senate must pass the bill on third reading before the President may sign it into law. At the time of writing, it is not possible to give an estimate of when this bill will come into law.

House Bill 4115 or the "Data Privacy Act of 2011" aims to establish fair practices and regulations relating to the collection, use and protection of an individual's private information in both private and government information and communications systems. If passed into law, the bill would, among other things, require organisations to: obtain express consent from the data subject to process personal information; establish safeguards to ensure the confidentiality of information; be responsible for transfers of information; and inform the Commission on Information and Communications Technology and any affected individuals in certain events, such as when the information may enable them to identify fraud. The bill seeks to apply to all types of personal information, and will have wide application, including a wide extraterritorial scope.

The Commission will ensure strict compliance with the law, and criminal and civil penalties will be imposed for certain violations of the Act.

Privacy

An individual's right to privacy is protected under the Civil Code of the Philippines. Individuals may have claims for damages or injunctive relief if information obtained on them is used to intrude into, or interfere with, their personal life. In addition, claims could be brought if an individual suffers harassment as a result of this right being breached.

2. *What steps can be taken by employers to minimise such risks?*

Assuming employers do not wish to take steps to ban all vetting of job applicants using information from social media sites, there are a number of steps which can be taken to minimise the legal risks of doing so:

(a) Seek the applicant's written consent for the collection, storage, maintenance, transfer, processing, handling and use of personal information by the company.

(b) Disclose to the applicant that the employer will conduct a vetting exercise using information available on social media sites.

(c) The employer should provide guidelines and training to employees responsible for vetting applicants to ensure that only information that is relevant and necessary for the recruitment process is retrieved.

(d) Access to applicants' personal information files must be limited to authorised officers and agents of the company who are under strict confidentiality obligations to ensure the protection of the applicant's privacy rights, and that information is used only for legitimate business and other lawful purposes.

3. *What problems could an employer face as a result of employees using social media sites?*

(a) Sexual Harassment

Under the Anti-Sexual Harassment Act of 1995, if employees use social media sites to create an intimidating, hostile or offensive working environment for fellow employees, this could amount to unlawful sexual harassment. Employers will be jointly liable, along with the offending employee, for the acts complained of.

(b) Vicarious Liability

If, during the course of their employment, an employee posts comments on a social media site which causes harm to others, for example, by posting hostile or defamatory statements or by revealing confidential information, then the employer could be liable for any damage caused.

Employers will avoid such liability if they can show that they took all care to avoid such damage being caused.

(c) Breach of confidentiality

Use of social media sites may result in disclosure, whether intentionally or unintentionally, of confidential information by employees. Confidential information could cover information about fellow employees, as well as information on suppliers, customers and the employer's trade secrets. Placing this kind of information into the public domain may lead to the employer being liable for damages and in significant damage to the employer's business and goodwill.

(d) Loss of productivity

Aside from the potential legal issues, there could be an obvious negative impact on productivity in the workforce should an employer permit its employees to access and use social media sites using its equipment during work hours. If employees were to spend time browsing social media sites (assuming it is not part of their assigned task) when they are meant to be working, productive hours and company resources are wasted.

(e) Loss of Company Data

There is always the danger that, when employees access third party sites, the employer's system may be infected by malicious software which could damage systems and steal data. Although employers could take action against hackers, this could be of little comfort if their confidential information is already in the public domain.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

An employer can take the following steps:

(a) Total Ban

Impose an outright ban on access to social media sites at work. Social media sites may not be absolutely harmful in the work environment. However, employers may decide that the possible liability and losses it could create far outweigh its benefits.

(b) Be Proactive

Develop a policy regarding the use of social media sites during work hours. It should include rules regarding the collection of data used to make employment decisions and restrictions on employees' access to, and use of, social media sites. Moreover, violation of these policies should be sanctioned, and penalties should be clearly set out in the policy. Policies should be regularly audited and reviewed to keep them up to date and relevant.

(c) Share Knowledge

Inform the employees of the actions which could expose them to liability, i.e. acts of discrimination, libel, or harassment. If employees have already attended seminars regarding these matters, a refresher course may be offered.

(d) Monitor

Monitor the employees' activities in regard to their use of social media sites. In order to do this, employees must be informed that employers have the capability to monitor, and are, in fact, monitoring, their internet usage.

(e) Contractual Provisions

Incorporate an appropriate confidentiality clause into contracts of employment, which could afford protection to the employer in the event that an employee posts confidential information on a social media site. Also include properly worded post-termination restrictive covenants to protect the legitimate interests of the employer.

Contributed by SyCip Salazar Hernadez & Gatmaitan

SINGAPORE

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Right to Privacy/Data Protection

There are, at present, no laws in Singapore that generally prohibit or regulate the collection and subsequent handling of personal data. However, the Singapore government has announced that a Data Protection Act will be drafted. This is expected to be implemented in 2012. According to a statement by the Singapore Government, the Data Protection Act would seek to "curb excessive and unnecessary collection of individual's personal data by businesses, and include requirements such as obtaining the consent of individuals to disclose their personal information". In addition, there are some current rules that employers need to be aware of.

The Computer Misuse Act ("CMA") prohibits the unauthorised interception of computer communications and unauthorised access to data. "Data" is defined by the CMA as "representations of information or of concepts that are being prepared, or have been prepared, in a form suitable for use in a computer". This is a very wide definition of "data", and is intended to capture a wide spectrum of computer-related information so as to avoid abuse by alleged offenders claiming that certain information and/or concepts do not constitute data. Nevertheless, case law in Singapore has provided various examples of what constitutes "data" under the CMA. This includes emails, information stored in computers, data stored in servers and credit card data. Unauthorised access to data is punishable under the CMA by imprisonment, a fine, or both.

Therefore, under the CMA, information that is uploaded onto social media sites such as Facebook and Twitter may contain "data" or may itself be considered as "data" under the CMA. This "data" cannot be accessed without permission. However, the data and information uploaded on such social media sites is generally done voluntarily. Further, the job applicant has

the option to adjust his privacy settings and decide which information is to be publicly viewable and which information is to be private. As a result, any information placed on social media sites, that is publicly viewable, or to which the employer has been given specific access, can arguably be used for vetting that job applicant.

The National Internet Advisory Committee ("NIAC") issued a Model Data Protection Code ("MDPC") for the Private Sector in December 2002. However, this is only a guide to the kind of behaviour that is expected from employers and is not mandatory.

Unlawful discrimination

The Singapore Constitution prohibits any discrimination against Singapore citizens on the basis of religion, race, descent, or place of birth. Since social media sites often contain information on applicants that includes such details, using social media to determine whether or not to employ someone may open the door for allegations of discrimination against the employer. Employers should, therefore, ensure that information from social media sites is not used in a discriminatory way. There are also provisions in the Singapore Penal Code that extend protection to all individuals, regardless of origin.

2. *What steps can be taken by employers to minimise the risks set out under Question 1 above?*

Employers who wish to vet job applicants using information from social media sites should follow the guidelines below:

(a) Employers should only use information that is publicly available. In other words, employers should not use spyware, back doors, viruses, worms, spam, Trojans, fake accounts and/or any other misleading or hidden programs, malicious code or software to retrieve

information that has not been made public by the employee on the social media sites.

(b) The person charged with collecting the information should be provided with adequate training to help them differentiate between information that is legitimate and relevant from that which is irrelevant and/or has been obtained via any of the methods set out in (a) above. This can be done by introducing a "Social Media Policy", which sets out guidelines for employees who collect such information. These guidelines may include information on data protection and anti-discrimination laws of Singapore. Further details of what should be included in such a policy are set out below.

(c) It is recommended that the person collecting and extracting the information and the decision maker be different individuals. This is to ensure that if any of the information collected is irrelevant, or is not legitimate for its purpose, then it will not influence the decision maker.

(d) Although not a strict requirement, applicants should ideally be notified that any publicly available information about them, including that on social media sites, may be used by the employer in making a decision about whether to employ them.

(e) Employers should remain abreast of legal developments to ensure that their practices remain compliant with the changing regulatory landscape.

3. What problems could an employer face as a result of employees using social media sites?

Breach of Confidentiality

The internet provides an outlet for individuals to freely share their thoughts and other information. There is no real barrier

to the sharing of information on the internet. However, employees using social media could inadvertently disclose sensitive data they receive in the course of employment, which could include data relating to customers.

Apart from disclosing confidential information relating to the employer's customers, an employee might also disclose critical business information relating to his employer on the various social media sites. Such information could include trade secrets, customer lists or highly sensitive technical specifications. This critical information could be crucial, and its disclosure may be detrimental, to the running of the business, especially if such information falls into the hands of a competitor.

Unauthorised Access

Apart from the risk of disclosure of confidential information, the company might also face the risk of unauthorised third party access to the company's computer systems. When an employee logs onto a social media website, there is the possibility of an unauthorised third party gaining access into the company's computer system if the company fails to put up adequate firewalls. This might result in certain critical information of the company being leaked into the public sphere, or might even result in the introduction of spywares, viruses, worms, spam or Trojans onto the company's computer systems. Given the high dependence of a modern-day company on its computer systems, any malicious software that cripples the entire system would naturally have a detrimental effect on the functioning of the company.

Potential Lawsuits

While the internet allows an employee's personal views and opinions on any subject matter to be shared, if an employee makes disparaging comments, and suggests that the comments are made on behalf of his employer, the employer

could also potentially be held liable for those comments and subjected to a defamation suit.

In addition to possible defamation suits, a company may also be held vicariously liable for the conduct of its employees on other grounds. For example, if an employee gives out advice, or expresses views or opinions that are misleading or are negligently made, and if it appears that these views and/or opinions are expressed on behalf of the employer, the employer could be held liable for any resulting damages. This would not only have a negative impact on the financial position of the company, but also on the overall reputation of the company.

An employer may be able to escape liability under such claims if he can show that the employee was not acting in the course of his employment, i.e. the employee's actions were not within the employee's express, implied or ostensible authority.

Harassment in the Workplace

An employee using social media may cause distress to a fellow employee by using threatening words or behaviours and/or making and displaying offensive visible representations against a fellow employee on such sites. For example, an employee may send suggestive messages or pictures to a fellow employee via Facebook or Twitter. Case law suggests that such behaviour by co-workers could lead to a civil claim against the employer on grounds that the employer has breached his duty to provide a safe working environment for its employees.

However, an employer may institute various practices to protect himself against such claims. Such practices may include, amongst others, a grievance policy whereby an employee can institute a complaint against her co-worker and/or against her superior, and a policy to dismiss employees who are found to have harassed their co-workers. Generally, upon receiving a complaint, the employer should carry out an

investigation and take any action that it deems necessary to resolve the situation.

Loss of Productivity and Efficiency

There is also a negative impact on the productivity of employees who use social media while at work. An employee who is frequently surfing social media sites is likely to have a reduced level of performance. Although a company may be able to terminate the employee for failing to meet his key performance indicators (subject to the terms of the employee's contract of service), the company will still suffer as business targets may not be met.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

Given the various risks involved, an employer could impose an outright ban on the use of all social media sites at work. However, such a move may have a negative impact on employees' morale. More importantly, the employer will itself be unable to capitalise on the advantages of social media sites, for example, by reaching out to a far wider audience than otherwise possible.

Apart from using personal computers and desktops, employees may still access social media like Facebook or Twitter on their handheld devices, notwithstanding that such devices are given to the employee so that they are readily contactable and able to carry out tasks efficiently. Again, while an employer may be able to impose an outright ban on the use of social media on such devices, it not likely to be a popular move. Further, given that technology is continually evolving, it is nearly impossible for a company to cover all bases if it attempts to impose such a ban. Instead, an employer should ensure that he has the right to monitor an employee's use of social media and that the employees are well aware that such monitoring takes place.

Further, employers will be unable to control what employees do in their free time once they leave work. An employee may still post comments, give out advice and share confidential information that he receives at work. The fact that such comments, advice and/or confidential information are posted outside work hours, and using personal electronic devices, does not remove the risk of claims or lawsuits against the company, especially if the employee concerned is seen as a representative of the company.

Therefore, rather than imposing an outright ban, employers can minimise the risks involved by evaluating the issues and adopting and implementing a Social Media Policy ("Policy") that is appropriate to their particular business and is customised to their particular circumstances. The Policy should be one that guides employees in the use of social media sites. This Policy could inform employees of the consequences of improper use of social media, both at work and after work, and also inform employees of the scope of activities that they can engage in, especially if they are seen as representing the employer. To ensure that employees comply with the Policy, it is important for the Policy to be communicated to all employees. It should also be explained that a failure to comply with the Policy could potentially result in disciplinary action, including termination of employment.

Some examples of the terms that could be included in the Policy are as follows:

(a) Employees are personally responsible for the content that they publish online, whether in a social media website or blog.

(b) Employees must provide their name and role when discussing matters related to the employer, including opinions about the employer's products and services.

(c) If employees provide opinions relevant to their work or to the employer, the employee should always add a disclaimer or seek prior written authorisation from the employer.

(d) The employee must not, at any time, disclose any confidential and/or proprietary information, including, but not limited to, the employer's business targets and customer lists.

(e) Employees should not make any reference to other employees on such social media sites with respect to race or religion, or use personal insults, obscenity, or engage in any conduct that would be seen as unacceptable in the workplace. All employees should respect the rights of their fellow colleagues.

(f) Employees should be prohibited from using the company's marks, logos or other insignia, unless specifically authorised to do so.

Apart from the above terms, the Policy could also inform employees of the personal risks involved when they fail to adhere to the Policy, including the fact that the employee concerned is legally responsible for his use of social media and that he may be subjected to liability if his use is in violation of any applicable law. Apart from the legal repercussions, the employer should also inform its employees that a violation of the Policy should result in disciplinary action, up to and including termination of employment.

It is recommended that employers provide training for employees on the appropriate use of social media sites at work and advise employees of the risks involved when employees do not use social media responsibly.

Contributed by Rajah & Tann

SOUTH KOREA

1. *Are there any risks for employers that use social media sites to vet job applicants?*

While there are general laws in South Korea intended to protect the personal data privacy of individuals, the mere use of information that is already provided on social media sites to vet job applicants does not appear to trigger any significant risks to the employer, particularly if the provision of the information on the social media sites is deemed to be with the consent of the applicant. This assumes that the use of the information by the employer is in accordance with South Korea's anti-discrimination laws.

2. *What steps can be taken by employers to minimise such risks?*

Notwithstanding the foregoing, to the extent that an applicant may reasonably argue that his/her personal data privacy right has been violated by an employer's use of social media sites to vet his/her application, the following steps can be taken to minimise any such risk:

(a) Applicants should be told at the start of the recruitment process that the employer will conduct a vetting exercise using information available on social media sites.

(b) Applicants should be provided with a personal data collection statement which sets out the arrangement on the collection, use and handling of personal data. The employer should comply with the provisions in the statement.

(c) An employer should provide guidelines and training to employees responsible for vetting the application using information on the social media sites to ensure that only relevant and necessary information for the recruitment process will be retrieved. Those scanning social media sites as part of the recruitment process should be instructed to extract only legitimate and relevant information for the job application process.

(d) A social media policy or other written guidelines should back this up, so that the employer can demonstrate an intention to extract only relevant information.

(e) Ideally, the person scanning the social media sites should not be the same as the person who makes the hiring decision. This way, the irrelevant material (which might contain details of protected attributes) will not make its way through to the decision maker.

(f) An employer should put in place and implement an anti-discrimination policy and to conduct training to, among others, the employees responsible for the recruitment exercise.

3. *What problems could an employer face as a result of employees using social media sites?*

(a) *Breach of confidentiality and post termination restrictive covenants*

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social media platforms, it is possible that an employee may post confidential information about the employer and/or other employees (whether inadvertently or deliberately). This could result in significant damage to the employer's business and reputation.

Networking sites such as LinkedIn allow an individual to connect online with others whom they may encounter during employment (e.g. customer contacts and suppliers), and provide the individual with a ready "contact list" or "client list" which may be accessed after cessation of employment. While banning the use of such networking sites might be impractical, an employer should consider whether its legitimate interests could be protected through the use of appropriately worded post-termination restrictive covenants.

(*b*) *Damage to employer's or third party's reputation*

Employees could post information on a social media site that causes damage to the reputation of the employer and/or a third party. An employer may be vicariously liable for the defamatory conduct of an employee. The fact that an employer may have a claim against the employee concerned could be of little comfort compared to the damage to the reputation of the employer.

(*c*) *Potential claim for unlawful discrimination and harassment*

An employee could post negative comments about a fellow employee on social media sites. The comments could relate to a protected attribute, such as disability, race or sex. If an employee were to make such comments 'in the course of their employment' and a reasonable person would be offended, humiliated and intimidated by such comments, there is a danger that such comments could constitute unlawful harassment under the relevant anti-discrimination laws in Korea. In such circumstances, an employer could be vicariously liable for the actions of that employee.

If an employer permits access to social media sites using work equipment and systems during work hours, and the conduct took place in the workplace such as to create a hostile or intimidating work environment, this could amount to unlawful sexual harassment or other types of harassment (as the case may be).

An employer could also risk facing other discrimination claims if employees use information they have obtained from social media sites about other employees relating to a protected attribute as the basis for treating them in a detrimental way.

An employer will not be held vicariously liable for any claim of unlawful discrimination or harassment if it has taken reasonably practicable steps to prevent the employee from committing the relevant act in question.

(*d*) *Loss of productivity*

Aside from the potential legal issues, there could be the obvious negative impact on productivity in the workforce should an employer permit its employees to access and use social media sites using its equipment during work hours. Loss of productivity may also arise from the potential technical hazards of allowing access to social media sites such as viruses, hacking, system crashes, and phishing attacks.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

An employer can take the following steps:

(a) Impose an outright ban on access to social media sites at work. This approach could prove to be unpopular amongst employees and have an adverse impact on the morale within a workforce. Ultimately, the employer would need to weigh up the potential advantages and disadvantages in deciding whether to permit employees to access social media sites at work. A complete ban would not address the potential problems that could arise from postings by employees outside of working hours. Employers can easily find themselves liable for comments made after hours by employees, particularly where there is an obvious and clear link to the employment. Accordingly, comments posted by one employee about another employee after hours on a social networking site could still end up as the responsibility of the employer.

(b) Put in place a social media policy which deals with the use of social media sites during and outside of work hours. Such a policy should have provisions dealing with social media activity but, in particular:

- set out the parameters governing the use of the employer's IT systems;

- remind employees that social media activity may not necessarily be private;
- prohibit discrimination, harassment or bullying of other employees, which could include negative comments about employees posted on social media sites;
- prohibit negative comments about the employer, its employees or third parties; and
- prohibit the disclosure of any confidential information that relates to the employer and/or other employees.

The policy should set out the consequences of a breach of the policy, which could include disciplinary action and, ultimately, dismissal.

(c) Provide awareness training to employees on conduct that could constitute discrimination, harassment and bullying. To the extent that one does not already exist, put in place, and implement, a written anti-discrimination and anti-harassment policy, and provide training to employees (in South Korea, sexual harassment prevention training is required annually). An employer would have a defence to any claim for unlawful discrimination or harassment if it can show that it took all reasonably practicable steps to prevent the employee from committing the discriminatory act in question.

(d) Monitoring the use of social media sites at work could help to determine whether there is a loss of productivity as a result of employees accessing such sites. However, it is important to bear in mind that such monitoring may be subject to data privacy protections in South Korea. Legal advice should be sought before engaging in any such monitoring.

(e) Incorporate within employment contracts an appropriate confidentiality clause, which could afford protection to the employer in the event that an employee posts confidential information on a social media site.

(f) Consider the use of post-termination restrictive covenants where an employee could build a "client list" of contacts acquired during employment through a networking site (like LinkedIn) which the employee can subsequently use after cessation of employment.

(g) Disciplinary action may be taken against an employee who misuses a social media site to the detriment of the employer. Depending on the degree of the misuse, an employer could consider dismissal. Each case will turn on its facts, and an employer might want to obtain legal advice before proceeding to dismiss the employee in question.

Contributed by Kim & Chang

SRI LANKA

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Unlawful discrimination

There is no general anti-discrimination legislation in Sri Lanka. There is, however, legislation in place which makes it a criminal offence for any person to impose a social disability on another person by reason of their caste. A person will be deemed to have imposed a social disability on another if he or she prevents that person from being employed as a teacher in any educational institution, or being engaged in any lawful employment or activity, because of that person's caste. When vetting/interviewing job applicants, an employer should not ask any questions about a prospective employee's caste. Where a claim is brought under this legislation, it will be presumed that a social disability was imposed by reason of a person's caste, and the burden of proof shall lie on the person charged.

There is provision in the Sri Lankan Constitution which prohibits discrimination of a citizen on the grounds of race, religion, language, caste, sex, political opinion, place of birth or any such grounds. While this fundamental right can be enforced in relation to actions taken by the State or any of its organs, the same remedy is not available to a prospective employee/an employee where the prospective employer/employer has acted contrary to that provision (provided the employer is not the State or a State entity/organ).

Therefore, provided employers do not discriminate on the basis of an applicant's caste, there is no risk for an employer in using social media sites to vet job applicants. Obviously, from a reputational risk point of view, an employment decision should not be based on one or more overtly discriminatory grounds.

Data Protection

There is no general legislation regulating the collection/use/storage of personal data in Sri Lanka. Therefore, there is nothing to restrict an employer from collecting personal information/data about a job applicant from social media sites as part of the job application process.

2. *What steps can be taken by employers to minimise such risks?*

In view of the legal position set out in the answer to question 1 above, it is not necessary for employers to take any steps to minimise the risks which arise as a result of using social media sites to vet job applicants, as these are minimal. However, from a reputational point of view, it would obviously be in an employer's best interest not to engage in any discriminatory conduct and to have in place clear guidelines as to what type of information can be gathered from social media websites, how that information is to be used and for what purposes.

3. *What problems could an employer face as a result of employees using social media sites?*

There are numerous problems which may arise from an employee's use/misuse of social media sites. For the employer, such problems include:

- risk of reputational damage in the event that an employee posts material, whether true or not, which is damaging to the reputation of the employee/employer;
- risk that an employee may disclose confidential information about the employer and/or his or her co-employees;
- risk that employees whose contracts of employment are terminated can easily access customers/clients of the business through the contacts they have made during the course of their employment and with whom, for

example, they are connected on a social media website, like "LinkedIn";

- arguably, an employee could claim that his/her employment contract has been constructively terminated if their employer or co-workers have used social media sites in such a way that it has become intolerable for the employee to continue in employment. The employee may seek relief from a Labour Tribunal or other labour law mechanism to obtain an order for payment of compensation/other relief; and
- loss of productivity among the workforce.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

An employer has the choice of several measures which could be taken to minimise the risks, including the following:

- prohibit employees from accessing social media sites during working hours and/or from using IT systems/ equipment provided/owned by the employer for personal use. Attempts could be made to regulate use of social media outside the workplace, in so far as references to the employer/other employees are concerned, by having employees sign up to appropriate policies governing the use of social media;
- allow employees to access social media sites during working hours and/or use of the employer's IT systems/ equipment provided/owned by the employer, but have employees sign up to a social media policy which regulates the use of social media sites, both during and outside of work hours. Such a policy would have to be carefully worded to address the risks referred to in 3 above and clearly set out the consequences of a breach of the policy, which could include disciplinary action and, ultimately, termination of employment. It should,

however, be borne in mind that, in Sri Lanka, it is quite possible that if an employee's contract was terminated for breaching a social media policy, and the employee sought relief from a Labour Tribunal or through another labour law mechanism, the seriousness of the breach may be viewed completely differently by the Tribunal (or other authority) to the view taken by the employer. The Tribunal might hold that, in the interests of justice and equity, the employee should be reinstated with back wages or paid compensation. Labour Tribunals can disregard the provisions in any contract of employment, and this would arguably also include a social media policy;

- address issues such as undesirable conduct on social media sites which, though not unlawful, could lead to reputational damage, by having wording which regulates conduct in the contract of employment and/or by training employees on the standards expected;
- monitor the use of social media by employees and evaluate the impact on productivity; and
- include confidentiality clauses in contracts of employment as well as restrictive covenants to address the danger of misuse of customer/client lists and to prevent employees posting confidential information on social media websites.

Contributed by John Wilson Partners

TAIWAN

1. *Are there any risks for employers that use social media sites to vet job applicants?*

There is an increasing trend for employers and their human resource teams to vet job applicants using the Internet ("Cyber Vetting") as part of their recruitment process. The recent boom of social media, such as Facebook, LinkedIn and Twitter" has provided an even more effective avenue for employers to access information regarding job applicants, allowing employers to obtain extensive personal data in an integrated fashion.

While Cyber Vetting provides an effective means for employers to recruit suitable employees and avoid recruitment mistakes, it also exposes employers to potential legal risks under the following two heads: (1) discrimination; and (2) personal data protection.

Discrimination

Under Taiwan's Constitution and employment law, it is prohibited to discriminate against employees or prospective employees on the basis of any characteristic that is not relevant to their role. Employers are prohibited from discriminating against job applicants or existing employees on the basis of: race; class; language; thought; religion; political party; place of origin; place of birth; gender; gender reassignment; sexual orientation; age; marital status; appearance; facial features; disability; or past membership in any labour union.

Given that the types of information found on social networking sites are those which could be easily used as a basis for unlawful discrimination, Cyber Vetting may create the perception that employers have an improper motive in collecting such information, and thereby give employees or job applicants a basis on which to bring claims for unlawful discrimination. In cases where the governing authority, the Council of Labour Affairs, finds the employer to have

unlawfully discriminated against employees or job applicants, a penalty of NT$600,000 to $1,500,000 may be imposed.

Personal Data Protection

As Internet privacy has become an increasingly crucial concern for individuals, it has also become a critical issue for employers who vet their potential employees using social media.

In Taiwan, the primary law governing personal data protection is currently the Computer-Processed Personal Data Protection Act (the "CPDPA"), which is extremely limited in scope. However, on April 27, 2010, the Legislative Yuan of Taiwan passed the Personal Data Protection Act (the "PDPA"). This amends and renames the CPDPA, and widens the legal protection given to personal data to cover all persons (including government agencies, individuals, legal entities, and other groups) and all personal data processed by any means. The PDPA may come into force as early as the end of 2011, and employers should therefore ensure that they use the PDPA as their benchmark for compliance.

In summary, the PDPA provides that personal data can only be collected and used for specific, legitimate purposes and with the informed, written consent of the individual concerned. There are stricter rules in respect of data that is classified as 'sensitive personal data'. This includes information on, among other things, an individual's health, sex life and criminal record, which may not be collected unless: (1) the law explicitly provides otherwise; (2) the sensitive personal data has been made known to the public by the individual or has been disclosed in accordance with the relevant law; and (3) the sensitive personal data is collected, processed or used out of the necessity to perform statutory obligations, and appropriate safe guards have been put in place for the protection of the data.

The fact that personal data found on social media sites could be considered to be publically available does not mean that it is excluded from the scope of the PDPA.

Failure to comply with the PDPA could lead to civil or criminal liability on the part of the employer, as well as fines being imposed by the relevant authority. The enforcement body varies for each industry.

The volume of information available on social media sites could present a problem for employers attempting to comply with their obligations under the PDPA. It would be easy for irrelevant or excessive information to be collected which would violate the requirement that data only be collected and used for specified purposes.

2. What steps can be taken by employers to minimise such risks?

To fully embrace the advantage of Cyber Vetting and minimise its legal risks, employers should put in place clear and unambiguous Cyber Vetting guidelines, which may include the following:

1. Job applicants should be informed in advance that Cyber Vetting will be carried out, and their prior written consent to this should be obtained. There is set information that should be provided to applicants for their consent to be valid, including being informed how their data will be used.

2. To avoid claims of unlawful discrimination, the following guidelines should be enforced:

   (a) Only information that is relevant to the job applicant's suitability for the role they have applied for should be collected and used.

   (b) The recruitment process should be carefully documented.

(c) Applicants should be provided with feedback regarding the recruitment process, setting out why their application has been accepted or rejected. This could minimise the risk of a claim for unlawful discrimination.

(d) The recruitment team should receive training on the employer's anti-discrimination policy, and how to carry out the recruitment process in a non-discriminatory way.

3. Job applicants should be provided with the opportunity to correct personal data collected from social media sites to ensure accuracy.

3. *What problems could an employer face as a result of employees using social media sites?*

Social media is now ubiquitous. Further, as employees often include the name of their employer in their social media profiles, not only would the employee outwardly become an "ambassador" of the employer, from a legal perspective, the employee could also be considered as acting on behalf of the employer. As a result, the employer may, in some circumstances, be jointly liable for the employee's conduct.

While social media could be beneficial to the employers, they could also, therefore, become a liability if employees use them in such a way as to harass co-workers, tarnish the employer's brand, or leak confidential information and trade secrets.

Disclosure of Confidential Information

Most people view social media as a platform for sharing information that is transitory and informal. This lack of awareness in using social media could lead to the unintentional leakage of personal or confidential business information, either of the employer itself or of its external clients. The problem could be made worse if an employee

intentionally uses social media as a platform to disseminate confidential information, as information can be spread very rapidly and effectively, using these sites.

Consequently, the use of social media in the workplace could expose the employee to civil and criminal actions, including breach of confidentiality, defamation lawsuits, and intellectual property infringement claims, among others.

Liability for Harassment

Under Taiwan's employment laws, employers have a duty to maintain a safe and harassment-free workplace. When an employee suffers damage because of the actions of a fellow employee, their employer can be jointly liable if the offending acts are carried out in the performance of the employee's duties. Employers will only escape such liability where they can show that they took all steps to prevent such behaviour from occurring. Vicarious liability can arise whether or not the acts complained of actually took place at work.

Damage to Reputation

As a new type of platform for employees to gather and socialise with each other, as compared to other social platforms, social media has a louder volume and broader audience. Consequently, minor complaints or emotional language made by an employee can now be very detrimental to the reputation of the employers and/or even their clients.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

Employers should develop a practical and enforceable social media policy through consultation with employment and data protection lawyers. This should set out details of the behaviour expected from employees when using social media, both inside and outside the workplace, and should include clauses that:

(a) clearly define social media for the purpose of specifying the scope of the policy;

(b) prohibit discrimination, harassment or bullying of fellow employees, including negative comments posted on social media sites;

(c) make it clear to employees that they are not free to post comments or reveal information that will harm the employer's business and reputation;

(d) prohibit the use of employer's trademarks, logos, and other similar business symbols on personal pages on social media sites. If necessary, employees could be advised or required to insert a disclaimer on their social media web pages stating that any opinions expressed are those of the employee and do not represent the opinions of the employer;

(e) set forth the consequences for employees if they fail to abide by the policy, including damage claims, penalties and/or even termination of employment.

In addition to this, employers should:

(a) create a reporting system and grievance channel for employees to report possible violations of the duty of confidentiality and file possible harassment complaints;

(b) maintain a secure IT system with the aim of preventing data leakage and to monitor the online activities of employees. Before any monitoring can take place, prior consent should be obtained from the employees concerned. Employers should also be careful to comply with data protection laws when conducting monitoring of employees' internet usage;

(c) train employees on appropriate behaviour when using social media, and ensure that employees understand the potential impact of misuse of such sites;

(d) take appropriate steps on termination of employment to remind employees of their continuing obligation of confidentiality and any relevant non-solicitation duties which apply to the employee.

Contributed by Lee, Tsai & Partners

TAIWAN

THAILAND

1. *Are there any risks for employers that use social media sites to vet job applicants?*

(a) *General right to Privacy*

Thailand's 2007 Constitution protects a person's family rights, dignity, reputation, and right to privacy, and also provides for the protection of individuals' personal data. Theoretically, an employer's use of information gathered from social media sites may violate these 'rights'. However, very little has yet been done in the way of statute to implement these Constitutional aspirations.

(b) *The Personal Data Protection Bill ("PDPB")*

The PDPB has been under consideration for a number of years and, at the time of writing, no date has been set for it to come into force. Based on the last version reviewed, it would establish a comprehensive data protection regime, which would have broad applicability across virtually all sectors, including employment (and applying to both current employment relationships and potential employment relationships).

The PDPB would provide a wronged applicant various means of redress, including civil actions, criminal actions, and administrative complaints. However, for now, these concerns are merely theoretical, as the PDPB has not yet been enacted.

(c) *Unlawful discrimination*

Social media sites typically contain personal information on job applicants, which may include information on which it would be inappropriate for employers to make employment decisions. The 2007 Constitution prohibits unjust discrimination against a person on the grounds of difference in origin, race, language, sex, age, disability, physical or health condition, personal status, economic or social standing, religious belief, education or political views. An employer who

makes an employment decision on the basis of one or more of these factors might be engaging in unlawful discrimination. However, the reality is that such a claim would be very unlikely, particularly given that there are no provisions of labour law which implement this aspiration. In addition, some laws actually have the effect of requiring discrimination in certain of these categories.

2. *What steps can be taken by employers to minimise such risks?*

As noted, the concerns in this area are, at present, largely theoretical, although there is a very small risk of a successful claim. Indeed, many HR experts are likely to advocate employers' use of social media sites in making hiring decisions, and would recommend it as a sensible policy. Nevertheless, when the PDPB becomes law, and if other new labour laws are enacted, it will be necessary to revisit this issue.

3. *What problems could an employer face as a result of employees using social media sites?*

(a) *Release of confidential information*

Employees using social media sites may intentionally or inadvertently post information and/or images which contain confidential information relating to the employer or to a third party. If the released confidential information relates to a business partner and is protected by a non-disclosure agreement, this may damage the business relationship, and could potentially result in a claim for damages against the employer.

(b) *Damage to employer's reputation*

Employees using social media sites may intentionally or inadvertently post information and/or images which reflect poorly on the employer, for example, photographs of inebriated staff at the office New Year party, or perhaps

'status updates' containing complaints about the employer. Given that employees may add business partners (or even customers) to their 'friend lists', this information may reach precisely the wrong people. Moreover, since many social media sites allow users to display their employment details, viewers of a user's profile may recognise that a particular user works for a particular employer, and the user's online persona may have some impact on viewers' opinions of the employer.

(*c*) *Claims for defamation*

There is also a risk that an employee's post could defame a third party. If the subject matter of the defamatory comment is sufficiently linked to the employee's work (for example, saying that the employer's main competitors are a bunch of frauds), then the employer may be liable for that comment. The risk to the employer would increase with the level of the employee's position, and the extent to which the comments are linked to the employee's work, as these factors may indicate that the employee was speaking on behalf of the employer, rather than in the employee's personal capacity.

(*d*) *Employee issues*

An employee's posted photos and/or updates may produce a negative reaction in other employees. This may lead to confrontation and bickering, as well as a loss of esprit de corps. However, it is unlikely that a successful claim could be brought against an employer as a result of acts of harassment committed by its employees, unless it can be shown that the employer was somehow complicit in the harassment.

(*e*) *Loss of productivity*

Though some employers expect employees to use social media sites in doing their work (e.g. marketing personnel), others are concerned about the drain on employee productivity. This concern often arises with respect to employees who are paid by the hour.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

(a) *Ban access*

Often, employers attempt to impose bans on access to social media sites during work hours. Though employers can set access controls for work computers, these bans are becoming less effective, given the prevalence of personal smart phones that can access the Internet. Indeed, smart phones are fast becoming the primary means of access to social media sites for many users. In addition to their lack of effectiveness, access bans can also be problematic because employees often react negatively to such restrictions, feeling that they are being treated like children or are being micro-managed. Moreover, this approach would certainly not work in situations in which employees were expected to use social media sites for work, e.g. employees who work in public relations or marketing. In this regard, if some employees are allowed to access social media sites, and others are not, an employer could be opening itself to claims for unfair employment practices.

(b) *Amend Work Rules*

Some employers may choose to amend their Work Rules (as registered with the Ministry of Labour) to provide clear standards for employees as to what is acceptable conduct and what is not, when using social media. Though some employers craft rules to only apply during work hours, some opt for more comprehensive rules that would purport to also apply outside work hours, and even outside the workplace. In any case, it is important that the Work Rules clearly describe the prohibited conduct, and also clearly state the disciplinary actions that could apply if the rules are violated.

Depending on the type of business, the employer could consider amending the Work Rules to establish:

- rules on employees' personal use of the employer's IT systems (possibly including an outright ban on the use of social media sites);
- rules on personal mobile phone usage during work hours;
- a prohibition on releasing confidential information, and information on who to ask, if an employee is unsure whether or not something constitutes confidential information;
- a prohibition on negative comments about the employer, its employees, and any third parties; and/or
- an outright ban on mentioning the employer's name on social media sites.

Should the employer ever need to enforce such a policy, it will be necessary to do so fairly, so as to avoid claims for unfair employment practices.

(*c*) *Monitor usage*

Many employers opt to monitor employee usage of the employer's IT systems and equipment. The information generated can be helpful in keeping the employer aware of employee concerns and issues, and is also useful when building evidence in advance of a potential termination. However, employee consent should be sought before initiating monitoring activities. Aside from the legal reasons for doing this, it is also beneficial in that it puts employees on notice that their online activities will be monitored, and this often results in moderation of personal use habits.

(*d*) *Restrictive covenants*

Surprisingly, many employers fail to include contractual provisions in employment agreements that impose obligations of confidentiality on employees. As such, these employers

should amend their employees' employment agreements to include restrictive covenants on confidentiality, and these clauses should be drafted to apply both during and after the employment. Also, depending on the type of employer, consideration should be given to including restrictive covenants on non-solicitation and non-competition.

Contributed by Tilleke & Gibbins

VIETNAM

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Unlawful discrimination

The labour laws of Vietnam prohibit any act of discrimination based on a person's sex, race, social status, belief or religion. An employer who treats a job candidate less favourably on the grounds of any of these protected attributes would be guilty of unlawful discrimination. An employer's use of social media sites to vet job applicants would entail a potential risk that the employer might infringe the prohibitions against unlawful discrimination if the sites contain personal details of the job applicant which are protected from discrimination.

Potential implications under the Civil Code

Under the Civil Code, an individual must consent to the collection, use and publication of private information which identifies them as an individual. There is no definition of what constitutes private information or data. It would therefore be for the courts to interpret.

Information on social media websites will most likely contain personal data relating to the job applicant. As such, where an employer collects this information for the purpose of vetting a job applicant, this collection, and subsequent handling of the personal data, will require the job applicant's consent.

2. *What steps can be taken by employers to minimise such risks?*

To avoid infringing the applicant's privacy, an employer should obtain their written consent to collect, use and publish his/her private information and data before they start reviewing social media websites. A similar measure is required in respect of collection, use and publication of private information from such forums in relation to employees.

3. *What problems could an employer face as a result of employees using social media sites?*

Breach of confidentiality or the right to privacy

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social media platforms, it is possible that an employee may post confidential information about the employer and/or other employees (whether inadvertently or deliberately). This could result in significant damage to the employer's business and reputation or infringement of the right to privacy as provided by the Civil Code.

Damage to employer's or third party's reputation

Employees could post information on a social media site that causes damage to the reputation of the employer and/or a third party. An employer may be vicariously liable for the defamatory conduct of an employee. The fact that an employer may have a claim against the employee concerned could be little comfort, compared to the damage to the reputation of the employer.

Sanctions imposed by the State

If an employee accesses a prohibited site and/or makes any statement against the State of Vietnam, the Communist Party or its leaders, the employee would be subject to a sanction imposed by the State. The employer would also encounter problems due to the employee's act, e.g. they could be questioned or subjected to an interview or check by a state agency.

Unlawful discrimination

It is not uncommon for employees to post negative comments about fellow employees on social media sites. The comments could relate to a protected characteristic such as sex, race or

religion. The risk that the employer is liable for the actions of the employee is remote. However, the employer could be questioned by the court if an employee brings a lawsuit against an employee who has made negative comments about him/her.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

An employer can take the following steps:

(a) Impose an outright ban on access to social media sites at work and impose penalties such as disciplinary measures on employees who breach this ban. Ideally, details of the ban should be incorporated in the internal labour regulations, which will be registered with the labour authority to give them legal effect. The internal labour regulations should, among others, include the rules on how to use social media sites, prohibitions and the consequence of a breach.

(b) Put in place a social media policy which deals with the use of social media sites during and outside of work hours. Such a policy should have provisions dealing with social media activity but, in particular:

- set out the parameters governing the use of the employer's IT systems;
- remind employees that social media activity may not necessarily be private;
- prohibit discrimination or bullying of other employees, which could include negative comments about employees posted on social media sites;
- prohibit negative comments about the employer, its employees or third parties; and

- prohibit the disclosure of any confidential information that relates to the employer and/or other employees.

The policy should set out the consequences of a breach of the policy, which could include disciplinary action and, ultimately, dismissal.

(c) Employees should receive regular training on the employer's policies relating to the protection of privacy, discrimination, harassment and the use of social media sites.

(d) If possible, it is advisable to use a firewall to prevent employees accessing and using prohibited sites.

(e) Incorporate within employment contracts an appropriate confidentiality clause, which could afford protection to the employer in the event that an employee posts confidential information on a social media site.

Contributed by Mayer Brown JSM (Vietnam)

EMEA

ANGOLA

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Yes. Employers risk unlawfully discriminating against an applicant if they use information related to a protected characteristic which they have taken from a social media site as the basis for refusing employment.

2. *What steps can be taken by employers to minimise such risks?*

- The information which an employer takes from a social media site must be publicly available.
- Only relevant information should be extracted.
- A social media policy should be produced.
- Advise applicants that social media sites are reviewed.
- The applicant should confirm the content of any relevant information extracted.

3. *What problems could an employer face as a result of employees using social media sites?*

Employees using social media sites could breach confidentiality and cause damage to the employer's or a third party's reputation. An employer could also be liable for discriminatory comments made by one employee against another in the course of their employment.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

- Inform employees that their use of social media sites will be monitored.
- Ban access to social media sites at work.
- Produce a social media policy, setting out the rules and standards expected, and the consequences of any breach.

ANGOLA

- Provide employees with training.
- Include a confidentiality clause in employment contracts.

Contributed by Tauil & Chequer

BELGIUM

1. *Are there any risks for employers that use social media sites to vet job applicants?*

   Yes. Employers risk unlawfully discriminating against an applicant if they use information related to a protected characteristic which they have taken from a social media site as the basis for refusing employment. There may also be data protection-related issues and problems with monitoring on-line communications.

2. *What steps can be taken by employers to minimise such risks?*

   - Only relevant information should be extracted.
   - A social media policy should be produced.
   - The person scanning the social media site should not be the same as the person determining the outcome of the recruitment process.
   - Advise applicants that social media sites are reviewed.
   - The applicant should confirm the content of any relevant information.

3. *What problems could an employer face as a result of employees using social media sites?*

   Employees using social media sites could breach confidentiality or insider rules and cause damage to the employer's or a third party's reputation. Employers could face loss of productivity across the work force and, in some circumstances, be liable for discriminatory comments made by one employee against another.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

   - Ban access to social media sites at work.
   - Produce a social media policy setting out the rules and standards expected and the consequences of any breach.

BELGIUM

- Provide employees with training.
- Include a confidentiality clause in employment contracts.

Contributed by Van Olmen Wynant

CZECH REPUBLIC

1. *Are there any risks for employers that use social media sites to vet job applicants?*

   Yes. Employers risk unlawfully discriminating against an applicant if they use information related to a protected characteristic which they have taken from a social media site as the basis for refusing employment.

2. *What steps can be taken by employers to minimise such risks?*

   - Only relevant information should be extracted.
   - A social media policy should be produced.
   - The person scanning the social media site should not be the same as the person determining the outcome of the recruitment process.
   - Advise applicants that social media sites are reviewed.
   - The applicant should confirm the content of any relevant information.

3. *What problems could an employer face as a result of employees using social media sites?*

   Employees using social media sites could breach confidentiality and cause damage to the employer's or a third party's reputation. An employer could be liable for discriminatory comments made by one employee against another in the course of their employment.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

   - Ban access to social media sites at work.
   - Produce a social media policy, setting out the rules and standards expected, and the consequences of any breach.
   - Monitor employees' use of social media sites.

CZECH REPUBLIC

- Provide employees with training.
- Include a confidentiality clause in employment contracts.

Contributed by Havel & Holásek s.r.o.

DENMARK

1. *Are there any risks for employers that use social media sites to vet job applicants?*

   Yes. Employers risk unlawfully discriminating against an applicant if they use information related to a protected characteristic which they have taken from a social media site as the basis for refusing employment.

2. *What steps can be taken by employers to minimise such risks?*

   - Only relevant information should be extracted.
   - A social media policy should be produced.
   - Provide training to the employees collecting the information.
   - Allow applicants to correct any information collected from social media sites.

3. *What problems could an employer face as a result of employees using social media sites?*

   Employees using social media sites could breach confidentiality, make statements on behalf of the employer which the employer does not endorse, damage the employer's reputation, expose the employer to IT risks and/or violate IP or other applicable laws.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

   - Ban access to social media sites at work.
   - Produce a social media policy setting out the rules and standards expected and the consequences of any breach.
   - Provide employees with training.
   - Monitor employees' use of social media sites.

Contributed by Kromann Reumert

EGYPT

1. *Are there any risks for employers that use social media sites to vet job applicants?*

   Yes. Employers risk unlawfully discriminating against an applicant if they use information related to a protected characteristic which they have taken from a social media site as the basis for refusing employment.

2. *What steps can be taken by employers to minimise such risks?*

   - Only extract legitimate and relevant information. A social media policy should set out guidelines to this effect.
   - The person scanning the social media site should not be the same as the person determining the outcome of the recruitment process.
   - Inform applicants that social media sites are reviewed.
   - Give applicants the opportunity to correct information retrieved.

3. *What problems could an employer face as a result of employees using social media sites?*

   Employees using social media sites could breach confidentiality and cause damage to the employer's or a third party's reputation. Employers could face a loss of productivity across the work force and, in some circumstances, be liable for discriminatory comments made by one employee against another if done so in the course of their employment.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

   - Ban access to social media sites at work.
   - Produce a social media policy setting out the rules and standards expected, including the consequences of any breach.

- Provide employees with training.
- Monitor employees' use of social media sites.
- Include a confidentiality clause in employment contracts.
- Take disciplinary action for misuse.

Contributed by Shalakany Law Office

FINLAND

1. *Are there any risks for employers that use social media sites to vet job applicants?*

   Yes. Employers risk unlawfully discriminating against an applicant if they use information related to a protected characteristic which they have taken from a social media site as the basis for refusing employment.

2. *What steps can be taken by employers to minimise such risks?*

   - Obtain the applicant's consent before retrieving the information from social media sites.
   - The person scanning the social media site should not be the same as the person determining the outcome of the recruitment process.

3. *What problems could an employer face as a result of employees using social media sites?*

   Employees using social media sites could breach confidentiality or insider rules and cause damage to the employer's or a third party's reputation. Employers could face loss of productivity across the work force and, in some circumstances, be liable for discriminatory comments made by one employee against another.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

   - Regulate use of electronic equipment.
   - Ban access to social media sites at work.
   - Produce a social media policy, setting out the rules and standards expected and the consequences of any breach.

Contributed by Dittmar & Indrenius

FRANCE

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Yes. Employers risk unlawfully discriminating against an applicant if they use information related to a protected characteristic which they have taken from a social media site as the basis for refusing employment. There may also be data protection related issues.

2. *What steps can be taken by employers to minimise such risks?*

- Only extract legitimate and relevant information. A social media policy should set out guidelines to this effect.
- Employees should be trained not to discriminate during the process.
- The person scanning the social media site should not be the same as the person determining the outcome of the recruitment process.
- Inform applicants and Works Councils that social media sites are reviewed.
- The applicant should be given the opportunity to correct any information relied on.

3. *What problems could an employer face as a result of employees using social media sites?*

Employees using social media sites could breach confidentiality and cause damage to the employer's or a third party's reputation. Employers could face a loss of productivity across the work force and, in some circumstances, be liable for discriminatory comments made by its employees.

FRANCE

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

- Ban access to social media sites at work.
- Create an official company social media site.
- Produce a social media policy, setting out the rules and standards expected, including the consequences of any breach.
- Provide employees with training.
- Monitor employees' use of social media sites.
- Include a confidentiality clause in employment contracts.
- Take disciplinary action.

Contributed by Mayer Brown

GERMANY

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Yes. Employers risk unlawfully discriminating against an applicant if they use information related to a protected characteristic which they have taken from a social media site as the basis for refusing employment. There may also be data protection related issues.

2. *What steps can be taken by employers to minimise such risks?*

- The employer's data protection officer should be informed before job applicants are vetted in this way.
- Only relevant information should be extracted from "professional" social media sites.
- The person scanning the social media site should not be the same as the person determining the outcome of the recruitment process.
- The applicant should have the opportunity to correct any relevant information.
- Consider any co-determination rights of the works council.
- Data no longer required should be deleted.

3. *What problems could an employer face as a result of employees using social media sites?*

Employees using social media sites could breach confidentiality and cause damage to the employer's or a third party's reputation. Employers could face a loss of productivity across the work force and, in some circumstances, be liable for discriminatory comments made by one employee against another in the course of their employment.

GERMANY

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

- Produce a social media policy, setting out the rules and standards expected, and the consequences of any breach.
- Provide employees with training.
- Comply with the works council's rights to information and co-determination.

Contributed by Mayer Brown LLP

GREECE

1. *Are there any risks for employers that use social media sites to vet job applicants?*

   Yes. Employers risk unlawfully discriminating against an applicant if they refuse to employ them based on information related to a protected characteristic, which they have taken from a social media site. There may also be data protection related issues.

2. *What steps can be taken by employers to minimise such risks?*

   - Inform applicants that social media sites are reviewed as part of the recruitment process.
   - Only extract legitimate and relevant information. A social media policy should set out guidelines to this effect.
   - Do not process personal data without a licence from the Data Protection Authority.
   - The applicant should have the opportunity to correct any relevant information.

3. *What problems could an employer face as a result of employees using social media sites?*

   Employees using social media sites could breach confidentiality and cause damage to the employer's or a third party's reputation. Employers could face a loss of productivity across the work force and, in some circumstances, be liable for discriminatory comments made by its employees.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

   - Ban access to social media sites at work.
   - Produce a social media policy setting out the rules and standards expected, including the consequences of any breach.

GREECE

- Provide employees with training.
- Monitor use of social media sites.
- Include a confidentiality clause in employment contracts.
- Consider whether disciplinary action for misuse can be justified.

Contributed by M & P Bernitsas Law Offices

HUNGARY

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Yes. Employers risk unlawfully discriminating against an applicant if they refuse to employ them based on information related to a protected characteristic, which they have taken from a social media site. There may also be data protection related issues.

2. *What steps can be taken by employers to minimise such risks?*

- Obtain consent before using information which is not publicly available.
- Only extract legitimate and relevant information. A social media policy should set out guidelines to this effect.
- Inform applicants that social media sites are reviewed.
- The applicant should have the opportunity to correct any relevant information.
- The person scanning the social media site should not be the same as the person determining the outcome of the recruitment process.

3. *What problems could an employer face as a result of employees using social media sites?*

Employees using social media sites could breach confidentiality and cause damage to the employer's or a third party's reputation. Employers could face a loss of productivity across the work force and, in some circumstances, be liable for discriminatory comments made by its employees in the course of their employment.

HUNGARY

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

- Produce a social media policy setting out the rules and standards expected, including the consequences of any breach.
- Include a confidentiality clause in employment contracts.
- Ask employees' consent before monitoring usage of social media sites.
- Provide employees with training.

Contributed by Ban, S. Szabo & Partners

ICELAND

1. *Are there any risks for employers that use social media sites to vet job applicants?*

   Yes. Employers risk unlawfully discriminating against an applicant if they refuse to employ them based on information related to a protected characteristic, which they have taken from a social media site. There may also be data protection related issues.

2. *What steps can be taken by employers to minimise such risks?*

   - Only extract legitimate and relevant information. Ignore any irrelevant material.
   - Obtain the applicant's consent before using information from social media sites.
   - The applicant should have the opportunity to correct any relevant information.

3. *What problems could an employer face as a result of employees using social media sites?*

   Employees using social media sites could breach confidentiality and cause damage to the employer's or a third party's reputation. Employers could face a loss of productivity across the work force and, in some circumstances, be liable for discriminatory comments made by its employees.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

   - Ban access to social media sites at work.
   - Remind employees of their duty of confidentiality.

ICELAND

- Produce a social media policy, setting out the rules and standards expected, including the consequences of any breach.
- Train employees on the dangers of bullying and harassment through social media.

Contributed by LOGOS Legal Services

IRELAND

1. *Are there any risks for employers that use social media sites to vet job applicants?*

   Yes. Employers risk unlawfully discriminating against an applicant if they refuse to employ them based on information related to a protected characteristic, which they have taken from a social media site. There may also be data protection related issues.

2. *What steps can be taken by employers to minimise such risks?*

   - Only extract legitimate and relevant information. A social media policy should set out guidelines to this effect.
   - The person scanning the social media site should not be the same as the person determining the outcome of the recruitment process.
   - Advise applicants that social media sites are reviewed.
   - The applicant should have the opportunity to correct any relevant information.

3. *What problems could an employer face as a result of employees using social media sites?*

   Employees using social media sites could breach confidentiality and cause damage to the employer's or a third party's reputation. Employers could also face a loss of productivity across the work force, and could be liable for harassment/discriminatory comments made by one employee against another in the course of their employment.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

   - Ban access to social media sites at work.
   - Produce a social media policy, setting out the rules and standards expected, and the consequences of any breach.

IRELAND

- Provide employees with training.
- Monitor employees' use of social media.
- Include a confidentiality clause in employment contracts.
- Take disciplinary action to enforce standards.

Contributed by A&L Goodbody

ISRAEL

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Yes. Employers face potential data protection related risks. An employer could also run the risk of facing claims for unlawful discrimination if it rejects an application on the basis of information it has obtained from a social media site that relates to one or more protected characteristics of the applicant.

2. *What steps can be taken by employers to minimise such risks?*

- Inform applicants prior to vetting social media sites and provide them with the opportunity to give their consent to such an exercise.
- The person scanning the social media sites should not be the same as the person who determines whether an applicant is successful.
- Put in place a social media policy.
- Employers should comply with the Israeli Privacy Protection Law 1981 registration requirements.

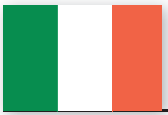
3. *What problems could an employer face as a result of employees using social media sites?*

An employee could post information on a social media site that breaches their obligations of confidentiality to their employer and their employer's obligations under the Israeli Privacy Protection Law 1981. An employee could also post information that damages their employer's reputation. An employer could also be held liable for any postings by employees that constitute harassment against other employees. The use of social media sites could also result in a loss of productivity within the workforce.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

- Ban the use of social media sites at work or during work hours.
- Put in place a social media policy.
- In exceptional cases, engage in limited monitoring of social media sites.
- Incorporate appropriate confidentiality clauses in employment contracts.
- Take disciplinary action against employees who misuse social media sites.

Contributed by Goldfarb, Levy, Eran, Meiri, Tzafrir & Co Law Offices



ITALY

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Yes. An employer could run the risk of facing claims for unlawful discrimination if it rejects an application on the basis of information it has obtained from a social media site that relates to one or more protected characteristics of the applicant.

2. *What steps can be taken by employers to minimise such risks?*

- Only extract information from a social media site that is relevant to the job.
- Put in place a social media policy.
- The person scanning the social media site should obtain the applicant's consent to access their profile on the site, and that person should be different to the person who determines whether the application should be successful.
- Applicants should be given the opportunity to correct any information that is relied upon before a final decision is taken.

3. *What problems could an employer face as a result of employees using social media sites?*

An employee could post information on a social media site that breaches their obligations of confidentiality to their employer. An employee could also post information that damages their employer's reputation. An employer could also be held liable for any postings by employees that constitute unlawful discrimination or harassment against other employees. The use of social media sites could also result in a loss of productivity within the workforce.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

- Impose an outright ban on the use of social media sites in the workplace.
- Provide training to employees on what could constitute a misuse of social media.
- Put in place a social media policy.
- Consider whether the use of social media could and should be monitored.
- Incorporate appropriate confidentiality clauses in employment contracts.
- Take disciplinary action against employees who misuse social media.

Contributed by Quorum Legal Network

MOZAMBIQUE

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Yes. Employers risk unlawfully discriminating against an applicant if they use information related to a protected characteristic which they have taken from a social media site as the basis for refusing employment.

2. *What steps can be taken by employers to minimise such risks?*

- The information which an employer takes from a social media site must be publicly available.
- Only relevant information should be extracted.
- A social media policy should be produced.
- Advise applicants that social media sites are reviewed.
- The applicant should confirm the content of any relevant information extracted.

3. *What problems could an employer face as a result of employees using social media sites?*

Employees using social media sites could breach confidentiality and cause damage to the employer's or a third party's reputation. An employer could be liable for discriminatory comments made by one employee against another in the course of their employment.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

- Inform employees that their use of social media sites will be monitored.
- Ban access to social media sites at work.
- Produce a social media policy, setting out the rules and standards expected, and the consequences of any breach.

MOZAMBIQUE

- Provide employees with training.
- Include a confidentiality clause in employment contracts.

Contributed by Tauil & Chequer

NETHERLANDS

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Yes. There are possible data protection implications for employers. An employer could also run the risk of facing discrimination claims if it rejects an application on the basis of information it has obtained from a social media site that relates to one or more protected characteristics of the applicant.

2. *What steps can be taken by employers to minimise such risks?*

- Extract only legitimate and relevant information for the job application process.
- Before processing personal data of the applicant, obtain their prior consent.
- Consider whether information gathered via a social media site is actually necessary.
- Put in place a social media policy.
- Try to ascertain whether the information obtained is accurate and reliable.
- Applicants who may be rejected should be given the opportunity to correct any information that is being relied upon by the employer.

3. *What problems could an employer face as a result of employees using social media sites?*

An employee could post information on a social media site that breaches their obligations of confidentiality to their employer. An employee could also post information that damages their employer's reputation. An employer could also be held liable for any postings by employees that constitute unlawful discrimination or harassment against other employees. The use of social media sites could also result in

a loss of productivity within the workforce. There could also be data protection issues and an employer could be liable if an employee posts information which infringes a third party's intellectual property rights.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

- Impose an outright ban on the use of social media sites in the workplace.
- Provide training to employees on what could constitute a misuse of social media.
- Put in place a social media policy.
- Consider whether the use of social media could and should be monitored.
- Incorporate appropriate confidentiality clauses in employment contracts.
- Take disciplinary action against employees who misuse social media.

Contributed by Van Doorne N.V.

NORWAY

1. *Are there any risks for employers that use social media sites to vet job applicants?*

   Employers could face discrimination claims if they use certain protected personal characteristics as the basis for rejecting applicants. There are also risks under Norway's data protection regime.

2. *What steps can be taken by employers to minimise such risks?*

   - Those scanning social media sites as part of the recruitment process should be instructed to extract only that information that is relevant to the job application process.
   - A social media policy or other written guidelines should be implemented.
   - Applicants should be informed at the start of the application process that a vetting or verification exercise using social media sites forms part of the process.
   - Applicants who are rejected because of information gleaned from social networking sites should be given an opportunity to review and, if necessary, correct that information before any final decisions are taken.

3. *What problems could an employer face as a result of employees using social media sites?*

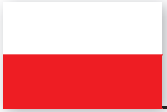
   Employees could breach obligations of confidentiality by posting information about the employer or their fellow employees. In addition, the employer could find themselves vicariously liable for defamatory comments posted by their employees.

NORWAY

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

- Impose restrictions on access to social media sites at work.
- Put in place a social media policy which deals with the use of social media sites during and outside of work hours.
- Monitor employee's use of social media sites at work. However, legal advice should be sought before engaging in any such activity.
- Incorporate appropriate confidentiality clauses into contracts of employment.
- Take disciplinary action against employees who misuse social media sites to the detriment of the employer.

Contributed by Advokatfirmaet Thommessen AS



POLAND

1. *Are there any risks for employers that use social media sites to vet job applicants?*

   Yes. Employers risk unlawfully discriminating against an applicant if they refuse employment based on use of protected information taken from a social media site. There may also be data protection related issues.

2. *What steps can be taken by employers to minimise such risks?*

   - Only relevant information should be extracted.
   - A social media policy should be produced.
   - Advise applicants that social media sites are reviewed at the start of the process.

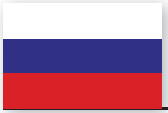
3. *What problems could an employer face as a result of employees using social media sites?*

   Employees using social media sites could breach confidentiality and cause damage to the employer's or a third party's reputation. Employers could face a loss of productivity across the work force and, in some circumstances, be liable for discriminatory comments made by one employee against another in the course of their employment.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

   - Ban access to social media sites at work.
   - Produce a social media policy, setting out the rules and standards expected, and the consequences of any breach.
   - Monitor the use of employees' use of social media sites, although legal advice should be sought beforehand.
   - Remind employees of their duty of confidentiality.

Contributed by Soltysinski Kawecki & Szlezak



RUSSIA

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Employers could face discrimination claims and/or penalties for infringement of Russian data protection law.

2. *What steps can be taken by employers to minimise such risks?*

- Employers are required by law to have in force a binding policy on the collection and use of personal data, which should include reference to the fact that background checks will be carried out using social media.
- The consent of employees and job applicants should be obtained before their details are collected and used.
- Social media sites should be scanned only to check information that has previously been obtained directly from the employee.
- Extracting data which relates to the employee's private life, religion, politics and membership of NGOs or labour unions should be prohibited.
- Decisions relating to employees and job applicants should not be based exclusively on data extracted from social media sites.

3. *What problems could an employer face as a result of employees using social media sites?*

- Employees could breach obligations of confidentiality by posting information about the employer or their fellow employees.
- There is a small risk that the employer could be vicariously liable if employees commit acts of harassment or post defamatory comments using social media sites.
- Finally, permitting employees access to social media sites while at work could lead to a loss of productivity.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

- Impose an outright ban on access to social media sites at work.
- Alternatively, put in place internal policies dealing with the use of social media sites during working hours.
- Monitor the use of the internet at work to assess potential risks and inform employees that such monitoring is taking place.
- Incorporate into employment contracts a special confidentiality clause, maintain internal rules on confidentiality and ensure that employees are properly acquainted with such rules. Under Russian law, employees do not have a general duty to keep confidential information belonging to the employer and the types of information that are protected by law are restricted, so it is prudent to impose a contractual obligation of confidentiality on employees.

Contributed by Secretan Troyanov Schaer SA

SPAIN

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Employers could find themselves in breach of Spanish Data Protection Law if they use 'personal data' to vet applicants without the consent of the individuals concerned and/or the relevant data protection principles are not followed.

There is also a small risk of discrimination claims being brought by rejected applicants.

2. *What steps can be taken by employers to minimise such risks?*

- Employers should implement an internal policy, providing guidelines for obtaining and using personal data.
- Applicants could be warned at the start of the application process that data may be collected from social media and used in the application process.

3. *What problems could an employer face as a result of employees using social media sites?*

Employees could breach confidentiality and cause damage to the employer's or a third party's reputation. Employers could also find themselves liable for claims for harassment and/or discrimination based on comments posted by employees.

There is also the risk of loss of productivity across the workforce.

In addition, Spanish laws governing access to computer systems make it hard to collect evidence on the misuse of such sites, making disciplinary action against offending employees difficult to bring.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

- Put in place a social media policy which deals with the use of social media sites during and outside of work hours.
- Provide awareness training to employees on conduct that could constitute discrimination, harassment and bullying.
- Monitor the use of social media sites at work to help to determine whether there is a loss of productivity as a result of employees accessing such sites. However, legal advice should be sought before engaging in any such activity.
- Incorporate within employment contracts an appropriate confidentiality clause.
- Disciplinary action may be taken against employees who misuse social media sites to the detriment of the employer.

Contributed by Ramón & Cajal Abogados

SULTANATE OF OMAN

1. *Are there any risks for employers that use social media sites to vet job applicants?*

   No

2. *What steps can be taken by employers to minimise such risks?*

   Not applicable.

3. *What problems could an employer face as a result of employees using social media sites?*

   Employees could use social media sites in such a way as to breach their obligations of confidentiality to their employer. They could also use such sites to post material which is damaging to the reputation of the employer and/or third parties.

   Employers will not generally be vicariously liable for the actions of their employees, however, there is a risk to the employer if their systems are used to transmit material that is 'contrary to public order or good morals'.

   There is also the obvious risk of a loss of productivity in the workforce.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

   - Forbid or restrict the use of social media sites at work.
   - Include a social media policy in the employer's disciplinary procedures set out in the company's HR manual.
   - Monitor the use of social media sites by employees to determine the extent of loss of productivity.
   - Take disciplinary action against employees who do not comply with the relevant company policies.

Contributed by SASLO

SWEDEN

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Employers run the risk of discrimination claims and/or sanctions for infringement of Swedish Data Protection law if information relating to individual applicants' protected characteristics is collected and used to make recruitment decisions.

2. *What steps can be taken by employers to minimise such risks?*

- Extract only legitimate and relevant information for the job application process.
- A social media policy or other written guidelines should back this up.
- Personal data obtained from social media should be kept as unstructured material.
- The person scanning the social media sites should not be the same as the person who determines the outcome of the recruitment process.
- Applicants should be informed, at the start of any application process, that a vetting or verification exercise using social media sites forms part of that process.
- Job applicants should be given an opportunity to correct that information before any final decisions are taken.

3. *What problems could an employer face as a result of employees using social media sites?*

The content of employees' posts could breach confidentiality, infringe third party intellectual property rights or cause damage to the employer's or a third party's reputation.

Employers could also face claims for harassment or unlawful discrimination as a result of employee's comments on such sites.

Finally, there is the obvious impact on productivity if employees are allowed to use social media sites during working hours.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

- Impose an outright ban on access to social media sites at work.
- Put in place a social media policy.
- Provide awareness training to employees.
- Consider whether monitoring of social media sites at work should and could be used.
- Incorporate within employment contracts an appropriate confidentiality clause.
- Disciplinary action may be taken against employees who misuse a social media site to the detriment of the employer.

Contributed by Advokatfirman Vinge KB

SWITZERLAND

1. *Are there any risks for employers that use social media sites to vet job applicants?*

   Yes. Employers face data protection restrictions when collecting and processing information about applicants from social media sites.

2. *What steps can be taken by employers to minimise such risks?*

   - Ban the use of fictitious user profiles for the purposes of vetting an applicant's social media site.
   - Extract only legitimate and relevant information from social media sites.
   - Put in place a social media policy.
   - The person scanning the social media site should not be the same as the person determining the outcome of the recruitment process.

3. *What problems could an employer face as a result of employees using social media sites?*

   Employees could post information on social media sites that damage their employer's reputation and breach confidentiality. Employers could also face a loss of productivity across the workforce.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

   - Impose an outright ban on the use of social media sites during working hours.
   - Put in place a social media policy.
   - Consider whether it would be lawful to monitor the use of social media sites at work.

- Insert appropriately worded confidentiality clauses in employment contracts.
- Provide training to employees on the pitfalls of using social media sites.

Contributed by Pestalozzi Attorneys at Law Ltd

TURKEY

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Yes. Employers risk unlawfully discriminating against an applicant if it uses certain information about them, which it has obtained from a social media site, as the basis for rejecting their application. Employers also face risks in relation to data protection issues and restrictions surrounding the termination of the applicant's employment.

2. *What steps can be taken by employers to minimise such risks?*

- Employers should obtain consent from the applicant before using information from social media sites as part of the vetting process.
- Only legitimate and relevant information should be used.
- A social media policy should be put in place.
- The person scanning social media sites should be different from the person determining the application process or interviewing the applicant.

3. *What problems could an employer face as a result of employees using social media sites?*

Employees could post confidential information about their employer or employer's business on social media sites and breach confidentiality as a result. They could also post information which damages their employer's reputation. Employers also face the risk that employees could post information on social media sites that constitutes unlawful discrimination and/or harassment against colleagues. Employers could also face a loss of productivity across the workforce.

TURKEY

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

- Impose an outright ban on access to social media sites at work.
- A confidentiality clause could be added to employment contracts restricting the employees' use of confidential information.
- Prevent employees from accessing social media sites during work hours.
- Training employees on the potential problems that could arise from misusing social media.
- Put in place a social media policy.
- Monitoring employees' use of social media sites, but only with their consent.

Contributed by Pekin & Pekin

UAE

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Yes, but only for employers who are based in the Dubai International Financial Centre (DIFC), which is considered to have independent jurisdiction with its own laws and regulations. Employers in the DFIC could risk facing a claim for unlawful discrimination if they use certain information about a job applicant, which has been obtained from a social media site, as the basis for refusing employment. Employers in the DFIC also face risks if they process information in contravention of data protection laws.

2. *What steps can be taken by employers to minimise such risks?*

- The person scanning the social media site should not be the same person who is determining the job application process or interviewing the applicant.
- Only extract legitimate and relevant information for the application process.
- A social media policy should be put in place.
- Applicants should be told that vetting using social media sites forms part of the process.
- Applicants who are rejected should be given an opportunity to correct any information that is relied upon.

3. *What problems could an employer face as a result of employees using social media sites?*

For employers based in the DFIC, employees could use information obtained from social media sites to unlawfully discriminate against colleagues. Otherwise, in the UAE more generally, employees could use social media sites to breach confidentiality and damage their employer's reputation. The use of social media in the workplace could also have an adverse effect on productivity amongst the workforce.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

- Ban access to social media sites at work.
- Put in place a social media policy.
- Provide training to employees on the pitfalls of using social media.
- Monitor the use of social media sites at work.
- Incorporate within employment contracts an appropriate confidentiality clause.
- Take disciplinary action against employees who misuse social media sites.

Contributed by Shalakany Law Office

UNITED KINGDOM

1. *Are there any risks for employers that use social media sites to vet job applicants?*

There is a risk of an unlawful discrimination claim if an employer uses information on protected characteristics obtained from a social media site when making decisions on recruitment.

In addition, the employer could infringe UK data protection law if it does not comply with its obligations in respect of the use and processing of personal data.

2. *What steps can be taken by employers to minimise such risks?*

- Those scanning social media sites as part of the recruitment process should be instructed to extract only legitimate and relevant information for the job application process.
- A social media policy or other written guidelines should back this up, so that the employer can demonstrate an intention to extract only relevant information.
- Ideally, the person scanning the social media sites should not be the same as the person who is determining the job application process or interviewing the individual.
- Applicants should be told, at the start of any application process, that a vetting or verification exercise using social media sites forms part of the process.
- Job applicants should be given an opportunity to correct any information held.

3. *What problems could an employer face as a result of employees using social media sites?*

The content of employees' posts could breach confidentiality, infringe third party intellectual property rights or cause damage to the employer's or a third party's reputation.

Employers could also face claims for harassment or unlawful discrimination as a result of employee's comments on such sites.

Finally, there is the obvious impact on productivity if employees are allowed to use social media sites during working hours.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

- Impose an outright ban on access to social media sites at work.
- Put in place a social media policy which deals with the use of social media sites during and outside of work hours.
- Provide awareness training to employees on conduct that could constitute discrimination, harassment and bullying.
- Monitoring the use of social media sites at work could help to determine whether there is a loss of productivity as a result of employees accessing such sites. However, legal advice should be sought before engaging in any such monitoring.
- Incorporate within employment contracts an appropriate confidentiality clause.
- Incorporate appropriate post-termination restrictive covenants within employment contracts.
- Disciplinary action may be taken against employees who misuse a social media site to the detriment of the employer.

Contributed by Mayer Brown International LLP

ANGOLA

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Employers are free to use information which is publicly available on social media websites when selecting job applicants. Social media sites could be used by employers to ascertain more information about an applicant if the information provided on their CV or that revealed during their interview is not sufficient for the employer to make a decision.

Unlawful discrimination

Social media sites will often contain personal profiles of the individual concerned, including certain characteristics, which are protected from discrimination. These characteristics could be age, disability, sex (including pregnancy and maternity), race (including nationality), religion or belief, and sexual orientation. It is unlikely that most, if any, of these characteristics will feature in a CV.

There are no restrictions on employers in this regard, provided that the information obtained from social media is not to be used in such a way as to discriminate against an applicant. It would, however, be very difficult for a job applicant to show that they have been discriminated against by a prospective employer using information which they obtained via social media sites.

Potential data protection implications

Employers are free to use social network information to the extent that the information which is extracted relates to the employment. If there is information on a social media site that is useful for an employer to set the profile of a job applicant, there should be no problem in using such information in the hiring process.

ANGOLA

2. *What steps can be taken by employers to minimise such risks?*

It is important that any information that an employer sources through social media websites is publicly available to whoever accesses the site. Employers should instruct those scanning social media sites as part of the recruitment process to extract only relevant information for the job application process. That information must be readily accessible to all and not be of a restricted nature.

A social media policy or other written guidelines should be produced by the employer, which states that only information relevant to the application process is accessed. This will be important for an employer so that they can demonstrate that they have legitimate reasons for using that information.

Applicants should be advised at the start of the recruitment process that social media sites are used to collect information. The employer should ask the applicant to confirm the content of any information that the employer deemed relevant to the selection process which was taken from a social media source.

3. *What problems could an employer face as a result of employees using social media sites?*

Breach of confidentiality

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social media platforms, it is not uncommon for employees to post confidential information about the employer and/or other employees. This could result in significant damage to the employer's business and reputation.

Damage to employer's or third party's reputation

Employees could post information on a social media site that causes damage to the reputation of the employer and/or a third party. An employer may be vicariously liable for

the defamatory conduct of an employee. The fact that an employer may have a claim against the employee concerned would be of little comfort compared to the damage to the employer's reputation.

Harassment/Unlawful discrimination

It is not uncommon for employees to post negative comments about fellow employees on social media sites. The comments could relate to a characteristic such as age, disability, race or sex, which are protected under discrimination laws. If an employee were to make such comments 'in the course of their employment', there is a danger that such comments could constitute discrimination/defamation. It would be difficult to establish liability against the employer for the employee's actions, but such conduct could ultimately have a detrimental affect on the working environment and the productivity of the workforce.

Although it would be difficult to consider the employer liable for any defamatory or discriminatory act carried out by an employee using a social networking site, it would be helpful to employers if they could show that they took all reasonable steps to prevent the employee from committing the discriminatory/defamatory act in question.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

An employer can take the following steps:

- Impose an outright ban on employee access to social media sites at work. This approach could prove to be unpopular among employees and have an adverse impact on workforce morale. Ultimately, the employer would need to weigh up the potential advantages and disadvantages in deciding whether to allow employees to access social media sites at work. A complete ban would

not address the problems that could arise from postings made by employees outside of working hours.

- Put in place a social media policy which deals with the use of social media sites during and outside of work hours. Such a policy should have provisions dealing with social media activity but, in particular:
    - set out the parameters governing the use of the employer's IT systems;
    - remind employees that social media activity may not necessarily be private;
    - prohibit discrimination, harassment or bullying of other employees, which could include negative comments about employees posted on social media sites;
    - prohibit negative comments about the employer, its employees or third parties; and
    - prohibit the disclosure of any confidential information that relates to the employer and/or other employees.

  The policy should set out the consequences of a breach of the policy, which could include disciplinary action and, ultimately, dismissal.
- Provide awareness training to all employees on conduct that could constitute discrimination, harassment and bullying. An employer would be able to defend any subsequent claim for discrimination or harassment if it can show that it took all reasonable steps to prevent the employee from committing the discriminatory act in question.
- Monitoring the use of social media sites at work could help to determine whether there is a loss of productivity as a result of employees accessing such sites. The

employee must, however, be given notice that their internet use is being monitored. The data retrieved from monitoring shall not be used without the consent of the employee, save for very specific situations, such as a criminal investigation or for national security purposes. Legal advice should be sought before engaging in any such monitoring.

- Incorporate an appropriate confidentiality clause in employment contracts, which protects the employer in the event that an employee posts confidential information on a social media site.
- Disciplinary action may be taken against employees who misuse a social media site to the detriment of the employer. In some cases, an employer could consider dismissal. Each case will turn on its facts, and an employer might want to obtain legal advice before proceeding to dismiss the employee in question.

Contributed by Tauil & Chequer

ANGOLA

BELGIUM

1. *Are there any risks for employers that use social media sites to vet job applicants?*

There is no specific legislation prohibiting employers from using social media sites to vet job applicants. Searching on the internet for information about job applicants is a widespread practice among employers.

However, when using information available on the internet, employers will have to comply with the general legal framework applicable to the screening and selection of candidates. If they do not, the employer exposes themselves to the risk of claims being brought against them for unlawful discrimination or for the abuse of data protection laws.

Discrimination

Anti-discrimination law prohibits all forms of discrimination, either direct or indirect, on the grounds of: age, sexual orientation, sex, marital status, place of/social class at birth, personal wealth, religious or philosophical beliefs, political convictions, language, current ill health or future predications as to a person's health, disability, physical characteristics, social class, nationality, race (actual or perceived), colour, ancestry, national or ethnic origin.

An employer can only use the above characteristics as selection criteria in their recruitment process, if:

- it is an essential professional requirement relevant to the nature of the role; or it is a necessary condition for the performance of the role; and
- it is a proportionate way of meeting one of those legitimate aims.

Regulations dealing with the recruitment and selection of employees also contain provisions preventing employers from discriminating against job applicants on the basis of personal data, if that personal data is irrelevant to the function or nature of the business.

BELGIUM

If an employer rejects a job applicant on the basis of one of the protected grounds, the employer risks a claim for unlawful discrimination. However, the job applicant would need to discover that their application was rejected on that basis before they could bring such a claim. For discrimination purposes, it is irrelevant whether the information was obtained via a social media site or from a CV submitted by the candidate.

If an employer was found to have discriminated in this way, they could be liable to criminal sanctions.

Personal Data Protection

Collecting information about job applicants from the internet and storing this information in a personnel file could amount to the "processing of personal data". "Processing" of such data is regulated by law in order to ensure that personal data is protected.

The processing of personal data may only be carried out in a limited number of situations. Moreover, in order to be legitimate, the processing has to also comply with a set of fundamental principles. For example, the information can only be collected for specified, explicit and legitimate purposes. The information must be adequate, relevant and not excessive when compared to the purpose for which it was collected. The information must be accurate and kept up to date.

It is questionable whether information found on social media websites is accurate. It is also arguable whether it is proportionate to use information from such sources in a recruitment process.

Strictly speaking the processing of the following data is prohibited:

- so-called "sensitive data", i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, as well as the transfer of information relating to a person's sex life;
- data relating to a person's health;
- data relating to legal proceedings.

The processing of sensitive data and data relating to an individual's health is nevertheless permitted if required by law. If this is not the case, an employer cannot process this kind of data, even with the written consent of the employee, unless this processing would also prove advantageous to the employee (and the employee gives his/her express consent to that effect). It is for the employer to decide whether the processing would be advantageous to the employee. However, they must be in a position to justify why this is the case.

In principle, data relating to legal proceedings may never be processed by an employer, not even if the employee has given his/her written consent.

Failure to comply with the legal obligations governing data privacy would render the controller of that data, or his representative, liable to criminal sanctions. In addition, if the case went to court, a judge could order that the outcome be published in the newspapers and/or that the data be confiscated or destroyed. Moreover, the judge could prevent the employer from processing personal data for a period of two years.

The subject of the data which has been misused could also claim damages. In that regard, the controller of the data is presumed to be liable unless he proves the contrary.

BELGIUM

Compliance with legislation

There is legislation in place which relates to the monitoring of electronic on-line communications. This legislation specifically addresses employees' access to, and the use of, on-line communication facilities at work, and the monitoring of such use.

Surveillance of on-line communications is only possible for the following limited purposes:

- the prevention of unlawful acts, defamatory acts, acts that are contrary to good moral conduct or acts that may violate another person's dignity;
- the protection of the economic, trade and financial interests of the company;
- the protection of the security and proper functioning of the company's IT system; or
- compliance with company policies in relation to on-line technologies.

Moreover, the monitoring of electronic on-line communications data is permitted only insofar as it is proportionate to do so and is done so in a transparent way.

If there are employee representatives, and the employer plans to install a system for monitoring electronic online-communications data, the representatives must be informed in advance of that monitoring taking place. If there are no employee representatives, the employer must discuss this with the employees directly.

An employer may not process the collected data in such a way that it can be attributed to an identifiable person, unless the monitoring is for one or more of the following purposes:

- the prevention of unlawful or defamatory acts, acts that are contrary to good moral conduct, or acts which may violate another person's dignity;

- the protection of the economic, trade and financial interests of the company; or
- the protection of the security and proper functioning of the company's IT system.

In all other cases, the data must remain anonymous, unless the employees have been notified that their use of electronic communications is being monitored.

2. What steps can be taken by employers to minimise such risks?

Assuming that employers do not wish to take steps to ban all vetting of job applicants using information from social media, there are a number of steps which can be taken to guard against unnecessary risk:

- Those scanning social media sites as part of the recruitment process should be instructed to extract only legitimate and relevant information for the job application process.
- A social media policy or other written guidelines should back this up, so that the employer can demonstrate an intention to extract only relevant information.
- Ideally, the person scanning the social media sites should not be the same as the person who is determining the job application process or interviewing the individual. This way, the irrelevant material (which might contain sensitive personal data) will not make its way through to the decision maker.
- Applicants should be told, at the start of any application process, that a vetting or verification exercise using social media sites forms part of the process.
- Job applicants who are rejected because of information gleaned from social networking should be given an opportunity to correct that information before any final decisions are taken.

BELGIUM

3. *What problems could an employer face as a result of employees using social media sites?*

Breach of confidentiality

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social media platforms, it is not uncommon for employees to end up posting confidential information about the employer and/or other employees. This could result in significant damage to the employer's business and reputation.

Damage to employer's or third party's reputation

Employees could post information on a social media site that causes damage to the reputation of the employer and/or a third party. An employer may be vicariously liable for the defamatory conduct of an employee if it is linked to the employment. The fact that an employer may have a claim against the employee concerned could be of little comfort compared to the damage to the reputation of the employer.

Harassment

It is not uncommon for employees to post negative comments about fellow employees on social media sites. In some circumstances, such behaviour could be qualified as harassment at work.

Inappropriate behaviour that takes place at or outside of work can, in some circumstances, amount to harassment. If the aim or consequence of such behaviour is that the individual's personality, dignity or physical or psychological integrity is compromised whilst he/she is at work, or his/her job is placed at risk, or a threatening, hostile, insulting, demeaning or hurtful environment is created, harassment will be established. A person can be harassed though words, threats, actions, gestures or one-sided communication.

Often, harassment is associated with religion or beliefs, disability, age, sexual orientation, gender or ethnic origin.

If an employee uses social media to harass a colleague, an employer could be personally and vicariously liable for the actions of that employee. They could then face criminal and/or civil liability.

Loss of productivity

In addition to the above, employees are likely to be less productive if they are able to access personal social media sites during working hours.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

- An employer can impose an outright ban on access to social media sites at work. This approach could prove to be unpopular amongst employees and have an adverse impact on the morale within a workforce. Ultimately, the employer would need to weigh up the potential advantages and disadvantages in deciding whether to permit employees to access social media sites at work. A complete ban would not address the potential problems that could arise from postings by employees via wireless media or outside of working hours. Employers can easily find themselves liable for comments made after hours by employees, particularly where there is an obvious and clear link to the employment. Accordingly, comments posted by one employee about another employee after hours on a social networking site could still end up as the responsibility of the employer.
- To comply with the legislation discussed above, an employer who wants to monitor the use of online communications should put in place a general policy

regarding the use of online communications and social media websites by employees, which advises employees of:

- the parameters governing the use of the employer's IT systems;
- the policy on monitoring, and the prerogatives of the employer and the supervisory staff;
- whether or not personal data is stored, where, and for how long it is stored; and
- whether or not the monitoring is permanent.

The policy should also contain a set of compliance rules regarding the use of social media sites during and outside of work hours. These compliance rules could relate to some of the following:

- the prohibition of discrimination, harassment or bullying of other employees, which could include negative comments about employees posted on social media sites;
- the prohibition of negative comments about the employer, its employees or third parties; and
- the prohibition of the disclosure of any confidential information that relates to the employer and/or other employees.

The policy should set out the consequences of a breach of the policy, which could include disciplinary action and, ultimately, dismissal.

Ideally this policy would be incorporated in the Company's employee handbook.

- Employers are required to take the necessary steps to prevent harassment within the company. To achieve that, employers could provide awareness training

to their employees on conduct that could constitute discrimination, harassment and bullying. An employer would be able to defend any subsequent claim for discrimination or harassment if it can show that it took all reasonable steps to prevent the employee from committing the discriminatory act in question.

- An appropriate confidentiality clause should be incorporated in employment contracts which would afford protection to the employer if any employee posts confidential information on a social media site.
- Disciplinary action may be taken against employees who misuse a social media site to the detriment of the employer. In some cases, an employer could consider dismissal. Each case will be considered on its facts, and an employer might want to obtain legal advice before proceeding to dismiss the employee in question.
- Larger companies with a marketing and communications department could screen social media sites for information that has been posted relating to the company.

Contributed by Van Olmen Wynant

BELGIUM

CZECH REPUBLIC

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Unlawful discrimination

Discrimination based on certain personal characteristics, such as age, disability, sex, pregnancy, maternity, fatherhood, race, ethnic origin, nationality, religion or belief, sexual orientation and disability is prohibited. These characteristics must not be used to discriminate against prospective employees during the recruitment process. Largely, these characteristics are irrelevant for the purposes of recruitment and would not normally be disclosed by the employee to the potential employer. The employer also has no right to request such information.

An employer may have access to information regarding an applicant's personal characteristics via a social media site. If an employer uses such information as the basis for refusing to recruit an applicant, that could constitute unlawful direct discrimination. The employer could face a claim for discrimination if the job applicant were to discover that their application was rejected because of one or more of the above characteristics. The employer would then have to prove that they did not unlawfully discriminate against that candidate.

Personal Data Protection

Vetting job applicants using information contained on social media sites could also have implications for employers in relation to data protection. The collection and use of "personal data" is regulated and protected. Personal data amounts to any information which relates to an identified or identifiable individual. An individual is considered identified or identifiable if it is possible to recognize the individual directly or indirectly, for example on the basis of a number, code or one or more factors specific to his/her physical, physiological, psychical, economic, cultural or social identity.

"Sensitive data" is personal data which reveals a person's nationality, racial or ethnic origin, political views, trade-union membership, religious and philosophical beliefs, past criminal convictions, details about their health and/or sexual life and genetic information. Sensitive data will also include biometric data from which an individual can be identified.

Certain obligations are imposed on employers who process personal data and these are even stricter for sensitive personal data. Collection, storage, disclosure, modification, retrieval, use, transfer, dissemination, publishing, preservation, exchange and sorting are all examples of "processing" data. Therefore, when an employer collects information about an applicant from a social media site, this could amount to the processing of sensitive information. Employers must comply with data protection principles in such circumstances.

Sensitive data can only be processed if the applicant has given their explicit consent, the sensitive data was published by the applicant or if one of a limited number of other legitimate aims has been satisfied. It will be a legitimate aim if the employer is required by employment law to process the sensitive information. However, this exception is not likely to apply to information which can be found on social media sites. Failure by an employer to comply with data protection principles could result in claims for compensation by an employee or action being taken against it by the Czech Office for the Protection of Personal Data.

Accuracy and reliability

An additional risk for employers using information from social media sites is that the information may not be wholly accurate. Therefore, information retrieved from such websites will not be reliable as an assessment tool for hiring purposes.

2. *What steps can be taken by employers to minimise such risks?*

Assuming employers do not wish to take steps to ban all vetting of job applicants using information from social media, there are a number of steps which can be taken to guard against unnecessary risk:

- Those scanning social media sites as part of the recruitment process should be instructed to extract only legitimate and relevant information for the job application process.
- A social media policy or other written guidelines should back this up, so that the employer can demonstrate an intention to extract only relevant information.
- Ideally, the person scanning the social media sites should not be the same as the person who is determining the job application process or interviewing the individual. This way, the irrelevant material (which might contain sensitive personal data) will not make its way through to the decision maker.
- Applicants should be told, at the start of any application process that a vetting or verification exercise using social media sites forms part of the process.
- Job applicants who are rejected because of information gleaned from social networking should be given an opportunity to correct that information before any final decisions are taken.

3. *What problems could an employer face as a result of employees using social media sites?*

Breach of confidentiality

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social media platforms, it is not uncommon for employees to end

up posting confidential information about the employer and/or other employees. This could result in significant damage to the employer's business and reputation.

Damage to employer's or third party's reputation

Employees could post information on a social media site that causes damage to the reputation of the employer and/or a third party. An employer may be vicariously liable for the defamatory conduct of an employee. The fact that an employer may have a claim against the employee concerned could be of little comfort compared to the damage to the reputation of the employer. In any event, the employer's ability to claim against the employee may be limited.

Harassment/Unlawful discrimination

It is not uncommon for employees to post negative comments about fellow employees on social media sites. The comments could relate to a protected characteristic such as age, disability, race or sex. If an employee were to make such comments 'in the course of their employment', there is a danger that such comments could constitute unlawful harassment. In such circumstances, an employer could also be vicariously liable for the actions of that employee.

An employer could also risk facing discrimination claims if employees use information they have obtained from social media sites about other employees as the basis for treating them in a detrimental way.

An employer will have a defence to any claim for discrimination or harassment if it can show that it took all reasonable steps to prevent the employee from committing the discriminatory act in question.

Currently employers cannot be held criminally liable for an offence committed by one of its employees. However, there is new legislation that has been proposed which could change this position if brought into effect.

Loss of productivity

Aside from the potential legal issues, employees may be less productive if they are permitted to use social media sites during working hours.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

An employer can take the following steps:

- Impose an outright ban on access to social media sites at work. This approach could prove to be unpopular amongst employees and have an adverse impact on the morale within a workforce. Ultimately, the employer would need to weigh up the potential advantages and disadvantages in deciding whether to permit employees to access social media sites at work. A complete ban would not address the potential problems that could arise from postings by employees outside of working hours. Employers can easily find themselves liable for comments made after hours by employees, particularly where there is an obvious and clear link to the employment. Accordingly, comments posted by one employee about another employee after hours on a social networking site could still end up as the responsibility of the employer.
- Put in place a social media policy which deals with the use of social media sites during and outside of work hours. Such a policy should have provisions dealing with social media activity, but in particular:
    - set out the parameters governing the use of the employer's IT systems;
    - remind employees that social media activity may not necessarily be private;

- prohibit discrimination, harassment or bullying of other employees, which could include negative comments about employees posted on social media sites;
- prohibit negative comments about the employer, its employees or third parties; and
- prohibit the disclosure of any confidential information that relates to the employer and/or other employees.

The policy should set out the consequences of a breach of the policy, which could include disciplinary action and, ultimately, dismissal.

- Provide awareness training to employees on conduct that could constitute discrimination, harassment and bullying. An employer would be able to defend any subsequent claim for discrimination or harassment if it can show that it took all reasonable steps to prevent the employee from committing the discriminatory act in question.
- Monitoring the use of social media sites at work could help to determine whether there is a loss of productivity as a result of employees accessing such sites. However, it is important to bear in mind that monitoring an employee's use of electronic equipment or websites would be classified as an activity which has certain regulations attached to it. Legal advice should be sought before engaging in any such monitoring.
- Incorporate within employment contracts an appropriate confidentiality clause, which would afford protection to the employer in the event that an employee posts confidential information on a social media site.

- Disciplinary action may be taken against employees who misuse a social media site to the detriment of the employer. In some cases, an employer could consider dismissal. Each case will turn on its facts and an employer might want to obtain legal advice before proceeding to dismiss the employee in question.

Contributed by Havel & Holásek s.r.o.

CZECH REPUBLIC

DENMARK

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Unlawful discrimination

Checking prospective employees' social media profiles as part of an application screening/background check process can expose an employer to discrimination claims.

Social media websites typically reveal certain characteristics about an individual, which are protected from discrimination under Danish anti-discrimination legislation. Discrimination is prohibited on the basis of a person's race, religion, disability, age, sexual preference, political beliefs and pregnancy, among other characteristics.

The employer will only be exposed to a claim for discrimination if the applicant is made aware that their social media profile has been checked as part of the recruitment process. Even then, just because a rejected job applicant has a protected characteristic, and the employer admits to knowing about the characteristic because it has checked a social media website, this will not in itself be enough to violate anti-discrimination legislation. However, the risk of a discrimination claim being made against an employer is increased in such circumstances. That said, the likelihood of such a claim being successful would be low, unless there was other evidence of discrimination.

Potential implications relating to data protection

Reviewing social media profiles for recruitment purposes will amount to the "processing" of personal data under data protection legislation and is therefore subject to certain regulations.

As a general rule, employers will be entitled to access publicly available social media profiles of applicants as part of their recruitment process. Neither the applicant's nor the employee's consent is required.

Any processing of personal data retrieved from a social media profile must only be for a legitimate purpose, and only to the extent that is necessary for that purpose. Therefore, employers are not permitted to access employee profiles simply out of curiosity.

Applicants and employees must be notified in writing of the employer's intention to collect personal data via their social media profiles. As mentioned above, their consent is not needed should an employer simply access personal data which is publicly available. The notification must include certain minimum information, including the identity of the data controller, the purpose of the processing, intra group/third party recipients of data, as well as a summary of the employee's/applicant's rights (for example, the right to access the data held, the opportunity to correct any incorrect data). If employees' use of social media is monitored, such monitoring must also be described in detail.

Employees should be notified by way of a separate policy, or amending an existing policy. Notification to applicants could be given when confirming receipt of their job application.

Currently, only very few Danish employers have social media policies or other policies in place which deal with the processing of personal data via social media profiles. This is despite the use of social media in the workplace being very widespread in Denmark. According to surveys, Denmark has one of the highest Facebook profiles per capita ratios. This could suggest that, in reality, very few employers actually comply with the legislation governing the processing of data retrieved from social media profiles.

Presumably, the reason for the apparent widespread non-compliance is lack of awareness and readiness for the legal challenges created by the use of social media in the workplace. The fact that the sanctions for non-compliance are minimal may also play a part. In most cases, the most detrimental

sanction would be negative Patrick Race, as the decisions of data protection cases are published on the internet, which is continuously checked by journalists.

2. *What steps can be taken by employers to minimise such risks?*

Obviously, the safest approach would be to ban the screening of applicant/employee social media profiles. However, less restrictive options are available. These include:

- giving clear written instructions to employees and external consultants to only extract legitimate and relevant information, and to avoid extracting information which could lead to discrimination claims;
- issuing a social media policy, or similar, for the purpose of being able to demonstrate that the employer has taken appropriate action to ensure compliance;
- providing training to the employees involved in processing personal data collected from social media profiles; and
- allowing applicants/employees the opportunity to correct any information collated from a social media site, unless this would frustrate other more compelling reasons, e.g. the integrity of an investigation into an employee's misconduct.

3. *What problems could an employer face as a result of employees using social media sites?*

Social media sites allow employees (and managers) to communicate with the general public. Consequently, there is an inherent risk of employees intentionally or unintentionally harming the employer's interests when using social media, e.g. by:

- sharing confidential information with the general public;

- making statements on behalf of the employer (or on their own behalf) which are not supported by the employer and/or conflict with the employer's interests;
- exposing the employer to IT-security risks by downloading "high risk" material, such as opening messages from unknown senders, installing software of unknown origin, etc.;
- interacting with customers and other employer stakeholders in a negative way;
- violating applicable laws (infringement of third party IP-rights, defamation, false/hidden advertising, etc.), causing employer liability or causing employer disputes with other employees.

Furthermore, an obvious risk is the loss of production among the workforce due to working hours being spent using social media websites. Many Danish employers are highly focused on combating this. However, this risk should be considered in light of the fact that, for many employees, using social media is simply an alternative to other non-work-related activities, such as internet surfing, coffee machine conversations and running errands. In some cases, the employees may be generating value for the employer through using such social media, e.g. by engaging in positive interaction with co-workers, customers and other employer stakeholders.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

As a general guideline, any employer should (i) review its policy on employee use of social media in the workplace, (ii) communicate the policy to the employees, and (iii) take appropriate steps to ensure that the policy is respected by employees.

(i) Reviewing the employer's policy:

- Analysis

  An employer should analyse the actual use of social media in the workplace. They should look at the specific risks and opportunities associated with such use and therefore whether to allow or ban such use. Employers should also consider how best to encourage employees to act consistently with (or at least not in conflict with) the employer's interests when using social media in and outside of the workplace.

- Should employee use of social media at work be banned?

  This will depend on the individual circumstances. For example, an employer may wish to impose a ban for IT security reasons in companies where integrity and security is particularly important (such as banks) or where the company is experiencing problems with lost production (i.e. working hours spent using social media without generating value for the employer). A ban will not eliminate all risks related to employee use of social media, since employees will still have access to social media in their spare time and will still be able to make statements regarding the employer, their customers or colleagues, and share confidential information in that way.

  The employer should also consider the disadvantages to a ban. The employer will not be able to take advantage of the possibilities associated with employee use of social media in the workplace, including positive interaction with stakeholders, employer branding, attracting talent, etc. Furthermore, employees and (potential) applicants

may react negatively, especially in companies where the employees are expected to demonstrate flexibility with regards to working hours and their work-life-balance in general. The important thing is to make an informed decision based on the individual circumstances of the company in question. The employer should be in a position to give a credible and compelling explanation to the employees if they choose to input a ban, rather than imposing the restriction without further consideration.

(ii) Communicating the policy:

- The employer should issue a written policy, setting out employee use of social media in and outside the workplace. There are many advantages to having a written policy, including alignment of employee and employer expectations, promoting behaviour consistent with the employer's interests, creating legal and moral grounds for sanctions against misconduct, and demonstrating responsible corporate governance. Key elements to be included in a social media policy are: vision/values behind policy; statements promoting employee awareness of the risks and opportunities related to social media use; general guidelines for acceptable behaviour; specific dos and don'ts; employer monitoring, if relevant; and disciplinary sanctions for violation of the policy.

(iii) Taking appropriate steps:

- Training

  Employees should be given training on their use of social media. Generally, employee training is a good way of promoting compliance with the relevant policies. Key elements to cover in such

training would be: avoiding beginner mistakes; acting consistently with company policy; avoiding discrimination and bullying; defining privacy settings; and generally promoting employee awareness of the risks and opportunities.

- Monitoring employee use

  Most Danish employers already monitor employees' use of IT facilities to a certain extent. If an employer explicitly reserves the right to monitor use of social media via the employer's IT facilities (or social media profiles in general), and actually takes action when appropriate, the effect should be to promote appropriate employee behaviour and demonstrate sound corporate governance. On the other hand, such monitoring could be seen as an unjustified invasion of privacy. Monitoring of employees' use of social media should generally not be commenced before legal advice is taken.

- Enforcing the policy

  It is important that any social media policy is in fact enforced. Otherwise, it will lose legal weight and compliance by employees.

Contributed by Kromann Reumert

DENMARK

EGYPT

1. *Are there any risks for employers that use social media sites to vet job applicants?*

An employer has the right to vet job applicants by using information on social media sites. An employer will require certain information about a prospective employee before they can make them an offer of employment. Such information may include details of the candidate's/employee's qualifications, his/her marital status and/or whether they have children, age, sex, nationality, a copy of his/her identification card or passport and a reference from a former employer. It is unlikely all this information will be included in an applicant's CV, but it may feature on a social media website profile.

Discrimination based on sex, ethnic origin, language, religion or belief, colour, sex, marital status, status as a parent, family obligations, pregnancy, or political views is prohibited, but only in relation to employees. Therefore termination of an employment contract on the basis of any of these characteristics will be unlawful, but job applicants are not afforded the same protection.

2. *What steps can be taken by employers to minimise such risks?*

There are not any inherent legal risks for employers who wish to vet job applicants using information from social media. However, the information from such sites may not be entirely accurate. There are a number of steps which employers can take to guard against unnecessary risk:

- Those scanning social media sites as part of the recruitment process should be instructed to extract only legitimate and relevant information for the job application process.
- A social media policy or other written guidelines should back this up, so that the employer can demonstrate an intention to extract only relevant information.

- Ideally, the person scanning the social media sites should not be the same as the person who is determining the job application process or interviewing the individual. This way, the irrelevant material (which might contain sensitive personal data) will not make its way through to the decision maker. This is at the employer's discretion.
- Applicants should be told, at the start of any application process, that a vetting or verification exercise using social media sites forms part of the process.
- Job applicants who are rejected because of information gleaned from social networking should be given an opportunity to correct that information before any final decisions are taken.

3. *What problems could an employer face as a result of employees using social media sites?*

Breach of confidentiality

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social media platforms, it is not uncommon for employees to end up posting confidential information about the employer and/or other employees. This could result in significant damage to the employer's business and reputation.

Damage to employer's or third party's reputation

Employees could post information on a social media site that causes damage to the reputation of the employer and/or a third party. An employer may be vicariously liable for the defamatory conduct of an employee if the information used by the employee was obtained directly from the employer. The fact that an employer may have a claim against the employee concerned could be of little comfort compared to the damage to the reputation of the employer.

Harassment/Unlawful discrimination

It is not uncommon for employees to post negative comments about fellow employees on social media sites. The comments could relate to a protected characteristic such as age, disability, race or sex. If an employee were to make such comments 'in the course of their employment', there is a danger that this could constitute harassment under Egyptian law and a breach of the employer's internal policies. However, an employer will not be liable for the discriminatory conduct of their employees.

An employer could only be liable for the discriminatory conduct of its employees if the information which was used to discriminate was obtained from a social media site and it was the employer who provided that information to the site.

An employer will have a defence to any claim for discrimination or harassment if it can show that it took all reasonable steps to prevent the employee from committing the discriminatory act in question.

Loss of productivity

Allowing employees to access social media sites at work could have a negative effect on their productivity.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

An employer can take the following steps:

- Impose an outright ban on access to social media sites at work. This approach could prove to be unpopular amongst employees and have an adverse impact on the morale within a workforce. Ultimately, the employer would need to weigh up the potential advantages and disadvantages in deciding whether to permit employees to access social media sites at work. A complete ban would not address the potential problems that

could arise from postings by employees outside of working hours. Employers can easily find themselves liable for comments made after hours by employees, particularly where there is an obvious and clear link to the employment. Accordingly, comments posted by one employee about another employee after hours on a social networking site could still end up as the responsibility of the employer. This will only be the case where the comments were based on information which the employee obtained from the employer, or where that information was provided by the employer to the social media site.

- Put in place a social media policy which deals with the use of social media sites during and outside of work hours. Such a policy should have provisions dealing with social media activity but, in particular:
    - set out the parameters governing the use of the employer's IT systems;
    - remind employees that social media activity may not necessarily be private;
    - prohibit discrimination, harassment or bullying of other employees, which could include negative comments about employees posted on social media sites;
    - prohibit negative comments about the employer, its employees or third parties; and
    - prohibit the disclosure of any confidential information that relates to the employer and/or other employees.

The policy should set out the consequences of a breach of the policy, which could include disciplinary action and, ultimately, dismissal.

- Provide awareness training to employees on conduct that could constitute discrimination, harassment and bullying.
- Monitoring the use of social media sites at work could help to determine whether there is a loss of productivity as a result of employees accessing such sites.
- Incorporate within employment contracts an appropriate confidentiality clause, which would afford protection to the employer in the event that an employee posts confidential information on a social media site.
- Disciplinary action may be taken against employees who misuse a social media site to the detriment of the employer. In some cases, an employer could consider dismissal. Each case will turn on its facts, and an employer might want to obtain legal advice before proceeding to dismiss the employee in question.

Contributed by Shalakany Law Office

EGYPT

FINLAND

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Unlawful discrimination

Social media sites will often contain personal profiles of the individual concerned including certain characteristics, which form the basis of protection against discrimination under Finnish employment legislation. These characteristics could include the individual's sex, race, nationality, and ethnic origin, skin colour, spoken language, age, family situation, sexual orientation, health, religion, political opinions or activities or membership of a trade union. It is unlikely that most, if at all any, of these characteristics will feature in a CV. Therefore, if an employer has access to this information via a social media site and uses such information as the basis for refusing to recruit that person, then the employer's actions could constitute unlawful direct discrimination. The employer could face an increased risk of a claim for discrimination against it if the job applicant were to discover that their application was rejected because of one or more of the above characteristics.

Potential data protection implications

In principle, it is possible for employers to carry out pre-employment checks on applicants in Finland. However, it is quite unlikely that using social media sites for such checks would comply with the somewhat strict and detailed rules governing the vetting of potential new employees.

The general principles regarding pre-employment checks are set out in data protection and privacy laws. Restrictions apply wherever an employer "processes" personal data. This covers the collection, use, transfer and disclosure of data, among other things. Any employer established in Finland or otherwise subject to Finnish law (this includes a non-resident employer using equipment for processing personal data which

is located in Finland) will have to comply with the legislation governing the use of personal data. There are privacy laws applicable to the work environment which complement the data protection laws which cover the processing of personal data in connection with employment relationships and job applications.

The most important issues for employers to bear in mind when using social media sites for pre-employment checks are:

(a) only information that is directly necessary for the application process may be retrieved (the necessity requirement); and

(b) no information regarding the applicant can be retrieved without the applicant's direct consent, or in some cases, without a prior notification that the employer will seek to obtain such information.

The necessity requirement is strict and cannot be deviated from even with the job applicant's consent. Furthermore, even if the employer has a job applicant's consent to access the applicant's information from a social media site, it is unlikely that the information obtained would be considered directly necessary for the application process. This is due to the nature of information on social media sites. Therefore, it would generally be contrary to Finnish law for an employer to use information from social media sites as a part of their recruitment process.

A recent case where an employer carried out a pre-employment check on an applicant by performing a "Google search" on them, established that collecting and saving personal information in this way was unlawful.

2. *What steps can be taken by employers to minimise such risks?*

As a general rule, an employer is allowed to collect personal data about an applicant from the applicant him/herself (provided that the necessity requirement discussed above is met). In order for an employer to legitimately collect personal data from other sources, e.g., from social media sites, the employer must obtain the applicant's prior consent.

According to Finnish law, the consent must be a "voluntary, detailed and a conscious expression of will". The applicant must be notified that their consent is required and therefore, no form of "tacit consent" will be considered valid for this purpose. As such, it is recommended that employers obtain written consent before performing any kind of pre-employment checks.

It is also recommended that an employer ensures that its personnel who are conducting the pre-employment checks (and who could potentially scan social media sites) are aware of the strict and detailed rules governing the recruitment process in Finland.

3. *What problems could an employer face as a result of employees using social media sites?*

Breach of confidentiality and insider rules

Both intentional and unintentional disclosure of business secrets or information subject to a non-disclosure agreement, on a social media site, could constitute a breach of confidentiality. In addition, any kind of disclosure of inside information will constitute a breach of insider rules under the Securities Markets Act. Employers and employees should be aware that even if certain aspects of the information that is released does not breach confidentiality or insider rules, several individual pieces of information published by an employee at different times or on different social media sites, together could lead to a breach of confidentiality or insider rules.

Damage to employer's or third party's reputation

Employees will often express their opinions on social media sites and therefore there is a potential risk for employers. Comments relating to company activities, customers and/or services are commonly found on social media sites. Employees could cause damage to the employer's or a third party's reputation by posting negative or false information about the company on a social media site.

There are also potential issues surrounding intellectual property rights. An employee may use a company's trade mark and business name improperly or without permission, inadvertently breaching certain rules. This could also affect an employee's reputation.

Unlawful discrimination and harassment

Employees could potentially post comments about their fellow employees on social media sites which amount to discrimination or harassment. This could result in the employee being liable for unlawful discrimination. The employer's reputation may also be adversely affected if some of its employees were found guilty of discrimination. Furthermore, if an employee is subject to harassment based on a prohibited ground and the employer is aware of the harassment but does nothing about it, the employer could be liable for discrimination. This could result in the employer being subject to a fine or up to 6 months imprisonment.

Loss of productivity

In addition to the potential legal issues described above, the use of social media during working hours can obviously have a negative impact on employees' productivity.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

An employer has a right to regulate and supervise the use of its electronic equipment. An employer could ban access to social media sites at work altogether however, often a complete ban is not the most appropriate or practical way of handling the risks associated with social media. An employer is not permitted to monitor the use of social media sites at work if such monitoring will reveal information regarding an individual employee's use of the internet. This type of information would be protected under Finnish law by the right to privacy of communications.

In order to deal with the possible challenges described above, employers should create a policy regarding the use of social media sites during and outside of working hours. The policy should include general rules of conduct for employees on social media sites, information regarding privacy settings (especially from the viewpoint of data security), prohibition of any disclosure of company's confidential information, inappropriate conduct (e.g. publishing negative comments about the employer or third parties, discrimination or harassment) and consequences of breaching the policy.

If an employee breaches a social media policy, the employer should be in a position to take disciplinary action against that employee. However, the seriousness and the extent of a disciplinary action will have to be assessed carefully on a case by case basis. For minor breaches, a warning is likely to be most appropriate. In severe cases, it could be necessary to evaluate whether there are grounds for ending the employment relationship. If the employer has suffered a loss due to the employee's misuse of a social media site, the employer could be entitled to damages. Employees also have a legal duty of loyalty towards their employer which, if breached, may give rise to disciplinary action. Whether this duty is relevant will depend on the employee's conduct.

FINLAND

To date there have been only a few cases before the Finnish courts regarding employees' inappropriate conduct using social media sites. So far only one judgment has been rendered. This case involved an employee who had posted negative comments about her employer on Facebook and other social media sites and had urged customers to boycott the employer's shops. However, the court held there was insufficient evidence that damage had been incurred by the employer so the claim for damages failed.

Contributed by Dittmar & Indrenius

FRANCE

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Unlawful discrimination

It is possible for French employers to consult social media sites to screen job applications prior to, or in the course of, the recruitment process. However, French employment law prohibits any discrimination against applicants based on a number of defined criteria. Information relating to such criteria could be contained in an individual's personal profile on a social networking site.

Under the French Labor Code, no person can be rejected from a recruitment process on the basis of a protected characteristic such as their gender, sexual orientation, age, marital status, pregnancy, ethnic group or origin, nationality, race, political or religious belief, trade union activities, physical appearance, last name or disability.

If an applicant feels that they have been unlawfully discriminated against during the recruitment process, they may be able to bring a claim against the employer. In order to bring such a claim, the applicant would have to provide evidence which suggests that the prospective employer has directly or indirectly discriminated against them by using information obtained from a social media site. It is then for the employer to prove that their decision not to hire the applicant was based on objective non-discriminatory criteria.

In practice, however, it will rarely be possible for applicants to prove that they have been discriminated against through the employer's use of social media in the recruitment process.

From a criminal law perspective, if an employer refuses to employ an applicant for an unlawful reason, this constitutes a criminal offence, which can be punishable by a three-year prison sentence and a maximum fine of €45,000. The only exception to this is for cases where sex, age or physical

appearance is an essential and determining requirement for the role, and there is a legitimate and proportionate objective for discriminating on that basis.

Relevance of data collected

Under French law, the information requested/obtained about a job applicant, in whatever format, from the applicant must be for the sole purpose of assessing their capability for the job offered or their professional skills.

This information must have a direct and necessary link with the job offered or with the assessment of their professional skills. The applicant must answer these requests for information in good faith. This applies to questionnaires given to applicants in order to establish their profile. However, it could also apply to an employer's use of social media to screen the applicant.

Informing the employees and Works Council

Applicants should be informed of the methods and techniques used in the recruitment process prior to its commencement.

No personal information concerning the applicant can be collected through a medium which has not been brought to the applicant's attention beforehand. Therefore, if an employer wanted to refer to an applicant's social media profile as part of the recruitment process, they would need to tell the applicant before doing so.

If the employer has recognised a Works Council, it must also be informed of the methods and techniques used for recruitment purposes prior to their implementation. Its consent is, however, not required.

Potential data protection implications

The CNIL (French data protection authority) has specified that the following information cannot be lawfully requested

from applicants (except in specific circumstances): date on which French citizenship was acquired, nationality of origin, social security registration number, military situation, former address, information in relation to the family (spouse, parents, sisters, brothers, children), health, size, weight, eyesight, ownership or rental of house, bank references, and loans.

Again, it will rarely be possible for applicants to prove that a company has had recourse to, and relied on, social media in their recruitment process, particularly where it is not an official practice within the company. It will therefore be rare for an applicant to bring a claim against the employer for not informing them prior to consulting social media sites.

The CNIL recently made a release to warn people of the potential risks of social media. They advised people to be cautious with what information they put on social media sites and to use restriction accesses/parameters of their accounts.

According to data protection legislation, an employer is required to declare any information in relation to recruitment to the French Data Protection Agency. This must be done prior to the data being processed, and the job applicants must also be informed that data on them is being collected and processed. The applicants should be informed of their right to access and amend the personal data that the employer holds on them.

2. What steps can be taken by employers to minimise such risks?

Assuming employers do not wish to take steps to ban all vetting of job applicants using information from social media, there are a number of steps which can be taken to guard against unnecessary risk:

- The CNIL has advised that an applicant's details should be managed centrally by the employer so that information is kept up to date, and to ensure that the employer does not keep the information for longer than

is necessary. The CNIL believes that having centralised management of data should enable applicants to access and modify their personal data, which they have a right to do under data protection regulations.

- The employer should ensure that its recruiters are not discriminating against applicants, based on one or more of the prohibited criteria set out above, when using social media in recruitment. The employer should offer training to those affected and told to only extract legitimate, relevant information for the job application process.
- Ideally, the person scanning the social media sites should not be the same as the person who is determining the job application process or interviewing the individual. This way, the irrelevant material (which might contain sensitive personal data) will not make its way through to the decision maker.
- The employer should create a policy setting out how a recruitment process, properly conducted, should be developed.
- The employer should ensure that they tell applicants and the Works Council (if one is recognised) that they will refer to social media sites during the recruitment process prior to using such sites.
- Job applicants who are rejected because of information gleaned from social networking should be given an opportunity to correct that information.

3. *What problems could an employer face as a result of employees using social media sites?*

Breach of confidentiality

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social

media platforms, it is not uncommon for employees to end up posting confidential information about the employer and/or other employees. This could result in significant damage to the employer's business and reputation.

Damage to employer's or third party's reputation

Employees could post information on a social media site that causes damage to the reputation of the employer and/or a third party. An employer may be vicariously liable for the defamatory conduct of an employee if it is proved that the damage was caused by an employee in the course of their employment. The only exception would be where the employee willingly exceeded the limits of their duties, but it is very seldom accepted by courts. The fact that an employer may have a claim against the employee concerned could be of little comfort compared to the damage to the reputation of the employer.

Recent cases have held that dismissing/disciplining employees for making damaging and disparaging comments on social networking pages was not a violation of the employee's privacy or freedom of speech. Social media sites were not considered to be a private space by the courts.

Harassment/Unlawful discrimination

It is not uncommon for employees to post negative comments about fellow employees on social media sites. The comments could relate to a protected characteristic such as age, disability, race or sex. If an employee were to make such comments 'in the course of their employment', an employer could be vicariously liable for the actions of that employee.

An employer could also risk facing other discrimination claims if employees use information they have obtained from social media sites about other employees as the basis for treating them in a detrimental way.

An employer will have a defence to any claim for discrimination or harassment if it can show that it took all reasonable steps to prevent the employee from committing the discriminatory act in question.

Loss of productivity

In addition to the issues described above, allowing employees to access social media sites while at work could affect their productivity.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

Employees have a duty of loyalty towards their employers in the course of their employment. Despite their entitlement to freedom of speech, employees would be in breach of their duty of loyalty if they were to make derogatory statements or defame their employers and/or colleagues publicly.

In light of the above, companies could:

- ban access to social networks: this solution is becoming more redundant as, increasingly, employees have smart phones, which allow them to access the social media websites without using the company's Internet connection or computer equipment.

  Moreover, it does not solve the problem once the employee is outside of the office environment;

- create an official company social media forum where employees can communicate with each other within the company, with the employer acting as a Webmaster, and put appropriate rules in place to ensure that there is no misuse.

  This could facilitate communication between employees within the company and reduce the need for them to use other social media sites. The employer may be able to

use this internal social media to prevent and defuse work tensions;

- set out the rules relating to the use of social media in the company's internal rules, or in a dedicated policy, that all employees are obliged to adhere to.

  Such a policy should prohibit discrimination, harassment or bullying of other employees, which could include negative comments about employees posted on social media sites. It should also prohibit negative comments being made about the employer or third parties in this way. Disclosure of confidential information should also be prohibited;

- ensure that the internal rules or policy make it clear that posting messages on social media websites could lead to disciplinary sanctions if disparaging or unlawful comments are made about the company, or if a provision in their employment agreements is breached (such as confidentiality, non-compete, non-solicitation, non-poaching). Disciplinary action may be taken for a more general reason, such as being disloyal to the company. The employer could add that sanctions may be incurred if the employee's right to freedom of speech is misused in such a way as to cause harm to the employer or its employees, even outside the company's premises and working hours;

- organise short training awareness sessions for employees on the possible adverse effects and sanctions of any misuse of social media. Employers should make it clear that social media websites are not (at least, not always) a private space;

- monitor the use of social media sites at work. This could help to determine whether there is a loss of productivity as a result of employees accessing such sites. However, legal advice should be sought before engaging in any

such monitoring, and an internal policy should be developed which deals with this;

- discipline an employee, should they become aware of the disloyal content of any message posted on a social networking site;
- initiate legal action before the civil or criminal courts if the employer is the victim of defamation, denigration or insults (which can constitute a criminal offence).

With regards to the last three points above, legal advice should be sought before embarking on any of these options.

Contributed by Mayer Brown

GERMANY

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Social media profiles will often contain information that is rarely featured in a job applicant's CV. Therefore, an increasing number of employers regard social media sites as a useful source of information for the recruitment process. However, the employer's understandable desire to learn as much as possible about an applicant may conflict with the applicant's personal rights. Obtaining information on applicants through social media sites can pose two risks for employers: (i) the risk that the employer could use that information in a way that could amount to unlawful discrimination and (ii) the risk that data privacy laws will be violated.

Risk of unlawful discrimination

German legislation governing equal treatment protects job applicants and employees against direct or indirect unlawful discrimination based on characteristics such as race, ethnic origin, gender, religion or secular belief, disability, age or sexual identity. These characteristics are often contained in social media profiles.

If an employer obtains such information through social media sites when vetting a job applicant and decides not to hire an applicant on the basis of that information, it could face a claim for unlawful discrimination. However, in order to bring such a claim, the applicant would need to know that the employer accessed his/her social media profile. In principle, the applicant bears the burden of proving that unlawful discrimination has taken place. The applicant would need to establish evidence that the employer's refusal to hire them was based on one of the characteristics outlined above. However, if the applicant can indicate that unlawful discrimination has taken place (such as the employee being able to show that the employer accessed their social media profile and

that the protected characteristic was contained therein), legislation provides for a reversal of the burden of proof. It would therefore be for the employer to show that they had not unlawfully discriminated against the applicant.

If an applicant has been discriminated against, they would be entitled to damages as well as compensation for pain and suffering. A claim must be brought within two months following the refusal of employment. Therefore, it is crucial that the employer is clear as to when the refusal was communicated to the applicant.

Risk of violation of data privacy

Social media profiles contain personal data within the meaning of the German data protection law. Personal data means any information related to an individual who can be identified from that information.

One of the principles of data protection law is that personal data must be collected directly from the individual, i.e. the applicant. As an exception to this rule any personal data that is publicly accessible, e.g. through a search engine such as Google, may generally be used by the employer. This is due to the fact that the applicant waived his/her right to privacy when publishing the information in question. Having said that, an exception must be made where it becomes evident that a third person has uploaded the information on the applicant. In this situation, the applicant's privacy will prevail over the employer's interest to collect such information.

Where personal data is collected from social media networks, a distinction must be made between private and professional networks. Data from private networks cannot be collected by employers as the applicant's privacy outweighs the employer's interests in learning more about the background of a prospective employee. This contrasts with professional networks which are typically used by their members to present

their professional qualifications. Therefore, information from such professional networks may be obtained and used by employers.

Where the provisions of data protection law are violated by an employer in the context of social media, the employer may face compensation claims from the applicant who is the subject of that data. Furthermore, the employer may be committing a regulatory offence.

2. What steps can be taken by employers to minimise such risks?

- The employer must inform its data protection officer before it vets job applicants through social media networks.
- The online search should be restricted to professional social networks to avoid the collection of any "inappropriate" personal data. It is also advisable to implement a research guideline to establish the employer's intention to extract relevant and appropriate information only.
- The person that conducts the online research should be different from the person that conducts the job interview and decides whether or not the applicant is hired. This will ensure that no inappropriate information that may have been discovered in the course of the online search will be used in the recruitment process.
- During the job interview the applicant should be given the chance to correct any outdated or potentially incorrect information that the employer has gained knowledge of by means of an online search.
- The German parliament is currently considering whether to make the collection of publicly accessible personal data relating to a job applicant only permissible if the applicant has been previously informed that this

will be the case. In the future, employers may be required to expressly state in job advertisements that publicly accessible data will be used during the recruitment process.

- The works council, if any, has a mandatory co-determination right to participate in the recruitment process under German law. The results of the employer's internet search may have to be made available to the works council along with the application documents submitted by the applicant.
- Personal data that is no longer required should be deleted. Where an applicant is refused, his/her personal data should be deleted once two months following the rejection have passed. At that point, any claims by the applicant will have expired.

3. *What problems could an employer face as a result of employees using social media sites?*

Damage to employer's reputation

Social networks provide an opportunity for the employees to post statements for everyone to read. Obviously, the risk is that this forum will be abused by dissatisfied employees to post negative comments about the employer. Even if there were no bad intentions, any statements regarding the employer, its business or its workforce could be mistaken for an official statement, depending on the employee's status within the employer's organization and the network or forum that is used. Both scenarios can pose a threat to the employer's reputation.

Breach of confidentiality

Employees could post information that qualifies as a business or trade secret of the employer out of thoughtlessness or because they become talkative when chatting with like-

minded people. This could result in damage to the employer's business.

Where an employee breaches confidentiality and this results in damage to a third party's (e.g. the employer's customer) reputation or interest, the employer could be held liable for any damage thereby caused.

Unlawful discrimination

Employees might also post offensive statements regarding colleagues on social networks which amounts to discrimination. An employer could face claims for compensation from the affected employees if it fails to intervene or take steps to prevent discrimination among the staff. The claim would be for the employer's failure to fulfil its protective duties towards its employees.

Loss of productivity

Aside from the potential legal issues, there could, of course, be a negative impact on employees' productivity should the employer permit them to access and use social media sites during work hours.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

- Employers should implement clear regulations as to whether the company IT equipment may be used for private purposes to access the internet generally and social networks in particular. From a legal perspective, it is advisable to ban private use of the company IT in the workplace. However, nowadays many employers regard the right to use the internet in the workplace for private purposes as an additional incentive for employees. In that case, it should be considered whether the private use could be limited in respect of timing (preferably outside working hours and only to a reasonable extent) and

content. Also, employers should explicitly reserve the right to monitor the employees' movements to the extent permitted by law or gain the employees' assent to such reserved measures.

Moreover, a social media policy should be developed. Such a policy should have provisions dealing with social media activity, but in particular:

- Provide whether or not social networks may be accessed in the workplace and the Dos and Don'ts – in particular, what must not be posted (for instance information that may qualify as a business or trade secret, offensive comments about the employer or colleagues).
- Emphasize the employee's contractual obligations to secrecy and loyalty as well as restrictions imposed by competition law, copyright and trademark law or any other statutory provisions or resulting from third parties' personal rights.
- Stress the employee's responsibility for his/her actions within social networks and increase awareness of risks associated with the use of social media e.g. their activity may not be private. Every employee represents the company.
- Clarify the potential legal consequences resulting from a violation, e.g. disciplinary action, a warning, ordinary dismissal with notice or even a dismissal for cause with immediate effect, damage claims, criminal liability.

• Employers who provide awareness training for their employees are deemed to have fulfilled their protective duties towards their workforce and job applicants.

- Employers must comply with the works council's rights to information and co-determination when introducing a social media policy and any systems or devices that enable the employer to monitor the employees' internet use.

Contributed by Mayer Brown LLP

GERMANY

GREECE

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Unlawful discrimination

Personal profiles on social media sites will often contain certain information about a person which is protected from discrimination under Greek equal treatment legislation. Characteristics which are protected from discrimination include sex, race and family status (i.e. whether married, divorced, widowed, and number of dependants). In Greece, candidates would normally include basic information regarding their family situation, such as their marital status and the number and age of their children, on their CV. The reason for this is to disclose the employee's entitlement to benefits which the employer is compelled to provide. If an employer uses such information, whether obtained via a social media site or otherwise, as the basis for refusing to recruit that person, this could potentially constitute unlawful direct or indirect discrimination. The employer could expose itself to a claim if the applicant could provide evidence that the application was rejected on the basis of one or more of the above characteristics. We consider, however, that such cases would be rare in the private sector as an employer can exercise its discretion when selecting successful candidates. It would be difficult for an applicant to evidence in court that the reason for the employer not selecting them was because the employer was influenced by information available on a social media site.

Potential implications under data protection laws

Vetting job applicants using information contained on social media sites could also have implications for employers in respect of their obligations under data protection law. There is legislation in place which regulates the collection and use of 'personal data'. Personal data is information relating to an individual who can be identified from that information.

'Sensitive' personal data includes information relating to a person's race or religion, political convictions, trade-union membership, sex life and/or a criminal prosecution. Employers have onerous obligations when 'processing' sensitive personal data. 'Processing' includes obtaining, recording, holding or using personal data. Therefore, when an employer collects information about an applicant from a social media site, it may be processing sensitive information. In such circumstances, employers must comply with general data protection principles, question as to whether or not the information obtained from social media sites is accurate, and whether it is proportionate to use it for recruitment purposes.

Sensitive data can usually only be processed if the applicant has given explicit consent and a licence to process sensitive data has been obtained from the Data Protection Authority (the Greek authority that enforces individuals' information and data privacy rights). Failure to comply with these data protection principles could result in claims for compensation being made against the employer, or action being taken against it by the Data Protection Authority.

There is guidance in place for employers regarding the recruitment and selection process. The guidance provides that a background check on an employee is lawful, provided that the candidate has been informed and has consented to it. As a result of this general obligation, job applicants should be given the opportunity to comment on the accuracy of any background checks or information that the recruiter has obtained about them.

2. What steps can be taken by employers to minimise such risks?

Assuming employers do not wish to take steps to ban all vetting of job applicants using information from social media, there are a number of steps which can be taken to guard against unnecessary risk:

- Applicants should be told, at the start of any application process, that a vetting or verification exercise using social media sites forms part of the process, and their consent should be obtained.
- Those scanning social media sites as part of the recruitment process should be instructed to extract only legitimate and relevant information for the job application process.
- A social media policy or other written guidelines should back this up, so that the employer can demonstrate an intention to extract only relevant information.
- Sensitive personal data should not be processed without a licence from the Data Protection Authority.
- Job applicants who are rejected because of information gleaned from social networking sites should be given an opportunity to correct that information before any final decisions are taken.

3. *What problems could an employer face as a result of employees using social media sites?*

Breach of confidentiality

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social media platforms, it is not uncommon for employees to end up posting confidential information about the employer and/or other employees. This could result in significant damage to the employer's business and reputation.

Damage to employer's or third party's reputation

Employees could post information on a social media site that causes damage to the reputation of the employer and/or a third party. An employer may be vicariously liable for the defamatory conduct of an employee. The fact that an

employer may have a claim against the employee concerned could be of little comfort compared to the damage to the reputation of the employer.

Harassment/Unlawful discrimination

It is not uncommon for employees to post negative comments about fellow employees on social media sites. The comments could relate to a protected characteristic such as age, disability, race or sex. If an employee were to make such comments there is a danger that these could amount to an offence under Greek law. If the comments are made 'in the course of their employment', then an employer could potentially be vicariously liable for the actions of that employee.

An employer could also risk facing other discrimination claims if employees use information they have obtained from social media sites about other employees as the basis for treating them in a detrimental way.

An employer will have a defence to any claim for discrimination or harassment if it can show that it took all reasonable steps to prevent the employee from behaving in a manner that amounts to discrimination or harassment.

Loss of productivity

Allowing employees to access and use social media sites while at work could have an obvious impact on their efficiency and productivity.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

An employer can take the following steps:

- Impose an outright ban on access to social media sites at work. This approach could prove to be unpopular amongst employees and have an adverse impact on the

morale within a workforce. Ultimately, the employer would need to weigh up the potential advantages and disadvantages in deciding whether to permit employees to access social media sites at work. A complete ban would not address the potential problems that could arise from postings by employees outside of working hours. Employers can easily find themselves liable for comments made after hours by employees, particularly where there is an obvious and clear link to the employment. Accordingly, comments posted by one employee about another employee after hours on a social networking site could still end up as the responsibility of the employer.

- Put in place a social media policy which deals with the use of social media sites during and outside of work hours. Such a policy should have provisions dealing with social media activity, but in particular:
    - set out the parameters governing the use of the employer's IT systems;
    - remind employees that social media activity may not necessarily be private;
    - prohibit discrimination, harassment or bullying of other employees, which could include negative comments about employees posted on social media sites;
    - prohibit negative comments about the employer, its employees or third parties; and
    - prohibit the disclosure of any confidential information that relates to the employer and/or other employees.

  The policy should set out the consequences of a breach of the policy, which could include disciplinary action or dismissal.

- Provide awareness training to employees on conduct that could constitute discrimination, harassment and bullying. An employer would be able to defend any subsequent claim for discrimination or harassment if it can show that it took all reasonable steps to prevent the employee from committing the discriminatory act in question.
- Monitoring the use of social media sites at work could help to determine whether there is a loss of productivity as a result of employees accessing such sites. However, it is important to bear in mind that electronic forms of workplace surveillance would involve activity regulated under data protection laws. Legal advice should be sought before engaging in any such monitoring.
- Incorporate within employment contracts an appropriate confidentiality clause, which would afford protection to the employer in the event that an employee posts confidential information on a social media site.
- Disciplinary action may be taken against employees who misuse a social media site to the detriment of the employer, provided that there is an approved Employment Regulation in place adopted in accordance with legal requirements. In some cases, an employer could consider dismissal. Each case will turn on its facts, and an employer might want to obtain legal advice before proceeding to dismiss the employee in question.

Contributed by M & P Bernitsas Law Offices

HUNGARY

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Unlawful discrimination

Social media sites often contain personal information within individual's profiles which is not strictly connected, or relevant, to their employment. Examples of such characteristics would be age, pregnancy, maternity, race (including nationality), religion or belief, sexual orientation, marriage or civil partnership status. In most cases, it is unlikely that this information would be revealed in a CV or interview with the employer.

Hungarian equal treatment and anti-discrimination legislation provides that any direct or indirect discrimination in the course of employment is prohibited. This includes discrimination in relation to the hiring of a new employee. Employers can only carry out pre-employment checks to the extent that the employee's personal rights are not violated under this legislation, and only to a degree that is necessary prior to making an offer of employment.

If an employer uses information which is not directly connected to employment, and was obtained via a social media site, as the basis for refusing to recruit an applicant, the employer could be liable for unlawful discrimination if the information relates to a protected characteristic. If, however, the information is connected to the employment (e.g. the applicant's work history, competency or any characteristics that are a key issue for employment), and that information is available for the public to view on a social media site, using such information in the recruitment process is not prevented by Hungarian law.

Potential implications under the Data Protection Act

There is legislation in place which governs the protection of personal data and the publication of data which is in

the public interest (the "Data Protection Act"). It regulates data processing, which includes the collection, recording, organisation, storage, adaptation or alteration, use, disclosure, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction of data. The Data Protection Act defines 'personal data' as any information relating to an individual who can be identified, whether directly or indirectly, from the information. Processing of personal data requires the consent of the individual it concerns. The Data Protection Act requires written consent to be given where the data processed is sensitive (for example, data related to racial or national origin, nationality and ethnic status, political opinion or party affiliation, religious or other convictions, as well as data related to health or a person's criminal record).

Based on the above, if the employer collects information about the employee from a social media site that is not connected or relevant to employment, this may amount to unlawful data processing. The collection or maintaining of data constitutes data processing. A court has recently ruled that when an employee uploads their personal information onto a social media site, they have only given their consent to the site using their information, and have not given consent to an employer to use it for employment purposes. Using this information for any other purpose will constitute a breach of data protection laws and the individual's personal rights. In addition, if sensitive information is collected from such a site and kept by an employer, this could also constitute a violation of the Data Protection Act as the written consent of the data subject has not been obtained.

If the information is connected to employment and it is published on a social media site accessible to anybody, the use of such information is not prevented by Hungarian law. However, as referred to above, the Hungarian courts have interpreted this very strictly.

It is unlikely, but theoretically possible, that an employee gives his/her consent to the employer to access restricted information available on a social media site (i.e. a closed profile). If the employee gives their consent and the information is connected to the employment, the information may be used for employment purposes. If, however, the information is irrelevant for employment purposes, regardless of whether the employee has given his consent, the employer cannot legitimately use such information for employment purposes. This could amount to a breach of data protection laws because the legitimate purpose needed for data processing is missing.

Failure to comply with data protection requirements could result in claims for compensation against the employer or an action by the Hungarian Data Protection Commissioner being brought.

An information memorandum published by the Data Protection Commissioner encourages users of social media sites to only publish personal information which they would be happy for anyone to review. The Commissioner also suggests that individuals restrict who can access such information.

2. *What steps can be taken by the employers to minimize such risks?*

If an employer decides to use information about a job applicant taken from a social media site, the following actions should be taken in order to avoid unnecessary risk:

- If the employer wishes to use information that is connected to the employment, and it is not available to the public, it should obtain the applicant's consent to use such information.
- Once the applicant's consent has been obtained, the HR personnel who scan social media sites as a part of the recruitment process should be instructed to collect

only legitimate and relevant information about the job applicant which is strictly necessary for the employment (e.g. details as to graduation, previous schools, previous work places, language skills, etc). As a key principle, data that is not strictly relevant to employment (and almost all sensitive personal data) should not be collected and used in the application process.

- Employers should implement a social media policy or other written guidelines to be adhered to by those conducting the recruitment process. This way, the employer will be able to demonstrate an intention to extract only relevant information. This will help to avoid or minimise any unlawful behaviour. It is advisable that the policy states that only public profiles can be looked at in the course of the recruitment process, unless the employee has given his explicit consent to look at closed profiles as well.
- Applicants should be informed, at the start of any application process, that scanning social media sites is part of the application process, and their consent to this obtained. This should also be declared in the social media policy of the employer.
- Job applicants who are rejected because of information obtained from social media sites should be given the opportunity to correct such information before final decisions are made. This way, the risk of a rejected applicant raising a claim against the employer for unlawful discrimination, may be reduced.
- Ideally, the person scanning the social media sites should not be the same as the person who is making the decision on whether to hire the employee.

These actions should be followed when an employer reviews social media profiles whilst making other employment-related decisions as well, e.g. in relation to employee promotion,

change of position, or termination of employment. Most importantly, when dismissing an employee, the reason for the termination must not be related to any matter that is out of the scope of the employment, i.e. information collected from social media sites which is unrelated to the employee's employment. Otherwise, the termination may be deemed unlawful.

3. *What problems could an employer face as a result of employees using social media sites?*

Breach of confidentiality

Social media sites provide an open forum for individuals to post and exchange information. It is not uncommon for employees, or previous employees, to post information about their employer. If the information revealed harms the legitimate business interests of the employer, the employee may be liable for any damage suffered by the employer as a result of acting against the legitimate interests of the employer. Employees must not behave in such a way that violates the business interests of the employer. Following the termination of employment, this confidentiality obligation continues. If the information made available on a social media site amounts to a business secret, the employee may be liable to the employer for compensation for the damage it suffers as a result of disclosure. Further, the employee's behaviour may amount to a breach of the employment contract and serve as a basis for dismissal.

Damage to employer's or third party's reputation

Employees could post information on social media sites about the employer or another third party that causes damage to their reputation. If this is the case, the employer may be liable for the damage caused to the third party. The fact that the employer may have a claim against the employee concerned could be little comfort compared to the damage to the

reputation of the employer. Further, if a third party initiates a claim against the employer as a result of the employee's behaviour, in all likelihood, the employer will not be able claim the full amount of damages back from the employee.

Harassment/Unlawful discrimination

If an employee posts and/or exchanges negative information about his/her colleagues, regarding their age, sex, disability or other characteristics, for example, this could pose problems for the employer. If comments are made in the course of employment and 'in the name of' or 'on behalf of' the employer (e.g. it is made by an executive or senior employee, or HR manager), there is a risk that it will be interpreted as being made by the employer. The exchange of such information may constitute harassment or unlawful discrimination, and the employer might be liable for such action. Liability for posting and exchanging information of this nature about fellow employees is primarily borne by the individual who made the comment. However, liability of the employer cannot be excluded, especially if the communication was made as a part of, or in connection with, the employment relationship. Employers will be in a stronger position if they can prove that they took reasonable measures to prevent the employee from communicating in such a way.

Loss of productivity

Aside from the potential liability issues, using social media sites during working hours could have a negative effect on employees' productivity.

4. *What steps can be taken by an employer to minimize the risks associated with employees using social media sites?*

An employer can take the following steps:

- Create an internal policy setting out rules relating to the use of social media sites. This can be very helpful

and significantly reduce the risks associated with the employer's potential liability. It would be prudent that such a policy addresses that:

- the posting and exchange of information about the employer, other employees, the business partners of the employer or their employees on social media sites is prohibited. In particular, this includes any business information or confidential information about the employer and its business partners, and any negative, discriminatory or confidential information about the employees. It should be made clear that, in some circumstances, the employee can open themselves up to liability under law, regardless of whether such information was made within or outside of working hours;
    - using social media sites is not permitted during working hours, unless such usage is required for the performance of working duties;
    - that the employer is entitled to monitor the employee's social media site usage during working hours; and
    - a failure to comply with the requirements of the policy may result in disciplinary action, which could result in a warning or dismissal.

The terms of the policy should be accepted by each employee in writing.

- The employment contract should contain a confidentiality clause which sets out the employee's liability if they breach the policy or disclose information about the employer or its business partners to third parties, including, making such information publicly available on the social media sites. The employment contract should also specify that using social media sites during working hours is not permitted.

- Employees should be asked to consent to the employer being entitled to monitor their Internet usage in order to ensure that employees comply with confidentiality obligations, in accordance with the employment contract and internal policies.
- It is advisable that periodic training is provided to the employees on this subject.

Contributed by Ban, S Szabo & Partners

ICELAND

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Unlawful discrimination

Discrimination on the basis of certain protected characteristics, including a person's sex, religion, political opinion, nationality, social class or ethnic origin, race, skin colour, financial standing or family situation, among others, is prohibited under Icelandic law. CVs and cover letters will usually not contain information on most of the characteristics listed above. If employers use social media sites to search for information on these characteristics, and reject applicants on the basis of such information, they could be found guilty of unlawful discrimination.

In the private sector, there is generally no obligation to state the reasons why an employer has decided not to recruit a particular individual. However, if an applicant discovers that his application was rejected on discriminatory grounds, the employer could be liable for damages. In the public sector, the principle that the most qualified candidate must be recruited, limits an employer's discretion to select from applicants. Their assessment of a candidate's qualifications has to be based on relevant and objective criteria. If applicants for jobs in the public sector are assessed on the basis of the abovementioned characteristics, or on the basis of other information gleaned from social media sites that is unrelated to an applicant's skills and competency, the employer could be liable for damages.

Potential implications under data protection law

Applicants are protected from interference with their privacy under Icelandic law. Collecting information on job applicants from social media sites (e.g. by copying and storing certain data) could amount to processing of personal data within the meaning of the applicable data protection legislation. "Personal data" is defined in the Data Protection Act as any

data relating to the data subject, i.e. information that can be traced to a specific individual. The term "processing" is defined as any operation (or set of operations) which is performed on the personal data, whether manual or automatic.

Processing personal data is only permissible if at least one of the limited conditions set out in the legislation is met, e.g. the individual has expressly consented to the processing of the data, or the employer has a legitimate interest that they are seeking to protect. Stringent requirements are also in place for the processing of sensitive personal data (e.g. information relating to ethnic origin, skin colour, race, political opinion and religious beliefs).

The processing of personal data must also conform to other principles set out in the Data Protection Act. These include ensuring that the data is processed in a fair manner, the data itself is relevant to the specific purpose it has been obtained for, and that it is not processed further for any other purpose. The employer has a duty to provide guidance and warning to the individual concerned, and implement appropriate technical and organisational measures to protect the personal data against unlawful destruction, accidental loss, alteration and unauthorised access.

In order for employers to process personal data on job applicants, they must comply with the above mentioned conditions and data protection principles. Consent of the applicant is therefore likely to be needed.

The Data Protection Authority monitors compliance with the rules on data protection, and any infringements could be punishable by means of fines or a prison term.

2. What steps can be taken by employers to minimise such risks?

Employers should only recruit on the basis of legitimate and relevant information that relates to a candidate's skills and competencies. Any irrelevant material gleaned from social media sites should be ignored. A social media policy or other written guidelines should back this up, so that the employer can demonstrate an intention to extract only relevant information.

Employers should obtain the applicant's consent before using information from social media sites during the recruitment process. An employer may be able to argue that the processing of such information is necessary to be able to safeguard its legitimate interests, therefore making it permissible under the legislation. However, the safest option would be to obtain the applicant's consent to the processing.

One way to obtain consent is to state on application forms that, by submitting the application, the applicant is granting the employer the right to obtain and process information from specific media sites. The applicant could be asked to tick a box to indicate their consent to the employer processing the information in question. It is important that applicants are informed of the kind of data that will be processed, the purpose of the processing, how the processing will be conducted, how data protection will be ensured, and that the applicant can withdraw their consent if they wish. If the processing of sensitive data only extends to information that the data applicants themselves have made available, the employers can process it.

When personal data is processed, there is a general duty on employers to ensure that the data is correct. Employers should therefore give applicants the opportunity to clarify or rectify any data that is incorrect. There are also additional duties on employers who process data, e.g. not to keep the information for too long.

3. *What problems could an employer face as a result of employees using social media sites?*

Breach of confidentiality

Under legislation, collective bargaining agreements and/or employment contracts, employees have a duty of confidentiality to their employer. If confidential information was released on a social media site by an employee through carelessness or directly through the fault of the employee, this could be potentially damaging to the employer's or a third party's business or reputation.

Harassment/unlawful discrimination

Employees could potentially bully and harass fellow employees using social media sites. If this were to occur, it is possible that the employer could be liable for damages.

Loss of productivity

Aside from the potential liability issues described above, using social media sites during working hours could also have a negative effect on employees' productivity.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

Employers should remind their employees of their duty of confidentiality and instruct them not to post confidential information, or any other information, on social media sites that might cause damage to the employer's business or to a third party. If the employer clearly instructs his employees not to behave in a certain way and they do so anyway, the employer is less likely to be liable for damages if an employee posts harmful information on a social media site.

The employer can also set rules regarding employee's Internet usage and monitor Internet usage in order to determine whether employees are using social media sites improperly

or excessively, reducing their productivity. There are regulatory guidelines in place that employers must follow when monitoring the Internet usage of their employees. The employers have a duty to inform their employees that they are proposing to monitor their Internet usage. New employees must be informed about existing monitoring policies when they are hired. Employers should issue written and easily understandable rules on the parameters of employees' Internet usage and the employer's ability to monitor this.

The employer also has a duty to take measures, including pre-emptive measures, against bullying and harassment, including sexual harassment. Employers should therefore make their employees aware of the dangers of bullying and harassment on social media sites and that they should be mindful of that when they are interacting using such sites. An employer would be able to defend any subsequent claim for discrimination or harassment if it can show that it took all reasonable steps to prevent the employee from committing the discriminatory act in question.

Employers could ban access to social media sites at work altogether. It is possible that would prove unpopular with employees, but the option is open for employers if they deem it to be the right course of action. It would be impossible in many workplaces to ban internet usage outright.

Contributed by LOGOS Legal Services

ICELAND

IRELAND

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Unlawful discrimination

Social media sites will often contain personal profiles of the individual concerned including certain characteristics, which form the basis of protection against discrimination under the Employment Equality Acts 1998 - 2008. These characteristics could be age, disability, sex (including pregnancy and maternity), race (including nationality), religion, sexual orientation, family status, and marital and civil partnership status. Many of these characteristics would not typically feature in a CV. Therefore, if an employer has access to this information via a social media site and uses such information as the basis for refusing to recruit that person, then the employer's actions could constitute unlawful direct discrimination. The employer could face an increased risk of a claim for discrimination against it if the job applicant were to discover that their application was rejected because of one or more of the above characteristics.

Potential implications under the Data Protection Acts 1988 - 2003

Vetting job applicants using information contained on social media sites could also have implications for employers in respect of its obligations under the Data Protection Acts 1988 - 2003 (DPA). The DPA regulates the collection and use of 'personal data'. Personal data means information (including expressions of opinion) that relates to a living individual who can be identified from that information. 'Sensitive' personal data includes information relating to a person's sexuality, race and religion. Under the DPA, employers have onerous obligations when 'processing' sensitive personal data. The concept of 'processing' includes obtaining, recording, holding or using personal data. Therefore, when an employer collects information about an applicant from a social media site, it may be processing sensitive information. In such

circumstances, the DPA requires employers to comply with general data protection principles and, in the context of the use of social media, this may raise questions as to whether or not the information is accurate and it is proportionate to use it in this way. In particular, sensitive data can usually only be processed if the applicant has given explicit consent, the information contained in the sensitive data has been made public as a result of steps taken by the applicant or if one of a limited number of other legitimate aims has been satisfied. The failure to comply with these data protection principles could result in complaints against the employer or action being taken against it by the Data Protection Commissioner (the Irish authority that upholds information rights and data privacy for individuals).

2. *What steps can be taken by employers to minimise such risks?*

Assuming employers do not wish to take steps to ban all vetting of job applicants using information from social media there are a number of steps which can be taken to guard against unnecessary risk:

- Those scanning social media sites as part of the recruitment process should be instructed to extract only legitimate and relevant information for the job application process.
- A social media policy or other written guidelines should back this up, so that the employer can demonstrate an intention to extract only relevant information.
- Ideally, the person scanning the social media sites should not be the same as the person who is determining the job application process or interviewing the individual. This way, the irrelevant material (which might contain sensitive personal data) will not make its way through to the decision maker.
- Applicants should be told, at the start of any application

process that a vetting or verification exercise using social media sites forms part of the process.

- Job applicants who are rejected because of information gleaned from social networking should be given an opportunity to correct that information before any final decisions are taken.

3. *What problems could an employer face as a result of employees using social media sites?*

Breach of confidentiality

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social media platforms, it is not uncommon for employees to end up posting confidential information about the employer and/other employees. This could result in significant damage to the employer's business and reputation.

Damage to employer's or third party's reputation

Employees could post information on a social media site that causes damage to the reputation of the employer and/or a third party. An employer may be vicariously liable for the defamatory conduct of an employee. The fact that an employer may have a claim against the employee concerned could be little comfort compared to the damage to the reputation of the employer.

Bullying & Harassment/Unlawful discrimination

It is not uncommon for employees to post negative comments about fellow employees on social media sites. The comments could be offensive, degrading and humiliating to such fellow employees. Alternatively such comments might relate to a protected characteristic such as age, disability, race or sex. If an employee were to make such comments 'in the course of their employment', there is a danger that such

comments could constitute bullying or alternatively could constitute harassment under the Employment Equality Acts 1998 - 2008. In such circumstances, an employer could be vicariously liable for the actions of that employee.

An employer could also risk facing other discrimination claims if employees use information they have obtained from social media sites about other employees as the basis for treating them in a detrimental way.

An employer will have a defence to any claim for bullying, discrimination or harassment if it can show that it took all reasonable steps to prevent the employee from committing the act in question.

Loss of productivity

In addition to the legal issues set out above, employers could experience a loss of productivity in the workforce if employees are allowed to access social media sites during working hours.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

An employer can take the following steps:

- Impose an outright ban on access to social media sites at work. This approach could prove to be unpopular amongst employees and have an adverse impact on the morale within a workforce. Ultimately, the employer would need to weigh up the potential advantages and disadvantages in deciding whether to permit employees to access social media sites at work. A complete ban would not address the potential problems that could arise from postings by employees outside of working hours. Employers can easily find themselves liable for comments made after hours by employees, particularly where there is an obvious and clear link to

the employment. Accordingly, comments posted by one employee about another employee after hours on a social networking site could still end up as the responsibility of the employer.

- Put in place a social media policy which deals with the use of social media sites during and outside of work hours. Such a policy should have provisions dealing with social media activity, but in particular:
    - set out the parameters governing the use of the employer's IT systems;
    - remind employees that social media activity may not necessarily be private;
    - prohibit discrimination, harassment or bullying of other employees, which could include negative comments about employees posted on social media sites;
    - prohibit negative comments about the employer, its employees or third parties; and
    - prohibit the disclosure of any confidential information that relates to the employer and/or other employees.

  The policy should set out the consequences of a breach of the policy, which could include disciplinary action and, ultimately, dismissal.
- Provide awareness training to employees on conduct that could constitute discrimination, harassment and bullying. An employer would be able to defend any subsequent claim for discrimination or harassment if it can show that it took all reasonable steps to prevent the employee from committing the discriminatory act in question.

- Monitoring the use of social media sites at work could help to determine whether there is a loss of productivity as a result of employees accessing such sites. However, it is important to bear in mind that electronic forms of workplace surveillance would involve activity regulated under the DPA. Legal advice should be sought before engaging in any such monitoring.
- Incorporate within employment contracts an appropriate confidentiality clause, which would afford protection to the employer in the event that an employee posts confidential information on a social media site.
- Disciplinary action may be taken against employees who misuse a social media site to the detriment of the employer. In some cases, an employer could consider dismissal. Each case will turn on its facts and an employer might want to obtain legal advice before proceeding to dismiss the employee in question.

Contributed by A&L Goodbody

ISRAEL

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Unlawful discrimination

Social media sites will often contain personal profiles of the individual concerned including certain characteristics such as age, disability, sex (including pregnancy and maternity), race (including nationality), religion or belief, sexual orientation, marriage and political opinion. It is unlikely that most, if any, of these characteristics will feature in a CV. Therefore, if an employer has access to this information via a social media site and uses such information as the basis for refusing to recruit that person, then the employer's actions could constitute unlawful discrimination under the Equal Opportunity in the Workplace Law 1988.

Potential implications under the Israeli Privacy Protection Law 1981 ("PPL")

The PPL imposes certain limitations on employers collecting and using "information" contained on social media sites for the purposes of its recruitment process:

- The PPL defines "*information*" as "*data on the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of a person*". The PPL only permits such information to be collected and used subject to the data subject's consent, and for the purpose for which such consent was provided. Information contained in social media websites may not have been provided for the purposes of supporting job applications.
- Israeli case law has determined that the processing of information must be based on reasonableness, good faith and proportionality. The requirement for proportionality is a constitutional requirement. Therefore, any use of information collected via social media sites should be

done only to the extent that it is directly and specifically required to assist with the recruitment and selection process, and assessing whether the applicant fulfills the job criteria. The PPL also provides applicants with a right to inspect, correct and/or delete any information about them contained within an employer's database.

- Employers are required to register any database they manage or possess with the Israeli Database Registrar (ILITA) if:
    - the database contains "sensitive information". "Sensitive information" is information about a person's personality, intimate affairs, state of health, economic position, opinions and beliefs;
    - the database contains information about the applicant that was not provided by him/her or was provided on their behalf without their consent; or
    - the database contains information on more than 10,000 individuals.

  The above is not an exhaustive list and the employer's database should also comply with certain other requirements in relation to accuracy, security and confidentiality. An employer's failure to comply with the registration requirements set out in the PPL could result in civil and criminal liability.

2. What steps can be taken by employers to minimise such risks?

- Employers should carefully read the privacy policies of the websites from which any information is extracted to verify the purpose behind the information that has been provided. Ideally, applicants should be informed of the vetting or verification exercise that proposes to use social media sites and be given the opportunity to provide their consent.

- Ideally, the person scanning the social media sites should not be the same as the person who is determining the job application process or interviewing the individual. This way, the irrelevant material (which might contain sensitive personal data) will not make its way through to the decision maker, and employers would use only that amount of information specifically and legitimately required for the recruitment process.
- A social media policy or other written guidelines should back this up, so that the employer can demonstrate an intention to extract only relevant information.
- Employers should comply with the PPL registration requirements and, if required, register any database containing social media generated information with ILITA. Employers should also ensure that they comply with the accuracy, security, confidentiality, inspection and rectification requirements under the PPL.

3. *What problems could an employer face as a result of employees using social media sites?*

Breach of confidentiality and the PPL

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social media platforms, it is not uncommon for employees to end up posting confidential information about the employer and/or other employees. In addition to the risks associated with the disclosure of confidential information, an employer could face liability if employees post information that is in breach of the PPL.

Damage to employer's or third party's reputation/business

Employees could post information on a social media site that causes damage to the reputation of the employer and/or a third party. An employer may be vicariously liable for

the defamatory conduct of an employee. The fact that an employer may have a claim against the employee concerned could be of little comfort compared to the damage to the reputation of the employer.

An employee could make binding representations on behalf of the employer when conducting business using social media sites and therefore expose the employer to further business related liabilities.

Harassment

An employee could make comments about other fellow employees that constitute harassment. In such circumstances, an employer could be held liable for the actions of that employee.

Loss of productivity

Finally, there could be a negative effect on productivity if employees use social media sites while at work.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

An employer may take the following steps:

- Prohibit access to social media sites at work or during working hours.
- Adopt a social media policy which sets out the parameters governing the use of social media sites. Such a policy should contain restrictions on the disclosure of information and know-how, the use of employer or third party information and use of intellectual property rights.
- In exceptional circumstances, it can engage in limited monitoring of the use of social media sites at work. Any monitoring should comply with certain requirements, which have been developed under Israeli case law. In summary:

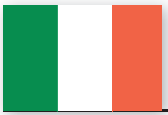
- informed consent will need to be obtained from the affected employees. Such informed consent should be based on the employer's full disclosure of the means by which it intends to monitor the employees' use of social media sites at work;
- monitoring should be undertaken in exceptional cases where severe damage could be caused to the employer;
- the monitoring itself should be reasonable and proportionate taking into consideration the employee's right to privacy;
- monitoring and collection of information should be undertaken for the specific purpose for which the employee provided his or her informed consent; and
- the affected employees will need to be informed about the information collected, the technology that was used to conduct the monitoring, the nature of the communications monitored and the duration that any information collected will be retained.

Legal advice should be sought before engaging in any such monitoring.

- Incorporate within employment contracts restrictions on the use of employer related information, know how and intellectual property.
- Disciplinary action may be taken against employees who misuse a social media site to the detriment of the employer. In some cases, an employer could consider dismissal. Each case will turn on its facts and an employer might want to obtain legal advice before proceeding to dismiss the employee in question.

Contributed by Goldfarb, Levy, Eran, Meiri, Tzafrir & Co Law Offices

ISRAEL



ITALY

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Social media sites will often contain personal profiles of the individual concerned, including certain characteristics, which form the basis of protection against discrimination under anti-discrimination legislation in Italy. These characteristics could be age, disability, sex (including pregnancy and maternity), race (including nationality), religion or belief, sexual orientation, gender reassignment, and marriage and civil partnership status. It is unlikely that most, if any, of these characteristics will feature in a CV. Therefore, if an employer has access to this information via a social media site and uses such information as the basis for refusing to recruit that person, then the employer's actions could constitute unlawful direct discrimination. The employer could face an increased risk of a claim for discrimination against it if the job applicant were to discover that their application was rejected because of one or more of the above characteristics.

2. *What steps can be taken by employers to minimise such risks?*

Assuming employers do not wish to take steps to ban all vetting of job applicants using information from social media, there are a number of steps which can be taken to guard against unnecessary risk:

- Those scanning social media sites as part of the recruitment process should be instructed to extract information that is contained in parts of the site that have no restricted access and is relevant to the job.
- A social media policy or other written guidelines should back this up, so that the employer can demonstrate an intention to extract only relevant information.
- Ideally, the person scanning the social media sites should obtain the candidate's written consent to access their profile on the site. It would also be sensible for the

person scanning the social media sites to be different from the person who is determining the job application process or interviewing the individual. This way, the irrelevant material will not make its way through to the decision maker.

- Applicants should be told, at the start of any application process, that a vetting or verification exercise using social media sites forms part of the process.
- Job applicants who are rejected because of information gleaned from social networking should be given an opportunity to correct that information before any final decisions are taken.

3. *What problems could an employer face as a result of employees using social media sites?*

Breach of confidentiality

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social media platforms, it is not uncommon for employees to end up posting confidential information about the employer and/or other employees. This could result in significant damage to the employer's business and reputation.

Damage to employer's or third party's reputation

Employees could post information on a social media site that causes damage to the reputation of the employer and/or a third party. An employer may be jointly liable for the defamatory conduct of an employee, should the conduct be carried on at the workplace. The fact that an employer may have a claim against the employee concerned could be of little comfort compared to the damage to the reputation of the employer.

Harassment/Unlawful discrimination

It is not uncommon for employees to post negative comments about fellow employees on social media sites. The comments could relate to a protected characteristic such as age, disability, race or sex. If an employee were to make such comments 'in the course of their employment', there is a danger that such comments could constitute harassment. In such circumstances, an employer could be liable for the actions of that employee.

An employer could also risk facing other discrimination claims if employees use information they have obtained from social media sites about other employees as the basis for treating them in a detrimental way.

An employer will have a defence to any claim for discrimination or harassment if it can show that it took all reasonable steps to prevent the employee from committing the discriminatory act in question.

An employer could also face liability for failure to comply with the contractual obligation to protect an employee.

Loss of productivity

In addition to the potential legal issues set out above, there could clearly be an impact on productivity in the workforce, should employees be permitted to access social media sites while at work.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

An employer can take the following steps:

- Impose an outright ban on access to social media sites at work. This approach could prove to be unpopular amongst employees and have an adverse impact on the morale within a workforce. In addition, an outright ban

could be unlawful. Legal advice should be sought before deciding to impose an outright ban.

- Put in place a social media policy which deals with the use of social media sites during and outside of work hours. Such a policy should have provisions dealing with social media activity, but in particular:
    - set out the parameters governing the use of the employer's IT systems;
    - remind employees that social media activity may not necessarily be private;
    - prohibit discrimination, harassment or bullying of other employees, which could include negative comments about employees posted on social media sites;
    - prohibit negative comments about the employer, its employees or third parties; and
    - prohibit the disclosure of any confidential information that relates to the employer and/or other employees.

  The policy should set out the consequences of a breach of the policy, which could include disciplinary action and, ultimately, dismissal.
- Provide awareness training to employees on conduct that could constitute discrimination, harassment and bullying. An employer would be able to defend any subsequent claim for discrimination or harassment if it can show that it took all reasonable steps to prevent the employee from committing the discriminatory act in question.
- Monitoring the use of social media sites at work could help to determine whether there is a loss of productivity as a result of employees accessing such sites. However,

it is important to bear in mind that electronic forms of workplace surveillance would involve activity regulated under Italian law. Legal advice should be sought before engaging in any such monitoring.

- Incorporating within the employment contracts an appropriate confidentiality clause, which may afford protection to the employer in the event that an employee posts confidential information on a social media site.
- Disciplinary action may be taken against employees who misuse a social media site to the detriment of the employer. In some cases, an employer could consider dismissal. Each case will turn on its facts and an employer might want to obtain legal advice before proceeding to dismiss the employee in question.

Contributed by Quorum Legal Network

ITALY

MOZAMBIQUE

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Employers are free to use information which is publicly available on social media websites when selecting job applicants. Social media sites could be used by employers to ascertain more information about an applicant if the information provided on their CV or that revealed during their interview is not sufficient for the employer to make a decision.

Unlawful discrimination

Social media sites will often contain personal profiles of the individual concerned including certain characteristics, which are protected from discrimination. These characteristics could be age, disability, sex (including pregnancy and maternity), race (including nationality), religion or belief and sexual orientation. It is unlikely that most, if any, of these characteristics will feature in a CV.

There are no restrictions on employers in this regard provided that the information obtained from social media is not used in such a way as to discriminate against an applicant. It would however be very difficult for a job applicant to show that they have been discriminated against by a prospective employer using information which they obtained via social media sites.

Potential data protection implications

Employers are free to use social network information to the extent that the information which is extracted relates to the employment. If there is information on a social media site that is useful for an employer to set the profile of a job applicant, there should be no problem in using such information in the hiring process.

2. *What steps can be taken by employers to minimise such risks?*

It is important that any information that an employer sources through social media websites is publicly available to whoever accesses the site. Employers should instruct those scanning social media sites as part of the recruitment process to extract only relevant information for the job application process. That information must be readily accessible to all and not be of a restricted nature.

A social media policy or other written guidelines should be produced by the employer which states that only relevant information to the application process is accessed. This will be important for an employer so that they can demonstrate that they have legitimate reasons for using that information.

Applicants should be advised at the start of the recruitment process that social media sites are used to collect information. The employer should ask the applicant to confirm the content of any information that the employer deemed relevant to the selection process which was taken from a social media source.

3. *What problems could an employer face as a result of employees using social media sites?*

Breach of confidentiality

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social media platforms, it is not uncommon for employees to post confidential information about the employer and/or other employees. This could result in significant damage to the employer's business and reputation.

Damage to employer's or third party's reputation

Employees could post information on a social media site that causes damage to the reputation of the employer and/or a third party. An employer may be vicariously liable for the defamatory conduct of an employee. The fact that an

employer may have a claim against the employee concerned would be of little comfort compared to the damage to the employer's reputation.

Harassment/Unlawful discrimination

It is not uncommon for employees to post negative comments about fellow employees on social media sites. The comments could relate to a characteristic such as age, disability, race or sex which are protected under discrimination laws. If an employee were to make such comments 'in the course of their employment', there is a danger that such comments could constitute discrimination/defamation. It would be difficult to establish liability against the employer for the employee's actions but such conduct could ultimately have a detrimental affect on the working environment and the productivity of the work force.

Although it would be difficult to consider the employer liable for any defamation or discriminatory act carried out by an employee using a social networking site, it would be helpful to employers if they could show that they took all reasonable steps to prevent the employee from committing the discriminatory/defamatory act in question.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

An employer can take the following steps:

- Impose an outright ban on employee access to social media sites at work. This approach could prove to be unpopular among employees and have an adverse impact on workforce morale. Ultimately, the employer would need to weigh up the potential advantages and disadvantages in deciding whether to allow employees to access social media sites at work. A complete ban would not address the problems that could arise from postings made by employees outside of working hours.

- Put in place a social media policy which deals with the use of social media sites during and outside of work hours. Such a policy should have provisions dealing with social media activity, but in particular:
    - set out the parameters governing the use of the employer's IT systems;
    - remind employees that social media activity may not necessarily be private;
    - prohibit discrimination, harassment or bullying of other employees, which could include negative comments about employees posted on social media sites;
    - prohibit negative comments about the employer, its employees or third parties; and
    - prohibit the disclosure of any confidential information that relates to the employer and/or other employees.

  The policy should set out the consequences of a breach of the policy, which could include disciplinary action and, ultimately, dismissal.
- Provide awareness training to all employees on conduct that could constitute discrimination, harassment and bullying. An employer would be able to defend any subsequent claim for discrimination or harassment if it can show that it took all reasonable steps to prevent the employee from committing the discriminatory act in question.
- Monitoring the use of social media sites at work could help to determine whether there is a loss of productivity as a result of employees accessing such sites. The employee must, however, be given notice that their internet use is being monitored. The data retrieved from

monitoring should not be used without the consent of the employee save for very specific situations such as a criminal investigation or for national security purposes. Legal advice should be sought before engaging in any such monitoring.

- Incorporate an appropriate confidentiality clause in employment contracts, which protects the employer in the event that an employee posts confidential information on a social media site.
- Disciplinary action may be taken against employees who misuse a social media site to the detriment of the employer. In some cases, an employer could consider dismissal. Each case will turn on its facts and an employer might want to obtain legal advice before proceeding to dismiss the employee in question.

MOZAMBIQUE

NETHERLANDS

1. *Are there any risks for employers who use social media sites to vet job applicants?*

In the Netherlands, as in other countries, it is not uncommon for individuals to submit information about their personal life on social media sites. When using social media to vet job applicants, employers should be aware that they face several legal risks under Dutch law.

Possible implications under the Dutch Data Protection Act

When an internet search is carried out, 'personal data' could be processed. Personal data may include the address of job applicants, their date of birth, employment history, photos, videos and information about their friends and family. Processing of personal data as part of an internet search may include acts such as the collection, storage, consultation or making available of personal data. In most instances, the employer will be considered to be the 'data controller', i.e. the legal person that determines the purpose and means of processing that data. An employer can legitimately process personal data if it can justify doing so. An employer will be able to justify the processing of personal data if it can show that the processing is a proportionate means of meeting a legitimate interest or that the job applicant gave his unequivocal consent to the processing of data from social media sites.

In addition, when processing personal data, the employer should comply with the following obligations of the Dutch Data Protection Act ("DDPA"):

- Where the employer uses an external recruitment agency to carry out an internet search on a job applicant, the recruitment agency will be considered to be the 'data processor'. In such circumstances, the DDPA requires that appropriate security measures in relation to the processing of the data should be set out in a written data

processing agreement between the employer and data processor.

- The employer may also have to notify the Dutch Data Protection Authority of the processing of data, unless such processing is exempt under the DDPA. There is a specific exemption for the processing of personal data of job applicants. Unless all of the conditions of this exemption are met, then the Authority will need to be notified with regard to the data processing within the context of an internet search on job applicants. Under this exemption, the processing of the name, contact details, nationality, education, and former and present employment of job applicants is allowed. This exemption also includes the processing of other personal data that may be relevant to the job, if such data has been provided either by the job applicant himself, or where the job applicant is familiar with this personal data (for example, the job applicant is familiar with the fact that he has a driver's license).

  In order to rely upon the above exemption, the employer should retain the personal data for no longer than four weeks after the application procedure has ended, unless the job applicant consents, in which case the retention period can be up to one year. If the employer does not process personal data other than the personal data mentioned above and if it complies with the retention period of four weeks (or one year with the consent of the job applicant), the employer is allowed to use social media sites to vet applicants without notifying the processing of the data to the Dutch Data Protection Authority.

In most instances, the employer may probably not be able to rely upon the above exemption. It will be common practice for an employer to combine personal data from different social

media sites. In such circumstances, it may become apparent that the job applicant had not posted the information on the internet nor was he aware that information about him had been posted.

If the employer cannot rely upon the above exemption, it will need to notify the Dutch Data Protection Authority. The notification needs to be drawn up in the Dutch language. It must include the name and address of the employer, the reasons for the processing of the data, the type of data that will be processed, the recipients of the data and whether the data will be transferred to countries outside the EU. Also, a general description of the security measures that are in place to protect the personal data should be provided. Submitting a notification to the Dutch Data Protection Authority is free of charge.

If the employer does not fulfill its duty to notify the Dutch Data Protection Authority, an administrative penalty with a maximum of EUR 4,500 can be imposed. In the event of a breach of another obligation under the DDPA, the Dutch Data Protection Authority may impose a period penalty payment.

Unlawful discrimination

If an employer rejects a job applicant based upon information available on social media sites, this may also lead to a breach of the Dutch Equal Treatment Act or other anti-discrimination legislation that is currently in place. A breach of the Dutch Equal Treatment Act would occur if the rejection of the applicant is due to certain protected characteristics, which are religion or belief, political opinion, race, gender (including pregnancy and maternity), nationality, sexual orientation and civil status. A job applicant could lodge a complaint at the Equal Treatment Commission if he finds out that his application has been rejected because of one or more of the above characteristics. However, the judgment of the

Commission is not legally binding. However, the judgment could provide the job applicant with grounds to file a civil claim against the employer. In practice, it may, however, be difficult to prove that the rejection of the application was an act of unlawful discrimination.

2. *What steps can be taken by employers to minimize such risks?*

A number of steps can be taken to guard against unnecessary risks:

- Those scanning social media sites as part of the recruitment process should be instructed to extract only legitimate and relevant information for the job application process.
- The safest course of action to take before processing the personal data of job applicants is to obtain the prior consent of the job applicant. It would be sensible to give the job applicant the option to consent to using social media sites as part of the application process.
- Assess carefully whether the use of social media sites is a proportionate means of meeting a legitimate aim and would prevail over the privacy interests of the applicant. In this respect, it would be sensible to consider whether information gathered via a social media site is actually necessary.
- Applicants should be told, at the start of any application process, that a vetting or verification exercise using social media sites forms part of the process. A social media policy or code of conduct could back this up, so that it can demonstrate an intention to extract only relevant information.
- Try to ascertain whether the information obtained is accurate and reliable.

- Job applicants who may be rejected because of information gleaned from social networking sites should be given an opportunity to correct that information before any final decisions are taken.

3. *What problems could an employer face as a result of employees using social media sites?*

Breach of confidentiality

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social media platforms, it is not uncommon for employees to end up posting confidential information about the employer and/or other employees. This could result in significant damage to the employer's business and reputation.

Damage to employer's or third party's reputation

Employees could post information on a social media site that causes damage to the reputation of the employer and/or a third party. An employer may be vicariously liable for the defamatory conduct of an employee. The fact that an employer may have a claim against the employee concerned could be of little comfort compared to the damage to the reputation of the employer.

Breach of the Dutch Data Protection Act

An employer could be liable if an employee posts personal data relating to another individual on a social media site that is in breach of the DDPA.

Harassment/Unlawful discrimination

Employees may post negative comments about fellow employees and other people on social media sites. The comments could relate to a protected characteristic such as age, disability, race or sex. If an employee were to make

such comments in the course of their employment, there is a danger that such comments could constitute unlawful discrimination under the Dutch Equal Treatment Act or even the Dutch Criminal Code. Under certain circumstances, an employer could be vicariously liable for the actions of that employee.

An employer could also risk facing other discrimination claims if employees use information they have obtained from social media sites about other employees as the basis for treating them in a detrimental way.

An employer will have a defence to any claim for discrimination if it can show that it took all reasonable steps to prevent the employee from committing the discriminatory act in question.

Infringement of intellectual property rights

An employee could, for example, upload a photo that is protected by copyright on the employer's social media site without the consent of the copyright owner. In such circumstances, the employer could be liable for violation of the copyright attached to the photo. Similar problems could also apply in relation to an employee's infringement of other intellectual property rights, such as trademarks.

Loss of productivity

Aside from the issues set out above, being permitted to use social media sites during working hours could have a negative effect on employees' productivity.

4. *What steps can be taken by an employer to minimize the risks associated with employees using social media sites?*

An employer can take the following steps:

- Impose an outright ban on access to social media sites at work. This approach could prove to be unpopular

amongst employees and have an adverse impact on the morale within a workforce. Ultimately, the employer would need to weigh up the potential advantages and disadvantages in deciding whether to permit employees to access social media sites at work. A complete ban would not address the potential problems that could arise from postings by employees outside of working hours. Employers can easily find themselves liable for comments made after hours by employees, particularly where there is an obvious and clear link to the employment. Accordingly, comments posted by one employee about another employee after hours on a social networking site could still end up as the responsibility of the employer.

- Provide awareness training to employees on the risks arising from the use of social media and the conduct that could constitute discrimination.
- Put in place a social media policy which deals with the use of social media sites during and outside of work hours. Such a policy should set out the parameters governing the use of social media sites. The policy should set out the consequences of a breach of the policy, which could include disciplinary action and, ultimately, dismissal. If there is a Works Council, the consent of the Works Council should be obtained before the introduction of such a policy.
- Monitoring the use of social media sites at work could help to determine whether there is a loss of productivity as a result of employees accessing such sites. However, any such monitoring should comply with the DDPA.
- A confidentiality clause may be incorporated in the employment agreement, specifically aimed at protecting against the risks of misusing social media sites.

- Disciplinary action may be taken against employees who abuse a social media site to the detriment of the employer.

Contributed by Van Doorne N.V.

NORWAY

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Unlawful discrimination

Social media sites will often contain information regarding an individual's personal characteristics, such as age, disability, sex (including pregnancy and maternity), race (including nationality), religion or belief, sexual orientation, gender reassignment, and marriage and civil partnership status. Such information is unlikely to be included in an applicant's CV and employers could face claims for unlawful discrimination if they use it as the basis for refusing to recruit a particular candidate.

Potential implications under the Personal Data Act 2000

Vetting job applicants using information contained on social media sites could also have implications for employers in respect of its obligations under the Personal Data Act 2000 (PDA). The PDA applies to the processing of 'personal data'. Personal data means information that relates to a living individual who can be identified from that information. 'Sensitive' personal data includes information relating to a person's sexuality, race and religion. Under the PDA, employers have onerous obligations when collecting and using sensitive personal data. In particular, they must ensure that they have a sound legal basis for the collection and use of such data, and that they provide information to employees on the uses to which the data will be put.

The DPA requires employers to comply with general data protection principles and, in the context of the use of social media to obtain information on employees and/or prospective employees, this may raise questions as to whether or not the employer has a sound legal basis on which to process the information, whether the information is accurate and if it is proportionate to use it in this way.

NORWAY

The failure to comply with the data protection principles could potentially result in claims for compensation against the employer or action being taken against it by the Data Inspectorate (the Norwegian authority that upholds information rights and data privacy for individuals).

2. *What steps can be taken by employers to minimise such risks?*

On the assumption that employers do not wish to take steps to ban all vetting of job applicants using information from social media, there are a number of steps which can be taken to guard against unnecessary risk:

- Those scanning social media sites as part of the recruitment process should be instructed to extract only information that is relevant to the job application process.
- A social media policy or other written guidelines should be implemented.
- Applicants should be informed at the start of the application process that a vetting or verification exercise using social media sites forms part of the process.
- Applicants who are rejected because of information gleaned from social networking sites should be given an opportunity to review and, if necessary, correct that information before any final decisions are taken.

3. *What problems could an employer face as a result of employees using social media sites?*

Breach of confidentiality

Employees might post confidential information about the employer and/or other employees. This could result in significant damage to the employer's business and reputation and also represent a breach of the employee's duty of confidentiality to his employer.

Damage to employer's or third party's reputation

Employees could post information on a social media site that causes damage to the reputation of the employer and/or a third party. An employer may be vicariously liable for the defamatory conduct of an employee, where the employee has intended to defame, or was grossly negligent, and where the employee has acted in the course of their employment. The fact that an employer may have a claim against the employee concerned could be of little comfort compared to the damage to the reputation of the employer.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

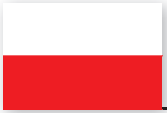
An employer can take the following steps to minimise the risks associated with employees using social media sites:

- Impose restrictions on access to social media sites at work.
- Put in place a social media policy which deals with the use of social media sites during and outside of work hours. Such a policy should have provisions dealing with social media activity, but in particular:
    - set out the parameters governing the use of the employer's IT systems;
    - remind employees that social media activity may not necessarily be private;
    - prohibit discrimination, harassment or bullying of other employees, which could include negative comments about employees posted on social media sites;
    - prohibit negative comments about the employer, its employees or third parties; and

    - prohibit the disclosure of any confidential information that relates to the employer and/or other employees.

- Monitoring the use of social media sites at work could help to determine whether there is a loss of productivity as a result of employees accessing such sites. However, it is important to bear in mind that electronic forms of workplace surveillance would involve activity regulated under the DPA and the Personal Data Regulations. Legal advice should be sought before engaging in any such monitoring.
- Incorporate within employment contracts an appropriate confidentiality clause, which would afford protection to the employer in the event that an employee posts confidential information on a social media site.
- Disciplinary action may be taken against employees who misuse a social media site to the detriment of the employer. In some cases, an employer could consider dismissal. Each case will turn on its facts and an employer might want to obtain legal advice before proceeding to dismiss the employee in question.

Contributed by Advokatfirmaet Thommessen AS



POLAND

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Privacy issues

Social media sites often contain information about individuals that is classified as sensitive data under Polish law. This includes information relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, religious, party or trade-union membership, data concerning an individual's health, genetic code, addictions or sex life, and data relating to any criminal or civil proceedings against the individual, including the outcome of those proceedings.

Employers who use information from social media sites to vet candidates as part of their recruitment processes should therefore ensure, when doing so, that they comply with their obligations concerning the processing of sensitive data. The processing of sensitive data is permitted, provided the person concerned has made that data public, which is often the case on social media sites.

However, employers should also be aware that using social media sites to vet job applicants could be found to be interfering with the applicants' personal freedom, particularly if the information obtained is not relevant to the applicant's suitability for the role for which they are being recruited.

Discrimination

Individual profiles on social media sites may contain details of personal characteristics that are not usually included in CVs, in particular, the candidate's racial or ethnic origin, nationality, political, religious or philosophical beliefs, religion or sexual orientation. Any decision by an employer not to employ a particular job applicant based on any of the above characteristics would be a violation of the principle of equal treatment, and would therefore constitute unlawful discrimination. Employers are under an obligation to prove

that any decision not to hire a particular candidate was based on objective criteria, if challenged.

2. *What steps can be taken by employers to minimise such risks?*

The above risks may be mitigated by taking the following steps:

- Candidates should be notified at the start of the application process that information from social media sites will be used as part of that process. Ideally, employers should obtain the consent of the candidates to do this.
- It should be made clear to applicants that only information that is relevant to the recruitment process will be obtained, for example, social media sites will only be used to verify the information contained in the applicant's CV.
- A policy on the rules and procedures to be followed when scanning social media sites should be introduced and those in charge of obtaining information from such sites on behalf of the employer should be instructed to extract only information which is relevant to the recruitment process.

3. *What problems could an employer face as a result of employees using social media sites?*

Employees can spend too much of their working time visiting social media sites, which may eventually lead to lower work efficiency.

In certain businesses, the employee's image is important. Employers may therefore face problems if their employees' profiles on social media sites contain information or pictures which have a negative impact on the business image of a given employee and, consequently, of the employer.

In addition, employees who make negative postings may find themselves facing civil or criminal liability under laws relating to defamation and/or harassment. In cases where postings could be classified as being part of the employees' performance of their employment obligations (which is unlikely), the employer could be found civilly liable for damages caused to a third party.

4. What steps can be taken by an employer to minimise the risks associated with employees' using social media sites?

Employers may consider prohibiting their employees from using social media sites during working hours. This is likely to be found to be justifiable, since employees should be fully devoted to the performance of their employment obligations during their working hours.

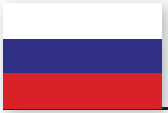
If employers do not intend to entirely prohibit the use of social media sites during working hours, the basic steps they could take to mitigate the risks related to the use of social media sites by employees would be as follows:

- It is recommended that employers introduce a policy on the use of social media by employees. Any such policy should draw a clear distinction between the use of social media during working hours and its use outside working hours, as attempts to control the latter will affect the personal freedom of the employee. However, there are grounds for employers to argue that they are able to prohibit employees from using social media outside of working hours in such a way as to cause damage to the employer's business.
- Employees should be reminded of their duty of confidentiality to their employer.
- The employer may consider the possibility of monitoring the use of social media sites by its employees. However, such monitoring may only be found to be lawful if: (i) it

is justified by any relevant law; (ii) it is carried out in a way that is proportionate and adequate in relation to the purpose of the monitoring, and (iii) employees have been notified in advance that monitoring may be carried out by the employer, the type of data that will be gathered by the employer and about the purposes of the monitoring. Ideally, employees should also be asked to consent, in writing, to such monitoring being carried out.

- The use of social media by an employee in breach of any applicable provisions of Polish Law or in breach of the employer's policy may be grounds for termination of employment. This should, however, be assessed on a case-by-case basis and legal advice may need to be sought before a decision to dismiss is made.

Contributed by Soltysinski Kawecki & Szlezak



RUSSIA

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Unlawful discrimination

Social media sites can contain personal profiles with details of an individual's personal characteristics, most of which are unlikely to feature in a CV or on a personnel file. An employer may therefore consider using such sites as a valuable source of information when deciding whether to recruit, promote or dismiss an employee and when making assessments on an employee's performance.

However, employers should bear in mind that the RF Labor Code prohibits any discrimination during recruitment and employment based on an individual's: sex; race; skin colour; nationality; language; ethnic origin; class; financial situation; family situation (i.e. marital status and/ or whether or not an individual has children), position within the company; age; place of domicile; religious or political opinions; membership of NGOs or political parties; and any other characteristics not directly related to the employee's job or assignment. Different or preferential treatment may be justified only where it can be shown that this was due to a requirement inherent to the job or assignment. This rule applies equally to any form of discrimination; discrimination based on race or sex is not viewed more strictly than the application of any other discriminatory criteria not related to the employee's professional qualities. There are, however, certain statutory provisions that allow for positive discrimination in order to protect certain categories of employees (pregnant women, for example).

Upon request, the employer must provide unsuccessful job applicants with written reasons for their rejection, and the applicant may challenge the employer's decision in court. Individuals who are able to prove that they have been discriminated against can demand that their rights be

restored. This could mean, for example, could demand that a rejected job applicant could demand that they be employed by the Company or an employee that their salary be paid at the level at which it would have been paid without discrimination. In addition, the individual may claim compensation or damages, including for non-pecuniary damage where the discrimination caused physical or mental suffering.

Data Protection

The RF Labor Code restricts the use of personal data held on employees and prospective employees. In particular, the Code permits the employer to process personal data only as necessary to comply with any relevant laws, to assist the employee with his job search, training or promotion, to ensure employees' personal safety, to control the quantity and quality of the employee's work and to ensure the safety of the employer's property. Browsing social media sites in order to vet job applicants or employees will constitute the processing of personal data and must therefore fulfil one of these purposes.

Employee data must be obtained from the employee directly. The employer can use third party sources only if it is not possible to obtain such data directly from the employee, and must obtain the employee's consent. For consent to be validly given, the employer must have informed candidates of the means by which personal data will be collected and the uses that the data will be put to. The employer cannot take decisions affecting employee's rights based on data obtained exclusively by automated or electronic means.

Information relating to an individual's membership of a trade union or other public associations (including political parties) can only be processed in certain circumstances specified by law, regardless of whether the individuals concerned have given their consent to such processing.

'Processing' is widely defined and will cover almost all dealings with personal data, whether done manually or by automated means.

Consent must be explicit and cannot be implied, so the fact that an individual may have included personal information on a social networking site does not mean that prospective employers or third parties are entitled to use this information.

Failure by an employer to comply with their obligations in relation to data processing could lead to claims for damages from both current and prospective employees. Individuals can also file complaints with the labour inspection (the state authority that controls compliance with employment law) and/or the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (Roskomnadzor).

2. What steps can be taken by employers to minimize such risks?

On the assumption that employers do not wish to ban the vetting of job applicants and employees using social media sites, the following steps should be taken to avoid unnecessary risk:

- the RF Labor Code requires employers to have in force a binding policy on the collection and use of personal data. Employees must confirm in writing that they are aware of the policy and its contents;
- the employer's internal data protection rules should mention, among other things, that personal data can be used to carry out background checks on employees and job candidates, and the employee's consent to this should be obtained;
- the rules should specify the purposes of such checks and the method used to obtain the information (e.g. browsing the internet);

- social media sites should be scanned only to check information that has previously been obtained directly from the employee. This limitation applies obviously only insofar as information posted on the site can be considered personal data or relates to the employee's private life;
- persons scanning the social media sites must be authorized to access personal data under the company's personal data protection rules;
- extracting data which relates to the employee's private life, religion, politics and membership of NGOs or labour unions should be prohibited;
- decisions relating to employees and job applicants should not be based exclusively on data extracted from social media sites;
- regardless of whether unsuccessful job applicants or existing employees are informed of the reasons for decisions taken in relation to them (whether on a general basis or only following a specific request) HR staff should be provided with a list of DOs and DON'Ts when providing such reasons. Care should be taken to refer only to information which could be obtained in strict compliance with data protection rules.

3. *What problems could an employer face as a result of employees using social media sites?*

Breach of confidentiality

Social media sites are open platforms for individuals to publish or exchange information. As such, individual users are personally responsible for complying with their legal and contractual obligations when using such sites. This will include duties of confidentiality to their employer and to their work colleagues.

However, if an employee acts in breach of these duties, for example by posting confidential details relating to a fellow employee, their employer could be liable for the employee's actions if the breach takes place in the course of employment. The fact that the employee could be dismissed or sued by the employer for damages may be of little comfort in this situation.

Damage to employer's or third party's reputation

Information posted on the internet can damage the reputation of the employer as well as the reputation of other employees, customers and suppliers. However, an employer would normally not be liable for an employee's defamatory conduct unless the employee was acting in the course of their employment.

Harassment/Unlawful discrimination

It is not uncommon for employees to use social media sites to post negative comments about fellow employees or to use information obtained from those sites as a basis for harassment of others. Under Russian law, the circumstances in which employers will be liable for such behaviour are limited. Liability will only accrue where the offending conduct has taken place under the instruction and control of the employer. In addition, there is no general duty on employers to protect their employees from harassment or ill-treatment.

Loss of productivity and other risks

Permitting employees to access social media sites during working hours could lead to a loss of productivity, a reduction in the quality of work produced by employees and a reduction in the level of discipline in the workforce. Employers should also consider the potential damage which could be caused to computer systems and software by employees visiting sites which are potentially infected with viruses and other malicious software.

4. What steps can be taken by an employer to minimize the risks associated with employees using social media sites?

An employer can implement the following policies to minimise risks:

- impose an outright ban on access to social media sites at work. Such a ban cannot eliminate all risks from the use of such sites as employees cannot be precluded from accessing them outside working hours. However, an employer should normally not incur liability for the employee's actions outside working hours;
- if an outright ban is not imposed, the employer should put in place internal policies dealing with the use of social media sites during working hours. Such policies should:
    - set out the parameters governing the use of the employer's IT systems;
    - stipulate that the employees visit social media sites at their own risk and not as part of the work assigned to them by the employer;
    - remind employees of the risks related to the use of the internet in general and social media in particular;
    - remind employees of their employment duties, in particular with regard to confidentiality and data protection, and specify the disciplinary sanctions (including, where applicable, dismissal) which can be taken against non-complying employees;
    - provide employees with a list of DOs and DON'Ts in connection with the use of social media;
- monitor the use of the internet at work to assess potential risks and inform employees that such monitoring is taking place. Russian law contains no

restrictions on workplace surveillance unless such surveillance involves the use of certain equipment which requires government authorisation;

- incorporate into employment contracts a special confidentiality clause, maintain internal rules on confidentiality and ensure that employees are properly acquainted with such rules. Under Russian law, employees do not have a general duty to keep confidential information belonging to the employer and the types of information that are protected by law are restricted, so it is prudent to impose a contractual obligation of confidentiality on employees.

Contributed by Secretan Troyanov Schaer SA

RUSSIA

SPAIN

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Social media sites, such as Facebook, Twitter and personal blogs, will often contain information about individual users, such as their sexual orientation, political beliefs, racial or ethnic origin, religion, marital status, disabilities, and data which reveals information about an individual's trade union memberships or health. Such information is afforded special protection under the Spanish Protection of Personal Data Act.

Implications under the Spanish Protection of Personal Data Act

Spanish law states that personal data may only be collected and processed if, to do so, it is adequate, relevant and not excessive in relation to the scope and the specified, explicit and legitimate purposes for which the data is obtained. "Processing" is widely defined and will encompass most circumstances in which data is used and stored. Therefore, when an employer gathers information concerning a job applicant from a social media site, it may be processing personal data.

Further, an employer may only process personal data if it has first obtained the explicit consent of the job applicant. The Company must also have informed the individual that the information will be held, the purposes for which it will be held, and the identity of the data controller. In certain cases, for example, information regarding an individual's racial origin, data may only be processed in particular circumstances specified by law.

If the data protection principles are not followed, the employer could face substantial financial penalties for the breach, and action may be taken against them by the Spanish Data Protection Agency.

In addition, job applicants who are rejected by a prospective employer on the basis of personal data obtained from social networking sites could bring claims for unlawful discrimination against the employer. However, the risk of such a claim being successful is generally low, as it will be difficult for an applicant to show that they were rejected on these grounds.

2. *What steps can be taken by employers to minimise such risks?*

In order to minimise the risks, employers might take the following steps:

- Implement an internal policy within the Company´s Human Resources Department, providing guidelines for obtaining and using personal data.
- Applicants could be warned at the start of the application process that data could be collected from social media and used in the application process. If they continue with the application, the applicants will be deemed to have consented to the use of their data in this way.

3. *What problems could an employer face as a result of employees using social media sites?*

Breach of confidentiality

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social media platforms, it is not uncommon for employees to end up posting confidential information about the employer and/or other employees. This could result in significant damage to the employer's business and reputation.

Damage to employer's or third party's reputation

Employees could post information on a social media site that causes damage to the reputation of the employer and/

or a third party. An employer may be vicariously liable for the defamatory conduct of an employee. The fact that an employer may have a claim against the employee concerned could be of little comfort compared to the damage to the reputation of the employer.

Harassment/Unlawful discrimination

It is not uncommon for employees to post negative comments about fellow employees on social media sites. The comments could relate to a protected characteristic, such as age, disability, race or sex. If an employee were to make such comments in the course of their employment, there is a danger that such comments could constitute harassment under the Spanish Workers' Statute and any relevant Collective Bargaining Agreement. In such circumstances, an employer could be vicariously liable for the actions of that employee.

An employer could also risk facing other discrimination claims if employees use information they have obtained from social media sites about other employees as the basis for treating them in a detrimental way.

Although, in Spain, there is no specific Act which provides protection from harassment, the Workers' Statute and the Health and Safety Act provide that employers may be found liable if they are aware that an employee is being harassed, and do nothing to prevent it or to protect the affected employee. If any claims of harassment are raised, it is therefore important that the employer carries out a full investigation into the complaints.

Loss of productivity

Aside from the potential legal issues, there could be an impact on productivity in the workforce if employees are able to access and use social media sites during work hours.

Problems of industrial espionage

Some companies have blocked access to Facebook because of concerns that, if their workers are connected to this type of social network during working hours, they may suffer industrial espionage.

Disciplinary Action

Employers should exercise caution when taking disciplinary action against, or dismissing, employees who have breached the Company's policy on the use of social media sites. For any dismissal on these grounds to be found to be fair by an Employment Tribunal, the employee's breach would need to be a very serious one. In addition, employers could face evidential difficulties as there are strict requirements that must be complied with when obtaining evidence on employees' use of computer systems. Any evidence of misuse that is obtained contrary to these requirements will be inadmissible before a Tribunal, which could lead to the dismissal being found to be automatically unfair, if there is insufficient admissible evidence to justify the dismissal.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

An employer can take the following steps:

- Impose an outright ban on access to social media sites at work. This approach could prove to be unpopular amongst employees and have an adverse impact on the morale within a workforce. Ultimately, the employer would need to weigh up the potential advantages and disadvantages in deciding whether to permit employees to access social media sites at work. A complete ban would not address the potential problems that could arise from postings by employees outside of working hours. Employers can easily find themselves liable for comments made after hours by employees,

particularly where there is an obvious and clear link to the employment. Accordingly, comments posted by one employee about another employee after hours on a social networking site could still end up as the responsibility of the employer.

- Put in place a social media policy which deals with the use of social media sites during and outside of work hours. Such a policy should have provisions dealing with social media activity but, in particular:
    - set out the parameters governing the use of the employer's IT systems;
    - remind employees that social media activity may not necessarily be private;
    - prohibit discrimination, harassment or bullying of other employees, which could include negative comments about employees posted on social media sites;
    - prohibit negative comments about the employer, its employees or third parties; and
    - prohibit the disclosure of any confidential information that relates to the employer and/or other employees.

  The policy should set out the consequences of a breach of the policy, which could include disciplinary action and, ultimately, dismissal.
- Provide awareness training to employees on conduct that could constitute discrimination, harassment and bullying. An employer would be able to defend any subsequent claim for discrimination or harassment if it can show that it took all reasonable steps to prevent the employee from committing the discriminatory act in question.

- Monitoring the use of social media sites at work could help to determine whether there is a loss of productivity as a result of employees accessing such sites. However, it is important to bear in mind that electronic forms of workplace surveillance would involve activity regulated under the Protection of Personal Data Act. Legal advice should be sought before engaging in any such monitoring.
- Incorporate within employment contracts an appropriate confidentiality clause which would afford protection to the employer in the event that an employee posts confidential information on a social media site.
- Disciplinary action may be taken against employees who misuse a social media site to the detriment of the employer. In some cases, an employer could consider dismissal. Each case will turn on its facts, and an employer might want to obtain legal advice before proceeding to dismiss the employee in question.
- If the employer decides to draft a policy on internet use, it may set different conditions for some workers or some categories of workers, allowing wider access to these social networks to some employees based on the work that they perform, and a more restricted access to other workers or categories of workers.

Contributed by Ramón & Cajal Abogados

SULTANATE OF OMAN

1. *Are there any risks for employers that use social media sites to vet job applicants?*

There are no provisions of Omani law that operate to govern or restrict the ability of employers to collect information on prospective employees from social media sites and to use that information to vet applicants. In particular, protection from discrimination is not extended to job applicants and applies only to existing employees.

In addition, Omani law has no real concept of data protection and the type of information that would be protected under, for example, European law (such as religion and marital status), is often included in CVs and on employee's personnel files.

2. *What steps can be taken by employers to minimise such risks?*

As stated above, there are no specific risks associated with the collection and use of information on prospective employees from social media sites.

If they wish, employers may adopt a code of conduct and/or establish their own internal rules on this point, but there is no legal obligation to do so.

3. *What problems could an employer face as a result of employees using social media sites?*

Breach of confidentiality

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social media platforms, it is not uncommon for employees to end up posting confidential information about the employer and/ other employees notwithstanding the duty of confidentiality that employees owe to their employer under the Omani standard form employment contract and the Labour Law. The duty of confidentiality of employees does not extend to other employees.

Damage to employer's or third party's reputation

Employees could post information on a social media site that causes damage to the reputation of the employer and/or a third party. Defamation is a criminal offence and can lead to imprisonment and/or a fine. There are also separate offences in relation to the use of telecommunications equipment to knowingly transmit defamatory statements, and to transmit material that is contrary to public order or good morals. There is no general definition of 'good morals' in these circumstances. However, the phrase should be interpreted in light of the prevailing culture of the Middle East.

It is unlikely, though, that employers would find themselves liable under these provisions for the actions of their employees, as employers are generally not vicariously liable in these circumstances. However, in the event that defamatory statements are made about a third party using the employer's telecommunications systems, the third party may have a cause of action against the employer. Having said this, the chances of such an action being successful are likely to be low, as the claimant would need to show that the employer had knowledge of the statements being made, and this would be very difficult to prove.

Harassment/Unlawful discrimination

Omani law does not have an offence of harassment. Unlawful discrimination as an offence is not relevant in these circumstances. It applies only to an employer's duty to treat employees equally under the Labour Law. The duty does not apply as between employees.

Loss of productivity

There could be the obvious negative impact on productivity if employees access and use social media sites during work hours.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

Employers could:

- Forbid or restrict the use of social media sites at work
- Include a social media policy in the employer's disciplinary procedures set out in the company's HR manual, including: (i) setting parameters for the use of the employer's IT systems; (ii) reminding employees that social media activity may not be private; (iii) prohibiting negative comments about the employer, its employees or third parties; and (iv) prohibiting the disclosure of confidential information that relates to the employer and/or other employees.
- Monitor the use of social media sites by employees to determine the extent of loss of productivity
- Take disciplinary action against employees who do not comply with the relevant company policies.

Contributed by SASLO

SULTANATE OF OMAN

SWEDEN

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Unlawful discrimination

Social media sites will often contain personal profiles of the individual concerned, which include information relating to certain characteristics, which form the basis of protection against discrimination under the Discrimination Act or the Parental Leave Act. These characteristics could be age, disability, sex (including pregnancy and maternity), race (including nationality), religion or belief, sexual orientation, gender reassignment, and marriage and civil partnership status. It is unlikely that most, if any, of these characteristics will feature in a CV. Therefore, if an employer has access to this information via a social media site and uses such information as the basis for refusing to recruit that person, then the employer's actions could constitute unlawful direct discrimination. The employer could face an increased risk of a claim for discrimination against it if the job applicant were to discover that their application was rejected because of one or more of the above characteristics.

Potential implications under the Personal Data Act

Vetting job applicants using information contained on social media sites could also have implications for employers in respect of their obligations under the Personal Data Act (PDA). The PDA regulates the 'processing' (i.e. collection, storage and all other use) of 'personal data'. Personal data means information that, directly or indirectly, relates to a living individual. 'Sensitive' personal data includes information relating to a person's sexuality, health, race and religion. Under the PDA, employers may process personal data as unstructured material (for example, personal data contained in word documents, e-mails or in texts published on the Internet) as long as such processing does not result in a violation of the individual's privacy, i.e. the processing

should be carried out for a proper purpose and information on individuals should not simply be collected and held for no reason. Consequently, the more information and sensitive personal data regarding an individual that is collected, the greater the risk that collecting and holding that information will be found to be a violation of privacy.

If any data collected from a social media network is stored in a structured, easily searchable system (for example, an HR records system, where the information on a particular employee can easily be located by a search under their name), the company will have to fulfil additional requirements in order to be able to justify the processing of this data under the PDA.

With respect to personal data included in such structured and searchable systems, the PDA requires employers to comply with general data protection requirements and, in the context of the use of social media, this may raise questions as to whether or not the requirements that the information held is accurate and that it is proportionate to use it in the way envisaged by the employer are fulfilled.

In particular, sensitive personal data can usually only be processed if the applicant has given explicit consent, the information constituting sensitive data has been made public as a result of steps taken by the applicant, or if one of a limited number of other legitimate aims has been satisfied. Further, the PDA requires employers to inform individuals concerned that their personal data is being processed. Failure to comply with data protection requirements could result in claims for compensation against the employer or action being taken against it by the Data Inspection Board (the Swedish data protection authority that protects the privacy of individuals in the information society).

2. What steps can be taken by employers to minimise such risks?

As a first step, employers should consider whether or not it is proportionate and relevant to use information obtained from social media in the recruitment process for the relevant position. If employers wish to use information from social media to vet job applicants, there are a number of steps which can be taken to guard against unnecessary risk:

- those scanning social media sites as part of the recruitment process (including external recruitment agencies) should be instructed to extract only legitimate and relevant information for the job application process;
- a social media policy or other written guidelines should back this up, so that the employer can demonstrate an intention to extract only relevant information;
- personal data obtained from social media should be kept as unstructured material and not be included in a system structured and searchable on personal data as such. This way, the processing of personal data can be justified under the PDA as long as the information collected is held for a proper purpose and does not violate the privacy of the job applicants;
- ideally, the person scanning the social media sites should not be the same as the person who determines the outcome of the recruitment process or who interviews the individual. This way, any irrelevant material (which might also contain sensitive personal data) will not make its way through to the decision maker;
- applicants should be informed, at the start of any application process, that a vetting or verification exercise using social media sites forms part of that process;
- job applicants who are rejected because of information gleaned from social media sites should be given an opportunity to correct that information before any final decisions are taken.

3. *What problems could an employer face as a result of employees using social media sites?*

Breach of confidentiality

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social media platforms, it is not uncommon for employees to end up posting confidential information about the employer and/or other employees. This could result in significant damage to the employer's business and reputation.

Damage to employer's or third party's reputation

Employees could post information on a social media site that causes damage to the reputation of the employer and/or a third party. An employer may be vicariously liable for the defamatory conduct of an employee. The fact that an employer may then have a claim against the employee concerned could be little comfort compared to the damage to the reputation of the employer.

Responsibility under the Personal Data Act

In the event that employees collect and maintain social media information about other individuals, e.g. customers or other employees, in the course of performing their job assignments, the employer may be required to comply with the requirements under the Personal Data Act in order to justify such processing of personal data. Any company that provides its own social media site (e.g. a company Facebook site) will also have a responsibility under the PDA for all comments posted on the site and must ensure that posted comments do not include defamatory or hostile statements or otherwise violate individuals' privacy.

Harassment/Unlawful discrimination

It is not uncommon for employees to post negative comments about fellow employees on social media sites. The comments could relate to a protected characteristic such as age, disability, race or sex. If an employee were to make such comments 'in the course of their employment', there is a danger that such comments could constitute harassment under the Discrimination Act. In such circumstances, an employer could be vicariously liable for the actions of that employee.

An employer could also risk facing other discrimination claims if employees use information they have obtained from social media sites about other employees as the basis for treating them in a detrimental way.

An employer will have a defence to any claim for discrimination or harassment if it can show that it took all reasonable steps to prevent the employee from committing the discriminatory act in question.

Loss of productivity

Aside from the potential legal issues, there could be the obvious negative impact on productivity in the workforce should an employer permit its employees to access and use social media sites using its equipment during work hours.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

An employer can take the following steps:

- impose an outright ban on access to social media sites at work. This approach could prove to be unpopular amongst employees and have an adverse impact on the morale within a workforce. It may also be difficult to uphold such policy in practice, as it is commonly accepted that employees (to a limited extent) may

use computers and telephones for private matters. Ultimately, the employer would need to weigh up the potential advantages and disadvantages in deciding whether to permit employees to access social media sites at work. A complete ban would not address the potential problems that could arise from postings by employees outside of working hours. Employers can easily find themselves liable for comments made after hours by employees, particularly where there is an obvious and clear link to the employment. Accordingly, comments posted by one employee about another employee after hours on a social networking site could still end up as the responsibility of the employer;

- put in place a social media policy which deals with the use of social media sites during and outside of work hours. Such a policy should have provisions dealing with social media activity, but, in particular, should also:
    - set out the parameters governing the use of the employer's IT systems;
    - remind employees that social media activity may not necessarily be private;
    - prohibit discrimination, harassment or bullying of other employees, which could include negative comments about employees posted on social media sites;
    - prohibit collection and registration of personal data from social media sites, unless it can be justified under the PDA;
    - prohibit negative comments about the employer, its employees or third parties; and
    - prohibit the disclosure of any confidential information that relates to the employer and/or other employees.

The policy should set out the consequences of a breach of the policy, which could include disciplinary action and, ultimately, dismissal:

- provide awareness training to employees on conduct that could constitute discrimination, harassment, bullying or a violation of the PDA. An employer would be able to defend any subsequent claim for discrimination or harassment if it can show that it took all reasonable steps to prevent the employee from committing the discriminatory act in question;
- monitoring the use of social media sites at work could help to determine whether there is a loss of productivity as a result of employees accessing such sites. However, it is important to bear in mind that electronic forms of workplace surveillance would involve activity regulated under the PDA. Legal advice should be sought before engaging in any such monitoring;
- incorporate within employment contracts an appropriate confidentiality clause, which would afford protection to the employer in the event that an employee posts confidential information on a social media site;
- disciplinary action may be taken against employees who misuse a social media site to the detriment of the employer. In some cases, an employer could consider dismissal. Each case will turn on its facts and an employer might want to obtain legal advice before proceeding to discipline or dismiss the employee in question.

Contributed by Advokatfirman Vinge KB

SWEDEN

SWITZERLAND

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Swiss law does not expressly address the collection and processing of data collected from the internet. The commonly held view is that information obtained from social media websites can be used by an employer when processing job applications. Nevertheless, employers do face some restrictions under the Swiss Civil Code of Obligations (CO) and the Data Protection Act (DPA). These restrictions are dealt with below.

Restrictions under the Swiss Code of Obligations

It is presumed that persons who disclose their personal data on a private website consent to their data being used by third parties. Despite such presumed consent, the CO provides that an employer may only use and process data of an applicant to the extent that such data is used to assess the aptitude of an applicant to perform the job in question. Such data could include sensitive data, such as age and sex. The type of data that can be lawfully used will depend on the job profile.

The exception to the above rule is in relation to data that relates to sexual orientation or the membership of a political party. The collection of such data could be unlawful under the CO.

Restrictions under the Data Protection Act

The DPA regulates the collection and use of 'personal data'. Personal data means information that relates to an individual who can be identified from that information. 'Sensitive' personal data includes information relating to a person's sexuality, race, health and religion. Under the DPA, employers have onerous additional obligations when 'processing' sensitive personal data that go beyond the restrictions under the CO.

When an employer collects information about an applicant from a social media site, it may be processing sensitive information. In such circumstances, the DPA requires employers to comply with general data protection principles, i.e. data may only be used for the purpose for which it was initially collected, and data processing requires the consent of the individual concerned. In the context of the use of social media sites, there may be an issue as to whether it is proportionate to use data from such sites. In particular, sensitive data can usually only be processed if the applicant has given explicit consent. However, as mentioned above, such consent will be irrelevant if the data that is being used is not required for the purpose of assessing the applicant's aptitude for the job.

Failure to comply with the data protection principles under the DPA could result in claims for compensation against the employer, or action being taken against it by the Federal Data Protection and Information Commissioner.

2. What steps can be taken by employers to minimise such risks?

Assuming employers do not wish to take steps to ban all vetting of job applicants using information from social media, there are a number of steps which can be taken to guard against unnecessary risk:

- Employers should ban the use of fictitious user profiles for the purposes of vetting an applicant's social media site. For example, where the employer registers on a social media site under a fictitious identity and becomes a "friend" of the applicant.
- Those scanning social media sites as part of the recruitment process should be instructed to extract only legitimate and relevant information for the job application process and the job profile in question.

- A social media policy or other written guidelines should back this up, so that the employer can demonstrate an intention to extract only relevant information.
- Ideally, the person scanning the social media sites should not be the same as the person who is determining the job application process or interviewing the individual. This way, the irrelevant material (which might contain sensitive personal data) will not make its way through to the decision maker.

3. *What problems could an employer face as a result of employees using social media sites?*

Damage to reputation and contractual risks

The company and its business are publicly linked to the employee in question, which may result in reputational risk for the employer, depending on the employee's behaviour in the social media site in question. Further, the careless use of social media sites may lead to disclosure of the employer's confidential information. There could also be disclosure of confidential information the employer has acquired from a contracting party. Such a disclosure could result in the employer's breach of contract with that party. The fact that the employer could have a claim against the employee for breach of their employment contract could be of little comfort if the damage incurred is substantial.

Loss of productivity

Aside from the potential legal issues, there could be the obvious negative impact on productivity in the workforce, should an employer permit its employees to access and use social media sites using its equipment during work hours. In addition, the extensive use of social media sites at work could cause problems with the employer's network capacity. To cite an example, the Zurich government banned access

to Facebook and similar social media sites due to the costs associated with 3.3 million monthly visits of such sites by its employees.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

Ban

The employer may issue an outright ban on accessing social media sites during working hours, and block such sites on its computers.

Guidelines

The employer could put in place a social media policy which deals with the use of social media sites during and outside of work hours. Such a policy should have provisions dealing with social media activity but, in particular:

- set out the parameters governing the use of the employer's IT systems;
- remind employees that social media activity (as with any other internet activity, including the use of e-mail) may not necessarily be private;
- prohibit discrimination, harassment or bullying of other employees, which could include negative comments about employees posted on social media sites;
- prohibit negative comments about the employer, its employees or third parties; and
- prohibit the disclosure of any confidential information that relates to the employer, its customer and/or other employees.

The policy should set out the consequences of a breach of the policy, which could include disciplinary action, dismissal or termination for cause.

Monitoring

Monitoring the use of social media sites at work could help to determine whether there is a loss of productivity as a result of employees accessing such sites. Such monitoring may be unlawful under the Swiss Labour Law Act. Therefore, legal advice should be sought before engaging in any such monitoring.

Confidentiality clauses in Employment Agreements

It should be considered whether to incorporate, within employment contracts, an appropriate confidentiality clause which would afford protection to the employer in the event that an employee posts confidential information on a social media site.

Training

Employers should constantly educate their employees with regard to the risks associated with the use of social media sites. Often, employees use such systems without the required level of awareness of the risks involved in posting data that could be detrimental to the employer.

Contributed by Pestalozzi Attorneys at Law Ltd

SWITZERLAND

REPUBLIC OF TURKEY

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Unlawful discrimination

Under the Labour Code, discrimination in employment on the grounds of language, race, colour, sex, political opinion, philosophical belief, religion and sect is prohibited. Therefore, an employer's access to this type of information through a social media web site and a subsequent decision to refuse to recruit a job applicant on the basis of such information could constitute unlawful discrimination. In such circumstances, the applicant could bring a claim against the employer and seek compensation.

Potential data protection implications

Privacy and personal data is protected under Turkish Constitutional Law, the Turkish Civil Code, the Turkish Criminal Code, and the Turkish Labour Code. Although there is no specific definition of "personal data" under Turkish law, it most likely can be defined as information which relates to health, family and private life, dignity and professional and family values of an individual. The unauthorised use and disclosure of personal data could constitute a violation of privacy under Turkish law.

An employer is, of course, permitted to vet applicants using information contained in their application form. In addition, an employer can legitimately undertake checks in a limited manner, and only in relation to any information that is publicly available from official government sites or sources (for example, social security number, ID details and other information relating to professional qualifications) without the consent of the applicant. Aside from these types of information, prior written consent is required before an employer can use information obtained from other sources to vet the applicant. Therefore, if an employer uses any

personal data contained in a social media site (even if widely accessible) to vet an applicant, without the written consent of that applicant, the employer's actions could be unlawful under Turkish law. In such circumstances, the employer could face a claim for compensation, and its actions might also constitute a criminal offence, which could result in imprisonment.

Restrictions in terminating employment

An applicant is bound by the information that he or she provides in a job application form and job interview, and is therefore under an obligation to give accurate information during the recruitment process. However, if the information provided is found to be incorrect, the employer will be entitled to terminate the employment contract. In contrast, if an employer relies upon information about an applicant that it obtained from a social media site which subsequently transpires to be incorrect, it will not be entitled to terminate the contract of employment for reasons that relate to the incorrect information it obtained.

2. *What steps can be taken by employers to minimise such risks?*

As mentioned above, privacy and personal data is protected under Turkish Constitutional Law, the Turkish Civil Code, the Turkish Criminal Code, and the Turkish Labour Code, and written consent will need to be obtained from the applicant when using information from social media sites to vet that applicant.

Therefore, if employers wish to vet job applicants using information from social media sites, then, in order to minimise the risks, prior consent should be obtained from the applicants. The applicants should be informed that the employer will scan social media sites as part of the recruitment process. In addition, in the event that the applicant is rejected because of information gained from social media sites, then it would be advisable for the employer

to explain the reasons to the applicant and give the applicant the opportunity to correct such information before any final decisions are taken.

In addition to the above steps, it is recommended that employers take the following steps:

- Those scanning social media sites as part of the recruitment process should be instructed to extract only legitimate and relevant information for the job application process.
- A social media policy or other written guidelines should back this up, so that the employer can demonstrate an intention to extract only relevant information.
- Ideally, the person scanning the social media sites should not be the same as the person who is determining the job application process or interviewing the individual. This way, the irrelevant material (which might contain sensitive personal data) will not make its way through to the decision maker.

3. *What problems could an employer face as a result of employees using social media sites?*

Breach of confidentiality

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social media platforms, it is not uncommon for employees to end up posting confidential information about the employer and/or other employees. This could result in significant damage to the employer's business and reputation.

Damage to employer's or third party's reputation

Under the Turkish Code of Obligation, the employer is vicariously liable for the acts of its employees. Employees could post information on a social media site that causes

damage to the reputation of the employer and/or a third party. The employer may be able to recover damages from the relevant employee if it can prove, with written evidence before a court, that the damages it has sustained arose from the failure of the employee to perform his or her duties under the contract of employment, employee handbook or in accordance with Turkish law.

Harassment/Unlawful discrimination

Under the Turkish Constitution and Labour Code, it is unlawful to discriminate on the protected grounds of language, race, colour, sex, political opinion, philosophical belief, religion and sect. Employees could post negative comments about fellow employees on social media sites. The comments could relate to one of the above protected grounds. If an employee were to make such comments, there is a danger that such comments could constitute discrimination or harassment. In such circumstances, an employer could be vicariously liable for the actions of that employee.

An employer could also risk facing other discrimination claims if employees use information they have obtained from social media sites about other employees as the basis for treating them in a detrimental way.

An employer will have a defence to any claim for discrimination or harassment if it can show that it took all reasonable steps to prevent the employee from committing the discriminatory act in question.

In addition, under the Turkish Criminal Code, harassment could constitute a criminal offence. The individual responsible for harassment in the workplace could face imprisonment.

Loss of productivity

Employers could find that there is a loss of productivity in their workforce as a result of employees using social media sites during working hours.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

The following steps can be taken to minimise the risks associated with employees using social media sites:

- Impose an outright ban on access to social media sites at work. This approach could prove to be unpopular amongst employees and have an adverse impact on the morale within a workforce. Ultimately, the employer would need to weigh up the potential advantages and disadvantages in deciding whether to permit employees to access social media sites at work. A complete ban would not address the potential problems that could arise from postings by employees outside of working hours. Employers can easily find themselves liable for comments made after hours by employees, particularly where there is an obvious and clear link to the employment. Accordingly, comments posted by one employee about another employee after hours on a social networking site could still end up as the responsibility of the employer.
- A confidentiality clause can be added to the employment contract restricting the use of confidential information and giving the right to the employer to terminate the employment contract without any notice and compensation in the event that there is a breach of confidentiality.
- Prevent employees from accessing social media sites during work hours.
- Training sessions can also be provided to educate employees on the problems that could arise from misusing social media sites.

- Put in place a social media policy which deals with the use of social media sites during and outside of work hours. Such a policy should have provisions dealing with social media activity but, in particular:
    - set out the parameters governing the use of the employer's IT systems;
    - remind employees that social media activity may not necessarily be private;
    - prohibit discrimination, harassment or bullying of other employees, which could include negative comments about employees posted on social media sites;
    - prohibit negative comments about the employer, its employees or third parties; and
    - prohibit the disclosure of any confidential information that relates to the employer and/or other employees.
- An employee's use of social media sites at work can be monitored, but only with the written consent of the employee. An employee's e-mails can be monitored and reviewed by the employer in the event that he or she is on sick leave, and the right to monitor is expressly referred to in the employment contract or in the employee handbook. The monitoring of employee communications should be limited to the date, the parties and other work-related content in order to avoid unlawful monitoring of personal and non-work related data of the employee.

Contributed by Pekin & Pekin

UAE

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Discrimination on the grounds of sex, marital status, race, nationality, religion or disability is prohibited, but only in the Dubai International Financial Centre (DIFC). The DIFC is considered to have independent jurisdiction with its own laws and regulations. Therefore, if an employer has access to any of this information via a social media site, and uses this as the basis for refusing to recruit that person, then the employer's actions could constitute unlawful direct discrimination under the DIFC Employment Law. An employer based in the DIFC could face a claim for discrimination if the job applicant were to discover that his or her application was rejected because of one or more of the above characteristics.

Potential implications under the Dubai International Finance Centre Data Protection Law

Currently, the UAE does not have any federal law relating to data protection. However, a law regulating personal data does exist in the DIFC.

The DIFC Data Protection Law (DPL) regulates the collection and use of personal data, which constitutes any information relating to an identifiable natural person. The DPL also regulates the collection and use of 'sensitive personal data', which constitutes any data revealing or concerning, either directly or indirectly, any racial or ethical origin, communal origin, political affiliation or opinion, religious or philosophical belief, criminal records, trade union memberships, health or sex lives. Therefore, if an employer has access to this information via a social media site and uses such information as the basis for refusing to recruit that person, then the employer's actions could constitute unlawful discrimination.

The DPL requires employers in the DIFC to comply with certain general data protection principles. It also requires that employers obtain the consent of the applicant to whom sensitive data relates, before processing such data. Without consent from the applicant, such data obtained from social media sites for the purposes of vetting can only be lawfully processed if such data is made public by the individual.

The above restriction does not apply if a permit to process such sensitive data has been obtained from the Commissioner of Data Protection, or if the employer applies adequate safeguards with respect to processing the sensitive personal data.

Where data is not obtained from the applicant, the employer is required to provide the applicant with certain information, including the following:

- the identity of the data controller;
- the purposes of the processing;
- any further information that is necessary, having regard to the specific circumstances in which the personal data is processed, to guarantee fair processing;
- the categories of data concerned;
- the recipients of the data; and
- the existence of the right of the applicant to access and rectify his or her personal data, and ascertain whether the data will be used for the purposes of direct marketing.

If an applicant has reasonable grounds to believe that an employer has breached the DPL, he or she could lodge a complaint with the Commissioner of Data Protection. Further, if an applicant suffers damage as a result of the employer's breach, he or she could be entitled to compensation from the employer.

Potential breach of privacy

The UAE Constitution guarantees the right to privacy. An employer that uses information about an applicant from a social media site that is not publicly available could result in a breach of the applicant's privacy. The UAE Constitution and Penal Code also provide protection to individuals against interception and subsequent disclosure or publication of their personal data. A breach of the Penal Code could result in fines and imprisonment.

2. *What steps can be taken by employers to minimise such risks?*

Assuming employers do not wish to take steps to ban all vetting of job applicants using information from social media, there are a number of steps which can be taken to guard against unnecessary risk:

- Those scanning social media sites as part of the recruitment process should be instructed to extract only legitimate and relevant information for the job application process.
- A social media policy or other written guidelines should back this up, so that the employer can demonstrate an intention to extract only relevant information.
- Ideally, the person scanning the social media sites should not be the same as the person who is determining the job application process or interviewing the individual. This way, the irrelevant material (which might contain sensitive personal data) will not make its way through to the decision maker.
- Applicants should be told, at the start of any application process, that a vetting or verification exercise using social media sites forms part of the process.

- Job applicants who are rejected because of information gleaned from social networking should be given an opportunity to correct that information before any final decisions are taken.

3. *What problems could an employer face as a result of employees using social media sites?*

Unlawful discrimination

An employer based in the DIFC could risk facing other discrimination claims if employees use information they have obtained from social media sites about other employees as the basis for treating them in a detrimental way.

Breach of confidentiality

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social media platforms, it is not uncommon for employees to end up posting confidential information about the employer and/or other employees. This could result in significant damage to the employer's business and reputation.

Loss of productivity

Aside from the potential legal issues, there could be the obvious negative impact on productivity in the workforce should an employer permit its employees to access and use social media sites using its equipment during work hours.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

An employer can take the following steps:

- Impose an outright ban on access to social media sites at work.

- Alternatively, put in place a social media policy which deals with the use of social media sites during and outside of work hours. Such a policy should have provisions dealing with social media activity but, in particular:
    - set out the parameters governing the use of the employer's IT systems;
    - remind employees that social media activity may not necessarily be private;
    - prohibit discrimination, harassment or bullying of other employees, which could include negative comments about employees posted on social media sites;
    - prohibit negative comments about the employer, its employees or third parties; and
    - prohibit the disclosure of any confidential information that relates to the employer and/or other employees.

  The policy should set out the consequences of a breach of the policy, which could include disciplinary action and, ultimately, dismissal.
- Provide awareness training to employees on conduct that could constitute discrimination, harassment and bullying.
- Monitoring the use of social media sites at work could help to determine whether there is a loss of productivity as a result of employees accessing such sites. Legal advice should be sought before engaging in any such monitoring.

- Incorporate within employment contracts an appropriate confidentiality clause, which would afford protection to the employer in the event that an employee posts confidential information on a social media site.
- Disciplinary action may be taken against employees who misuse a social media site to the detriment of the employer. In some cases, an employer could consider dismissal. Each case will turn on its facts and an employer might want to obtain legal advice before proceeding to dismiss the employee in question.

Contributed by Shalakany Law Office

UNITED KINGDOM

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Unlawful discrimination

Social media sites will often contain personal profiles of the individual concerned, including certain details which form the basis of protection against discrimination under the Equality Act 2010. These characteristics could be age, disability, sex (including pregnancy and maternity), race (including nationality), religion or belief, sexual orientation, gender reassignment, and marriage and civil partnership status. It is unlikely that most, if at all any, of these characteristics will feature in a CV. Therefore, if an employer has access to this information via a social media site and uses such information as the basis for refusing to recruit that person, then the employer's actions could constitute unlawful direct discrimination. The employer could face an increased risk of a claim for discrimination against it if the job applicant were to discover that their application was rejected and one or more of the above characteristics had been identified by the employer before the application was rejected.

Potential implications under the Data Protection Act 1998

Vetting job applicants using information contained on social media sites could also have implications for employers in respect of its obligations under the Data Protection Act 1998 (DPA). The DPA regulates the collection and use of 'personal data'. Personal data means information (including expressions of opinion) that relates to a living individual who can be identified from that information. 'Sensitive' personal data includes information relating to a person's sexuality, race and religion. Under the DPA, employers have onerous obligations when 'processing' sensitive personal data. The concept of 'processing' includes obtaining, recording, holding or using personal data. Therefore, when an employer collects information about an applicant from a social media

site, it may be processing sensitive information. In such circumstances, the DPA requires employers to comply with general data protection principles. In the context of the use of social media, this may raise questions as to whether or not the information is accurate and it is proportionate to use it in this way. In particular, sensitive data can usually only be processed if the applicant has given explicit consent, the information contained in the sensitive data has been made public as a result of steps taken by the applicant or if one of a limited number of other legitimate aims has been satisfied. The failure to comply with these data protection principles could result in claims for compensation against the employer or action being taken against it by the Information Commissioner (the UK authority that upholds information rights and data privacy for individuals).

The Employment Practices Data Protection Code provides best practice guidance for employers on the use of information in the context of recruitment and selection. It recommends that employers give job applicants the opportunity to comment on the accuracy of any background checks or information it has obtained about them. Although a breach of the Code is not actionable in itself, it could be taken into account when considering whether or not the employer has breached any of its obligations under the DPA.

2. What steps can be taken by employers to minimise such risks?

Assuming employers do not wish to take steps to ban all vetting of job applicants using information from social media there are a number of steps which can be taken to guard against unnecessary risk:

- Those scanning social media sites as part of the recruitment process should be instructed to extract only legitimate and relevant information for the job application process.

- A social media policy or other written guidelines should back this up, so that the employer can demonstrate an intention to extract only relevant information.
- Ideally, the person scanning the social media sites should not be the same as the person who is determining the job application process or interviewing the individual. This way, the irrelevant material (which might contain sensitive personal data) will not make its way through to the decision maker.
- Applicants should be told, at the start of any application process that a vetting or verification exercise using social media sites forms part of the process.
- Job applicants who are rejected because of information gleaned from social networking should be given an opportunity to correct that information before any final decisions are taken.

3. *What problems could an employer face as a result of employees using social media sites?*

Breach of confidentiality/IP rights

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social media platforms, it is not uncommon for employees to end up posting confidential information about the employer and/other employees. This could result in significant damage to the employer's business and reputation.

In addition, employees could post material on social media sites that infringes the intellectual property rights of third parties, and the employer could be held liable for such infringement.

Damage to employer's or third party's reputation

Employees could post information on a social media site that causes damage to the reputation of the employer and/or a third party. An employer may be vicariously liable for the defamatory conduct of an employee. The fact that an employer may have a claim against the employee concerned could be little comfort compared to the damage to the reputation of the employer.

Harassment/Unlawful discrimination

It is not uncommon for employees to post negative comments about fellow employees on social media sites. The comments could relate to a protected characteristic such as age, disability, race or sex. If an employee were to make such comments 'in the course of their employment', there is a danger that such comments could constitute harassment under the Equality Act 2010. In such circumstances, an employer could be vicariously liable for the actions of that employee.

An employer could also risk facing other discrimination claims if employees use information they have obtained from social media sites about other employees as the basis for treating them in a detrimental way.

An employer will have a defence to any claim for discrimination or harassment if it can show that it took all reasonable steps to prevent the employee from committing the discriminatory act in question.

An employer could also find face civil or criminal liability under the Protection from Harassment Act 1997. Although the precise standards of behaviour necessary to create liability under the Act are still being worked through by the Courts, in one recent case three letters sent during litigation were enough to create liability under the Act, since they overstepped the boundaries of a robust litigation strategy. In

the circumstances, posting a series of comments which are offensive or derogatory about a colleague may be sufficient to create liability.

Solicitation

Employees frequently build up lists of contacts during their employment. Colleagues and clients could be 'friends' on sites such as Facebook, or contacts on dedicated business networking sites such as LinkedIn. While this can be very valuable to an employer while an individual is their employee, such contact lists can be equally valuable to their competitors or to the individual themselves once that employment has ended. Former employees could use information gained during their employment to solicit employees or key clients of their former employer, which could have a substantial impact on the employer's business.

Loss of productivity

Aside from the potential legal issues, there could be the obvious negative impact on productivity in the workforce should an employer permit its employees to access and use social media sites using its equipment during work hours.

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

An employer can take the following steps:

- Impose an outright ban on access to social media sites at work. This approach could prove to be unpopular amongst employees and have an adverse impact on the morale within a workforce. Ultimately, the employer would need to weigh up the potential advantages and disadvantages in deciding whether to permit employees to access social media sites at work. A complete ban would not address the potential problems that could arise from postings by employees outside of

working hours. Employers can easily find themselves liable for comments made after hours by employees, particularly where there is an obvious and clear link to the employment. Accordingly, comments posted by one employee about another employee after hours on a social networking site could still end up as the responsibility of the employer.

- Put in place a social media policy which deals with the use of social media sites during and outside of work hours. Such a policy should have provisions dealing with social media activity, but in particular:
    - set out the parameters governing the use of the employer's IT systems;
    - remind employees that social media activity may not necessarily be private;
    - prohibit discrimination, harassment or bullying of other employees, which could include negative comments about employees posted on social media sites;
    - prohibit negative comments about the employer, its employees or third parties; and
    - prohibit the disclosure of any confidential information that relates to the employer and/or other employees.

  The policy should set out the consequences of a breach of the policy, which could include disciplinary action and, ultimately, dismissal.
- Provide awareness training to employees on conduct that could constitute discrimination, harassment and bullying. An employer would be able to defend any subsequent claim for discrimination or harassment if it can show that it took all reasonable steps to prevent the

employee from committing the discriminatory act in question.

- Monitoring the use of social media sites at work could help to determine whether there is a loss of productivity as a result of employees accessing such sites. However, it is important to bear in mind that electronic forms of workplace surveillance would involve activity regulated under the DPA and possibly the Regulation of Investigatory Powers Act 2000. Legal advice should be sought before engaging in any such monitoring.
- Incorporate within employment contracts an appropriate confidentiality clause, which would afford protection to the employer in the event that an employee posts confidential information on a social media site.
- Incorporate appropriate post-termination restrictive covenants within employment contracts, which prevent former employees from soliciting colleagues, customers and/or suppliers for a set period post-termination.
- Disciplinary action may be taken against employees who misuse a social media site to the detriment of the employer. In some cases, an employer could consider dismissal. Each case will turn on its facts and an employer might want to obtain legal advice before proceeding to dismiss the employee in question.

Contributed by Mayer Brown International LLP

UNITED KINGDOM

The Americas

BRAZIL

1. *Are there any risks for employers that use social media sites to vet job applicants?*

   Yes. Employers risk unlawfully discriminating against an applicant if they refuse employment based on use of protected information taken from a social media site.

2. *What steps can be taken by employers to minimise such risks?*

   - Avoid disclosing that social media sites are reviewed.
   - Only extract legitimate and relevant information. A social media policy should set out guidelines to this effect.
   - The person scanning the social media site should not be the same as the person determining the outcome of the recruitment process.

3. *What problems could an employer face as a result of employees using social media sites?*

   Employees using social media sites could breach confidentiality and cause damage to the employer's or a third party's reputation. Employers could also face a loss of productivity across the work force.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

   - Inform employees that their use of electronic equipment should be for work purposes only and that this will be monitored.
   - Ban access to social media sites at work.

BRAZIL

- Produce a social media policy, setting out the rules and standards expected.
- Provide employees with training.
- Include a confidentiality clause in employment contracts.

Contributed by Tauil & Chequer

UNITED STATES

1. *Are there any risks for employers that use social media sites to vet job applicants?*

   Yes. An employer could run the risk of facing discrimination claims if it rejects applications on the basis of information it has obtained from a social media site that relates to one or more protected characteristics of the applicant.

2. *What steps can be taken by employers to minimise such risks?*

   - Ban the use of social media sites for screening applicants.
   - Choose a person to scan social media sites who is not the same person who determines which applicant will go to the next stage in the application process.
   - Applicants should be told at the start of any application process that social media sites might be used as part of the screening process.
   - Extract and use only legitimate and relevant information.
   - Put in place a social media policy.
   - Applicants should be given an opportunity to correct any information that is relied upon before any final decisions are taken.

3. *What problems could an employer face as a result of employees using social media sites?*

   An employee could post information on a social media site that breaches their obligations of confidentiality to their employer. An employee could also post information that damages their employer's reputation. An employer also runs the risk of its employees posting endorsements about products without the requisite authorisation, which could result in the employer being held liable under the Federal Trade Commission guidelines. An employer could also be held liable for any postings by employees that constitute unlawful

discrimination or harassment against other employees. The use of social media sites could also result in a loss of productivity within the workforce.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

- Impose an outright ban on the use of social media in the workplace.
- Put in place a social media policy which deals with the use of social media sites during and outside of working hours.
- Provide training to employees on the pitfalls of using social media sites.
- Monitor the use of social media sites at work.
- Incorporate within employment contracts an appropriate confidentiality clause.
- Take disciplinary action against employees who misuse social media sites.

Contributed by Mayer Brown LLP

BRAZIL

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Unlawful discrimination

Brazilian legislation is very protective with respect to equal opportunities in employment, and there are several legal provisions that expressly forbid any kind of prejudice in relation to the recruitment process and the employment relationship.

Social media sites will often contain personal profiles of the individual concerned, including certain characteristics, which form the basis of protection against discrimination under the Brazilian Constitution. These characteristics could be age, disability, sex (including pregnancy and maternity), race (including nationality), religion or belief, sexual orientation and marital status. It is unlikely that most, if any, of these characteristics will feature in a CV. Therefore, if an employer has access to this information via a social media site, and uses such information as the basis for refusing to recruit that person, then the employer's actions could constitute unlawful direct discrimination. The employer could face an increased risk of a claim for discrimination against it if the job applicant were to discover that their application was rejected because of one or more of the above characteristics.

If a candidate is not offered the job due to their race, ethnic or national origin, gender, skin colour or religion, this will be considered a crime, which could result in a prison sentence of between 2 and 5 years. Employers should ensure that the admission process is based on the technical ability/ qualifications of the applicant, regardless of his/her age, gender, race, disabilities, or ethnic origin.

BRAZIL

2. What steps can be taken by employers to minimise such risks?

In Brazil, employers are not obliged to justify to applicants the reason why they were not chosen for the job they applied for. As such, it would not be advisable for employers to make applicants aware that information from social media sites was used in the recruitment process. If they know that social media sites were referred to, an unsuccessful applicant could attribute the employer's refusal to hire him to the information gleaned from social media. There are a number of steps which can be taken to guard against unnecessary risk:

- The employer should not disclose to applicants that reviewing information on social media sites is part of the recruitment process.
- If the employer decides to disclose that information from social media is used in the recruitment process, those scanning social media sites as part of the recruitment process should be instructed to extract only legitimate and relevant information for the job application process.
- A social media policy or other written guidelines should back this up, so that the employer can demonstrate that their intention was to extract only relevant information.
- Ideally, the person scanning the social media sites should not be the same as the person who is determining the job application process or interviewing the individual. This way, the irrelevant material (which might contain sensitive personal data) will not make its way through to the decision maker.

3. *What problems could an employer face as a result of employees using social media sites?*

Breach of confidentiality

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social media platforms, it is not uncommon for employees to end up posting confidential information about the employer and/or other employees. This could result in significant damage to the employer's business and reputation.

Damage to employer's or third party's reputation

Employees could post information on a social media site that causes damage to the reputation of the employer and/or a third party. An employer may be vicariously liable for the defamatory conduct of an employee. The fact that an employer may have a claim against the employee concerned could be little comfort compared to the damage to the reputation of the employer.

Loss of productivity

Aside from the risks described above, being permitted to use social media sites during working hours could clearly have a negative effect on employees' productivity.

4. *What steps can be taken by an employer to minimise the risks associated with employees using social media sites?*

An employer can take the following steps:

- Expressly inform employees that their email and use of the internet will be monitored by the employer and state that the use of company electronic systems should be exclusively for work purposes. Monitoring an employees'

use of social media sites at work could help to determine whether there is a loss of productivity as a result of employees accessing such sites.

- Impose an outright ban on access to social media sites at work. This approach could prove to be unpopular amongst employees and have an adverse impact on the morale within a workforce. Ultimately, the employer would need to weigh up the potential advantages and disadvantages in deciding whether to permit employees to access social media sites at work. A complete ban would not address the potential problems that could arise from postings by employees outside of working hours. Employers can easily find themselves liable for comments made after hours by employees, particularly where there is an obvious and clear link to the employment. Accordingly, comments posted by one employee about another employee after hours on a social networking site could still end up as the responsibility of the employer.
- Put in place a social media policy which deals with the use of social media sites during and outside of work hours. Such a policy should have provisions dealing with social media activity but, in particular:
    - set out the parameters governing the use of the employer's IT systems;
    - remind employees that social media activity may not necessarily be private;
    - prohibit discrimination, harassment or bullying of other employees, which could include negative comments about employees posted on social media sites;

- prohibit negative comments about the employer, its employees or third parties; and
- prohibit the disclosure of any confidential information that relates to the employer and/or other employees.

The policy should set out the consequences of a breach of the policy, which could include disciplinary action and, ultimately, dismissal.

- Provide awareness training to employees on conduct that could constitute discrimination, harassment and bullying. An employer would be able to defend any subsequent claim for discrimination or harassment if it can show that it took all reasonable steps to prevent the employee from committing the discriminatory act in question.
- Incorporate, within employment contracts, an appropriate confidentiality clause which would afford protection to the employer in the event that an employee posts confidential information on a social media site.
- Disciplinary action may be taken against employees who misuse a social media site to the detriment of the employer. In some cases, an employer could consider dismissal. Each case will turn on its facts, and an employer might want to obtain legal advice before proceeding to dismiss the employee in question.

Contributed by Tauil & Chequer

BRAZIL

UNITED STATES

1. *Are there any risks for employers that use social media sites to vet job applicants?*

Social media sites will often contain pictures or personal profiles of the individual applying for a position that disclose to the viewer certain protected characteristics that can form the basis of protection against discrimination. Under US federal law, the protections are provided through Title VII of the Civil Rights Act of 1964, the Age Discrimination in Employment Act, the Americans with Disabilities Act, the Genetic Information Non-Discrimination Act and various laws protecting whistleblowers.

The characteristics protected under federal law are gender (including pregnancy), race, national origin, religion or belief, age, disability, genetic information or whistleblower status. In addition, many states have laws that protect against discrimination on the basis of characteristics such as sexual orientation, gender reassignment, and marital status. Many states also have laws that limit the extent to which a potential employer can consider an applicant's criminal history, especially arrest records. Federal and state laws also limit an employer's ability to take into account an applicant's credit history or require additional disclosures when an employer does so. The US Equal Employment Opportunity Commission, the federal agency charged with preventing discrimination, also discourages the use of criminal background checks and credit checks, on the grounds that such criteria have a disparate impact on minority applicants. Finally, many states have statutes that protect a person's right to engage in lawful activity, such that an applicant may have a basis for bringing an action if the applicant were rejected for employment because the applicant had engaged in lawful activity that was distasteful to the employer, such as smoking, drinking, or political activity.

UNITED STATES

Looking at all of the potentially protected criteria described above, it is unlikely that most of these characteristics would be featured in a CV. The fact that the employer does not solicit information regarding protected characteristic status and does not have access to such information tends to protect an employer from claims that protected characteristics were improperly considered in selecting job applicants. Conversely, if an employer obtains access to information about protected characteristics via a social media site, or even affirmatively seeks out information on a social media site, it puts the employer at risk of claims. Of course, if the employer uses such information as the basis for refusing to recruit the applicant, then the employer's actions could constitute unlawful discrimination. Even if there is no specific evidence that the employer took into account protected characteristics, if an applicant is rejected by an employment decision maker that had access to this prohibited information, the applicant would be able to present a prima facie case of discrimination, and the burden would then shift to the employer to demonstrate that there was a different reason for the decision to show that the information did not factor into the decision not to hire.

One state in particular – the state of Maryland – has actively discouraged employers from using social media to review potential job applicants. In March 2011, the state of Maryland recently referred for consideration a law that would prohibit Maryland employers from demanding that workers and job applicants turn over their passwords to specific websites or web-based accounts. Employers had been requesting password access in order to review the applicant's use of social media while not invading the individual's social media presence without his or her permission. The proposed law would prohibit employers from terminating, disciplining, refusing to hire, or otherwise penalizing workers or applicants for refusing to reveal their external website passwords. The bill would also ban employer threats to take such actions if

the employee or applicant refused to comply with a request to hand over a password.

2. What steps can be taken by employers to minimise such risks?

Some employers, after experimenting with using social media to review job applicants, have decided to ban all vetting of job applicants using information from social media. However, for employers who continue to wish to use social media screening for applicants, there is a process which can be taken to guard against unnecessary risk:

- Choose a person to scan social media sites that is not the same person who is reviewing applications to determine which applicants will go to the next step in the job application process. This way, the irrelevant material (which might contain sensitive personal data) will not make its way through to the decision maker.
- Applicants should be told, at the start of any application process, that a vetting or verification exercise using social media sites forms part of the process. It is most protective if the individual consents in writing to the potential employer's review of social media sites with respect to the applicant.
- The person vetting the applicants should be instructed to extract only legitimate and relevant information for the job application process. Such information might include the applicant's engaging in unlawful activity, making disparaging comments about the company or conveying that he or she was not serious about the position or planned to only hold the position for a short time.
- A social media policy or other written guidelines should back this up, so that the employer can demonstrate an intention to extract only relevant information.

- Job applicants who are rejected because of information gleaned from social networking should be given an opportunity to correct that information before any final decisions are taken.

However, given the risks described above, as well as the unreliability and insignificance of the majority of information gleaned from such vetting, this decision requires careful balancing for employers in the US.

3. *What problems could an employer face as a result of employees using social media sites?*

Breach of confidentiality

Social media sites provide an open forum for individuals to post and exchange information. Due to the nature of social media platforms, it is not uncommon for employees to end up posting confidential information about the employer and/or other employees. This could result in significant damage to the employer's business and reputation. This is especially true in regulated industries like financial services and health care, as well as in technology oriented businesses. Disgruntled former employees could also use social media to post confidential information regarding his or her former employer as a form of revenge.

Damage to employer's or third party's reputation

Employees could post information on a social media site that causes damage to the reputation of the employer and/or a third party. The injured party may try to hold the employer vicariously liable for the tortious conduct of an employee. The fact that an employer may have a claim against the employee concerned could be little comfort compared to the damage to the reputation of the employer.

Liability for endorsements

If an employee uses social media to make positive comments about a product made by his or her employer and fails to disclose his or her relationship with that company, the employer may be liable under the Federal Trade Commission guidelines. Further, should a consumer rely on that "endorsement" to his or her detriment, any ensuing damage could be attributed to the company. Endorsements or advice about using the product, if offered by employees, could also violate regulatory schemes, such as those put in place by the Food and Drug Administration.

Harassment/Unlawful discrimination

It is not uncommon for employees to post negative comments about fellow employees or others on social media sites. The comments could relate to a protected characteristic such as age, disability, race or gender. The comments may also constitute sexual or other legally prohibited harassment as a result of protected characteristics. In such circumstances, an employer could be vicariously liable for the actions of that employee.

An employer could also risk facing other discrimination claims if employees use information they have obtained from social media sites about other employees as the basis for treating them in a detrimental way.

An employer will have a potential defence to a claim for discrimination or harassment if it can show that it took all reasonable steps to prevent the employee from committing the discriminatory act in question.

Loss of productivity

In addition to the legal risks described above, there is also the risk of a loss of productivity if employees use social media sites while at work.

UNITED STATES

4. What steps can be taken by an employer to minimise the risks associated with employees using social media sites?

An employer can take the following steps:

- Impose an outright ban on access to social media sites at work. This approach could prove to be unpopular among employees and have an adverse impact on the morale within a workforce. Ultimately, the employer would need to weigh up the potential advantages and disadvantages in deciding whether to permit employees to access social media sites at work. A complete ban would not address the potential problems that could arise from postings by employees outside of working hours. Employers can easily find themselves liable for comments made after hours by employees, particularly where there is an obvious and clear link to the employment. Accordingly, comments posted by one employee about another employee after hours on a social networking site could still end up as the responsibility of the employer.
- Put in place a social media policy which deals with the use of social media sites during and outside of work hours. Such a policy should have provisions dealing with social media activity, but in particular:
    - set out the parameters governing the use of the employer's IT systems;
    - remind employees that social media activity may not necessarily be private;
    - prohibit discrimination, harassment or bullying of other employees, which could include negative comments about employees posted on social media sites;

- prohibit negative comments about the employer, its employees or third parties while making it clear that the policy does not infringe upon an employee's right to discuss wages, hours and working conditions with their co-workers;
- prohibit the disclosure of any confidential information that relates to the employer and/or other employees;
- train employees on how to avoid creating the appearance that employees may be speaking on behalf of company and require compliance with these processes;
- prohibit anonymity by stating that employees must disclose who they work for when commenting on the company or its business; and
- provide regular reminders and training about the policy

The policy should set out the consequences of a breach of the policy, which could include disciplinary action and/or dismissal.

- Provide awareness training to employees on conduct that could constitute discrimination, harassment and bullying. An employer would be able to defend any subsequent claim for discrimination or harassment if it can show that it took all reasonable steps to prevent the employee from committing the discriminatory act in question.
- Monitoring the use of social media sites at work could help to determine whether there is a loss of productivity as a result of employees accessing such sites. Monitoring employees' internet use during company time is less problematic from a legal standpoint. Giving notice of internet monitoring to employees and obtaining their consent is advisable.

UNITED STATES

- Employers should not attempt to gain access to private social media sites used by employees without permission. The Stored Communications Act arguably prohibits employers from monitoring employees' online activity without proper authorization.
- Incorporate within employment contracts or confidentiality agreements an appropriate confidentiality clause, which would afford protection to the employer in the event that an employee posts confidential information on a social media site.
- Disciplinary action may be taken against employees who misuse a social media site to the detriment of the employer. In some cases, an employer could consider dismissal. Each case will turn on its facts and an employer might want to obtain legal advice before proceeding to dismiss the employee in question.
- To restrict former employees from using social media sites such as LinkedIn to solicit former co-workers and clients, draft restrictive covenants to include social media.

Contributed by Mayer Brown LLP

Contact Details

Contact details

Asia

Hong Kong

Hong Tran
Mayer Brown JSM
16th - 19th Floors, Prince's Building,
10 Chater Road, Central, Hong Kong

E: hong.tran@mayerbrownjsm.com
T: +852 2843 4233
F: +852 2103 5070

People's Republic China

Rachel Zhang
JSM Shanghai Representative Office
Suite 2301, Tower II, Plaza 66,
1366 Nan Jing Road W.,
Shanghai 200040, China

E: rachel.zhang@mayerbrownjsm.com
T: +86 21 6120 1066 ext. 585 | +852 2843 4482
F: +86 21 6120 1068/69

Australia

John Denton
Corrs Chambers Westgarth
Bourke Place, 600 Bourke Street,
Melbourne VIC 3000, Australia

E: john.denton@corrs.com.au
T: +61 3 9672 3158
F: +61 3 9672 3010

India

Anand Prasad
Trilegal
A-38, Kailash Colony,
New Delhi -110 048, India

E: anand.prasad@trilegal.com
T: +91 11 4163 9393
F: +91 11 4163 9292

Indonesia

Richard Emmerson
Soewito Suhardiman Eddymurthy Kardono
14th Floor, Mayapada Tower,
Jl. Jend. Sudirman Kav. 28, Jakarta 12920,
Indonesia

E: richardemmerson@ssek.com
T: +62 21 521 2038
F: +62 21 521 2039

Japan

Chisato Higashio
Anderson Mori & Tomotsune
Izumi Garden Tower, 6-1, Roppongi 1-chome,
Minato-ku, Tokyo 106-6036, Japan

E: chisato.higashio@amt-law.com
T: +81 3 6888 1150
F: +81 3 6888 3150

Malaysia

Sivabalah Nadarajah
Shearn Delamore
7th Floor, Wisma Hamzah-Kwong Hing,
No. 1 Leboh Ampang 50100, Kuala Lumpur,
Malaysia

E: sivabalah@shearndelamore.com
T: +60 3 2076 2866
F: +60 3 2026 4506

New Zealand

Phillipa Muir
Simpson Grierson
Level 27, Lumley Centre,
88 Shortland Street, Auckland 1141

E: phillipa.muir@simpsongrierson.com
T: +64 09 977 5071
F: +64 09 977 5083

Pakistan

Salim Hasan

Meer & Hasan
1-Farid Kot Road Lahore,
54000 Pakistan

E: mail@meerhasan.com
T: +92 42 3723 5812
F: +92 42 3723 4332 | +92 42 3724 9893

Philippines

Rene Soriano

SyCip Salazar Hernandez & Gatmaitan
SyCipLaw Center, 105 Paseo de Roxas,
Makati City 1226, Philippines

E: rysoriano@syciplaw.com
T: +63 2 982 3500-3600
F: +63 2 818 7562

Singapore

Kala Anandarajah

Rajah & Tann
9 Battery Road,
No.25-01 Straits Trading Building,
Singapore 049910

E: kala.anandarajah@rajahtann.com
T: +65 6232 0111

South Korea

C.W. Hyun

Kim & Chang
Jeongdong Building, 17F, 21-15 Jeongdong-gil,
Jung-gu, Seoul 100-784, Korea

E: cwhyun@kimchang.com
T: +82 2 3703 1130
F: +82 2 737 9091 | +82 2 737 9093

Sri Lanka

John Wilson

John Wilson Partners
365 Dam Street Colombo 12,
Sri Lanka

E: john@srilankalaw.com
T: +94 11 232 4579 | +94 11 244 8931
F: +94 11 244 6954

Taiwan

Jaclyn Tsai

Lee, Tsai & Partners
9th floor, 218 Tun Hwa S. Road, Sec. 2,
Taipei 106, Taiwan, R.O.C.

E: jaclyntsai@leetsai.com
T: +886 2 2378 5780 ext. 2218
F: +886 2 2378 5781

Thailand

David Duncan

Tilleke & Gibbins
Supalai Grand Tower, 26th Floor,
1011 Rama 3 Road, Chongnonsi,
Yannawa, Bangkok 10120, Thailand

E: david.d@tillekeandgibbins.com
T: +66 2653 5555
F: +66 2653 5678

Vietnam

Suong Dao Nguyen

Mayer Brown JSM (Vietnam)
17th Floor, Saigon Tower, 29 Le Duan Street,
District 1, Ho Chi Minh City, Vietnam

E: dao.nguyen@mayerbrownjsm.com
T: +84 8 3822 8860 ext.128
F: +84 8 3822 8864

Contact details

EMEA

Angola

Gonçalo Falcão
Tauil & Chequer
Rua do Carmo, 43, 8º Andar - Centro,
20011-020 Rio de Janeiro, Brazil

E: gfalcao@mayerbrown.com
T: + 55 21 2127 4239
F: + 55 21 2127 4209

Belgium

Stéphane Baltazar
Van Olmen Wynant
Avenue Louise 221,
B-1050 Brussels, Belgium

E: stephane.baltazar@vow.be
T: +32 2 644 05 11
F: +32 2 646 38 47

Czech Republic

Richard Otevřel
Havel Holasek & Partners s.r.o
Tyn 1049/3, 110 00 Prague 1, Czech Republic

E: richard.otevrel@havelholasek.cz
T: +420 224 895 950
F: +420 224 895 980

Denmark

Tommy Angermair
Kromann Reumert
Raadhuspladsen 3, DK-8000 Aarhus C.,
Denmark

E: tma@kromannreumert.com
T: +45 3877 4310
F: +45 7012 1311

Egypt

Sally El Shalakany
Shalakany Law Firm
12, El Marashly St.,
Zamalek 11211, Cairo, Egypt

E: s_shalakany@shalakany.com
T: +202 2739 9390
F: +202 2737 0661

Finland

Seppo Havia
Dittmar & Indrenius
Pohjoisesplanadi 25A,
FI-00100 Helsinki, Finland

E: seppo.havia@dittmar.fi
T: +358 9 6817 0105
F: +358 9652 406

France

Laurence Dumure Lambert
Mayer Brown
20, Avenue Hoche, 75008 Paris, France

E: ldumurelambert@mayerbrown.com
T: +33 1 53 53 03 56
F: +33 1 53 96 03 83

Germany

Nicolas Rössler
Mayer Brown LLP
Bockenheimer, Landstrasse 98-100,
60323 Frankfurt am Main, Germany

E: nroessler@mayerbrown.com
T: +49 69 7941 2681
F: +49 69 7041 100

Greece

Christina Vlachtsis
M. & P. Bernitas Law Offices
5 Lykavittou Street,
GR-10672 Athens, Greece

E: christina.vlachtsis@bernitsaslawoffices.gr
T: +30 210 339 2950
F: +30 210 364 0805

Hungary

Péter Szemán
Ban, S.Szabo and Partners
H-1051, Budapest,
József nádor tér 5-6, Hungary

E: pszeman@bansszabo.hu
T: +36 1 266 3522
F: +36 1 266 3523

Iceland

Ólafur Eiríksson
Logos Legal Services
Efstaleiti 5, 103 Reykjavík,
Kt. 460100-2320, VSK 65426, Iceland

E: oe@logos.is
T: +354 5 400 300
F: +354 5 400 301

Ireland

Barry Walsh
A & L Goodbody
International Financial Services Centre,
Northwall Quay, Dublin 1,
Ireland

E: bwalsh@algoodbody.ie
T: +353 1 649 2000
F: +353 1 649 2649

Israel

Ashok Chandrasekhar
Goldfarb Seligman & Co.
Electra Tower, 98 Yigal Alon Street,
Tel Aviv 64239, Israel

E: ashok.chandrasekhar@goldfarb.com
T: +972 3 608 9917
F: +972 3 608 9120

Italy

Andrea Patrizi
Tonucci & Partners
Quorum Legal Network,
Viale Bruno Buozzi 32, 00197 Roma

E: apatrizi@tonucci.it
T: +972 3 1363 587

Mozambique

Gonçalo Falcão
Tauil & Chequer
Rua do Carmo, 43, 8º Andar - Centro,
20011-020 Rio de Janeiro, Brazil

E: gfalcao@mayerbrown.com
T: +55 21 2127 4239
F: +55 21 2127 4209

Netherlands

Elisabeth Thole
Van Doorne N.V.
Jachthavenweg 121, 1081 KM Amsterdam,
P.O. Box 75265, 1070 AG Amsterdam,
The Netherlands

E: thole@vandoorne.com
T: +31 20 6789 293
F: +31 20 7954 589

Contact details

Norway

Kristine Schei
Advokatfirmaet Thommessen AS
Haakon VII's Gate 10, PO Box 1484 Vika,
N-0161, Oslo, Norway

E: ksc@thommessen.no
T: +47 23 11 11 17
F: +47 91 36 88 55

Poland

Slawomir Paruch
Soltysinski Kawecki & Szlezak
ul. Wawelska 15 B
02-034 Warszawa, Poland

E: slawomir.paruch@skslegal.pl
T: +48 22 608 7370
F: +48 22 608 7070

Russia

Markus Schaer
Secretan Troyanov Schaer SA
Uliksa Usacheva 33, Bldg 1, 7th Floor,
119048 Moscow

E: markus.schaer@sts-law.ru
T: +7 495 232 0301
F: +7 495 232 0302

Spain

Antonio de Mariano Sánchez Jauregui
Ramón & Cajal Abogados.
Calle Almagro, 16-18,
28010 Madrid, Spain

E: amariano@ramoncajal.com
T: +34 91 576 1900
F: +34 91 575 8678

Sultanate of Oman

Syed Ali Naveed Arshad
Saslo
PO Box 1288, Ruwi, PC 112,
Sultanate of Oman

E: ana@saslo.com
T: +968 2463 6920
F: +968 2460 3400

Sweden

Nicklas Thorgerzon
Advokatfirman Vinge KB
Box 1703, SE-111 87,
Stockholm, Sweden

E: nicklas.thorgerzon@vinge.se
T: +46 70 7143 155
F: +46 8 614 3190

Switzerland

Christian Roos
Pestalozzi Attorneys at Law Ltd.
Loewenstrasse 1, Zurich 8001,
Switzerland

E: christian.roos@pestalozzilaw.com
T: +41 44 217 9200
F: +41 44 217 9217

Turkey

Gülnisa Coskun
Pekin & Pekin
Lamartine Caddesi No.10,
Taksim Istanbul, Turkiye 34437

E: gcoskun@pekin-pekin.com
T: +90 212 313 3548
F: +90 212 313 3535

UAE

Yasser Omar
Shalakany Law Office
Fortune Tower, Suite 2504, 25th Floor,
Jumeirah Lakes Towers, Sheikh Zayed Road,
PO Box 22880 Dubai, United Arab Eminates

E: yasser.omar@shalakany.ae
T: +971 4 332 7879
F: +971 4 332 7870

United Kingdom

Nicholas Robertson
Mayer Brown International LLP
201 Bishopsgate
London EC2M 3AF, United Kingdom

E: nrobertson@mayerbrown.com
T: +44 20 3130 3919
F: +44 20 3130 8944

Contact details

The Americas

United States

Marcia Goodman

Mayer Brown LLP
71 S. Wacker Drive, Chicago, IL 60606,
United States

E: mgoodman@mayerbrown.com
T: +1 312 701 7953
F: +1 312 706 9162

United States

Debbie Hoff man

Mayer Brown LLP
71 S. Wacker Drive, Chicago, IL 60606,
United States

E: dhoffman@mayerbrown.com
T: +1 312 701 7219
F: +1 312 706 9121

Brazil

Ivan Tauil

Tauil & Chequer
Rua do Carmo, 43, 8º Andar - Centro,
Rio de Janeiro, Brazil

E: itauil@mayerbrown.com
T: +55 21 2127 4213
F: +55 21 2127 4211

MAYER • BROWN

About Mayer Brown

Mayer Brown is a global legal services organization advising clients across the Americas, Asia and Europe. Our presence in the world's leading markets enables us to offer clients access to local market knowledge combined with global reach.

We are noted for our commitment to client service and our ability to assist clients with their most complex and demanding legal and business challenges worldwide. We serve many of the world's largest companies, including a significant proportion of the Fortune 100, FTSE 100, DAX and Hang Seng Index companies and more than half of the world's largest banks. We provide legal services in areas such as banking and finance; corporate and securities; litigation and dispute resolution; antitrust and competition; US Supreme Court and appellate matters; employment and benefits; environmental; financial services regulatory & enforcement; government and global trade; intellectual property; real estate; tax; restructuring, bankruptcy and insolvency; and wealth management.

OFFICE LOCATIONS

AMERICAS
- Charlotte
- Chicago
- Houston
- Los Angeles
- New York
- Palo Alto
- Washington DC

ASIA
- Bangkok
- Beijing
- Guangzhou
- Hanoi
- Ho Chi Minh City
- Hong Kong
- Shanghai
- Singapore

EUROPE
- Berlin
- Brussels
- Cologne
- Frankfurt
- London
- Paris

TAUIL & CHEQUER ADVOGADOS
in association with Mayer Brown LLP
- São Paulo
- Rio de Janeiro

ALLIANCE LAW FIRM
- Spain (Ramón & Cajal)

Please visit www.mayerbrown.com for comprehensive contact information for all Mayer Brown offices.